ISSN 1816-0301 (Print)
ISSN 2617-6963 (Online)

ИНФОРМАТИКА

ТОМ 17

1

ЯНВАРЬ-МАРТ

2020

ОТ РЕДАКЦИИ

В журнале «Информатика» публикуются оригинальные и обзорные статьи, описывающие результаты фундаментальных и прикладных исследований специалистов академического и вузовского профиля в области информатики и информационных технологий. Основной целью журнала является публикация наиболее значимых новых результатов в указанной области. Приветствуются статьи, описывающие заключительные результаты научных проектов и диссертационных исследований, открывающие новые направления исследований, которые находятся на стыке информатики и других наук.

Основные разделы журнала: математическое моделирование; обработка сигналов, изображений и речи; прикладные информационные технологии; интеллектуальные системы; космические информационные технологии и геоинформатика; параллельные вычисления; системы, приборы и устройства; распознавание образов; информационная безопасность; автоматизация проектирования.

Журнал «Информатика» включен Высшей аттестационной комиссией Республики Беларусь в список научных изданий для опубликования результатов диссертационных исследований. В декабре 2017 г. журнал включен в базу данных Российского индекса научного цитирования (РИНЦ). С помощью инструментов и сервисов, доступных на платформе eLIBRARY (раздел «Личный кабинет»), можно самостоятельно корректировать список своих публикаций и цитирований в РИНЦ.

Журнал рассчитан на широкий круг специалистов в области информатики и информационных технологий.

Адрес редакции:
ул. Сурганова, 6, к. 305, г. Минск, Беларусь
Тел. +375(017)284 26 22
E-mail: rio@newman.bas-net.by

Сайт журнала: inf.grid.by

THE EDITOR'S NOTE

The journal «Informatics» is a scientific publication in computer sciences and information technologies which reviews the results in basic and applied research of scientists from the universities and academies in the given field. The journal focuses on the most significant and modern papers such as research projects results and PhD/DSc papers in computer sciences, IT and at the boundaries.

The journal covers the following topics: mathematical modeling; processing and recognition of signals, images and speech; applied information technology; intelligent systems; space information technology and GIS technologies; parallel computing; systems, devices and equipment; image recognition; information security; computer aided design.

The journal «Informatics» is in the list of scientific publications recommended by the Higher Attestation Commission of the Republic of Belarus for scientists to publish the results of PhD/DSc research. In December 2017 the journal was included in the database of the Russian Science Citation Index (RISC) and provides the free access to reviewed electronic scientific paper, improving scientific information traffic and also raising quotation of works of the authors who are published in this journal (please use https://elibrary.ru or section for authors https://elibrary.ru_author_tools).

The journal is edited for a wide range of specialists in IT and computer sciences.

For further information:
Phone +375 (017) 284 26 22
E-mail: rio@newman.bas-net.by
Office 305, Surganova 6, 220012
Minsk, Belarus

Learn more at: https://inf.grid.by/jour

ISSN 1816-0301 (Print)
ISSN 2617-6963 (Online)

ОБЪЕДИНЕННЫЙ ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ
НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК БЕЛАРУСИ

ИНФОРМАТИКА

Том 17, № 1, январь-март 2020

Ежеквартальный научный журнал

Издается с января 2004 г.

Учредитель и издатель – Объединенный институт проблем информатики
Национальной академии наук Беларуси

ИНФОРМАТИКА

Том 17, № 1, январь-март 2020

Ответственный за выпуск *Мойсейчик Светлана Сергеевна*
Редактор *Гончаренко Галина Борисовна*
Корректор *Михайлова Анна Антоновна*
Компьютерная верстка *Бутевич Ольга Борисовна*

Сдано в набор 02.03.2020. Подписано в печать 23.03.2020. Формат 60×84 1/8. Бумага офсетная. Гарнитура Таймс. Ризография. Усл. печ. л. 13,7. Уч.-изд. л. 13,4. Тираж 50 экз. Заказ 1.

Государственное научное учреждение «Объединенный институт проблем информатики Национальной академии наук Беларуси».
Свидетельство о государственной регистрации издателя, изготовителя, распространителя печатных изданий № 1/274 от 04.04.2014. ЛП № 02330/444 от 18.12.13. Ул. Сурганова, 6, 220012, Минск, Беларусь.

ISSN 1816-0301 (Print)
ISSN 2617-6963 (Online)

THE UNITED INSTITUTE OF INFORMATICS PROBLEMS
OF THE NATIONAL ACADEMY OF SCIENCES OF BELARUS

INFORMATICS

Vol. 17, no. 1, January-March 2020

Published quarterly

Issued since January 2004

Founder and publisher – the United Institute of Informatics Problems
of the National Academy of Sciences of Belarus

INFORMATICS

Vol. 17, no. 1, January-March 2020

Issue Head *Sviatlana S. Maiseichyk*
Editor *Halina B. Hancharenka*
Corrector *Hanna A. Mikhailava*
Computer Imposition *Volha B. Butsevich*

Sent for press 02.03.2020. Output 23.03.2020. Format 60×84 1/8. Offset paper. Headset Times. Riesography. Printed sheets 13,7. Publisher's signatures 13,4. Circulation 50 copies. Order 1.

State Scientific Institution "The United Institute of Informatics Problems of the National Academy of Sciences of Belarus".
Certificate on the state registration of the publisher, manufacturer, distributor of printing editions no. 1/274 dated 04.04.2014. License for the press no. 02330/444 dated 18.12.13.
6, Surganov Str., 220012, Minsk, Belarus.

ISSN 1816-0301 (Print)
ISSN 2617-6963 (Online)

СОДЕРЖАНИЕ

ISSN 1816-0301 (Print)
ISSN 2617-6963 (Online)

CONTENTS

ISSN 1816-0301 (Print)
ISSN 2617-6963 (Online)

БИОИНФОРМАТИКА

BIOINFORMATICS

УДК 51-76:577.322:539.19:004.94
https://doi.org/10.37661/1816-0301-2020-17-1-7-17

Поступила в редакцию 15.01.2020
Received 15.01.2020

Принята к публикации 10.02.2020
Accepted 10.02.2020

Разработка генеративной состязательной нейронной сети для идентификации потенциальных ингибиторов ВИЧ-1 методами глубокого обучения

Г. И. Николаев[1], Н. А. Шульдов[2], А. И. Анищенко[2], А. В. Тузиков[1], А. М. Андрианов[3]✉

[1]Объединенный институт проблем информатики Национальной академии наук Беларуси, Минск, Беларусь
✉E-mail: alexande.andriano@yandex.ru

[2]Белорусский государственный университет, Минск, Беларусь

[3]Институт биоорганической химии Национальной академии наук Беларуси, Минск, Беларусь

Аннотация. Методами глубокого обучения разработан генеративный состязательный автоэнкодер для рационального дизайна потенциальных ингибиторов проникновения ВИЧ-1, способных блокировать участок белка gp120 оболочки вируса, критический для его связывания с клеточным рецептором CD4. Были выполнены исследования, включающие создание архитектуры автоэнкодера, формирование молекулярной библиотеки потенциальных лигандов белка gp120 ВИЧ-1 для обучения нейронной сети, молекулярный докинг лигандов с белком gp120 и расчет свободной энергии связывания, генерацию молекулярных дескрипторов химических соединений обучающего набора данных, обучение нейронной сети, оценку результатов обучения и работы автоэнкодера.

Рассмотрены результаты тестирования автоэнкодера на широком наборе соединений из молекулярной библиотеки ZINC. Показано, что совместное использование нейронной сети с виртуальным скринингом баз данных химических соединений формирует продуктивную платформу для идентификации базовых структур, перспективных для создания новых противовирусных препаратов, ингибирующих ранние стадии развития ВИЧ-инфекции.

Ключевые слова: методы глубокого обучения, генеративно-состязательный автоэнкодер, белок gp120, ингибиторы проникновения ВИЧ-1, методы молекулярного моделирования

Для цитирования. Разработка генеративной состязательной нейронной сети для идентификации потенциальных ингибиторов ВИЧ-1 методами глубокого обучения / Г. И. Николаев [и др.] // Информатика. – 2020. − Т. 17, № 1. – С. 7–17. https://doi.org/10.37661/1816-0301-2020-17-1-7-17

Development of a generative adversarial neural network for identification of potential HIV-1 inhibitors by deep learning methods

Grigory I. Nikolaev[1], Nikita A. Shuldov[2], Arseny I. Anischenko[2], Alexander V. Tuzikov[1], Alexander M. Andrianov[3]✉

[1]The United Institute of Informatics Problems of the National Academy of Sciences of Belarus, Minsk, Belarus
✉E-mail: alexande.andriano@yandex.ru

[2]Belarusian State University, Minsk, Belarus

[3]Institute of Bioorganic Chemistry of the National Academy of Sciences of Belarus, Minsk, Belarus

Abstract. A generative adversarial autoencoder for the rational design of potential HIV-1 entry inhibitors able to block the region of the viral envelope protein gp120 critical for the virus binding to cellular receptor CD4 was developed using deep learning methods. The research were carried out to create the architecture of the neural

network, to form virtual compound library of potential anti-HIV-1 agents for training the neural network, to make molecular docking of all compounds from this library with gp120, to calculate the values of binding free energy, to generate molecular fingerprints for chemical compounds from the training dataset. The training the neural network was implemented followed by estimation of the learning outcomes and work of the autoencoder. The validation of the neural network on a wide range of compounds from the ZINC database was carried out. The use of the neural network in combination with virtual screening of chemical databases was shown to form a productive platform for identifying the basic structures promising for the design of novel antiviral drugs that inhibit the early stages of HIV infection.

Key words: deep learning methods, a generative adversarial neural network, gp120 protein, HIV-1 entry inhibitors, molecular modeling

For citation. Nikolaev G. I., Shuldov N. A., Anischenko A. I., Tuzikov A. V., Andrianov A. M. Development of a generative adversarial neural network for identification of potential HIV-1 inhibitors by deep learning methods. *Informatics*, 2020, vol. 17, no. 1, pp. 7−17 (in Russian). https://doi.org/10.37661/1816-0301-2020-17-1-7-17

Введение. Современные методы компьютерного конструирования потенциальных лекарств значительно расширяют возможности фармацевтической индустрии, позволяя существенно сократить время и затраты, необходимые для создания новых терапевтических средств. Несмотря на то что эффективность компьютерных методов в создании лекарственных препаратов в настоящее время является общепризнанной, разработка новых математических подходов в сочетании с доступностью мощных и дешевых вычислительных ресурсов способствует их постоянному совершенствованию. Среди этих подходов важное место занимают методы машинного обучения (Machine Learning) и, в частности, методы глубокого обучения (Deep Learning), которые имеют большой потенциал для дальнейшего прогресса в данной области исследований. На сегодняшний день компьютерное конструирование потенциальных лекарств с помощью методов машинного обучения – одна из наиболее важных и быстро развивающихся областей хемоинформатики [1]. В отличие от физических моделей, основанных на физических закономерностях, таких же, как в квантовой химии или моделировании молекулярной динамики, в подходах машинного обучения реализуются алгоритмы распознавания образов для определения математических взаимосвязей между эмпирическими наблюдениями за малыми молекулами и их экстраполяциями для прогнозирования химических, биологических и физических свойств новых соединений. Кроме того, по сравнению с физическими моделями методы машинного обучения более эффективны и могут легко масштабироваться до больших наборов данных. Одним из преимуществ применения машинного обучения для конструирования лекарств является помощь исследователям в понимании и использовании взаимосвязи между химической структурой и ее биологической активностью (Quantitative Structure-Activity Relationship, QSAR) [2]. Современные методы машинного обучения могут использоваться для моделирования такой взаимосвязи или количественных отношений между структурой и свойством (Quantitative Structure-Property Relationship, QSPR), а также разработки интеллектуальных инструментов, способных достаточно точно предсказывать влияние химических модификаций соединения на его биологическую активность, фармакокинетические и токсикологические характеристики [1]. В связи с этим применение методов машинного обучения для компьютерного дизайна потенциальных лекарств имеет важное научное и практическое значение [3].

За последние несколько лет идея использования технологий искусственного интеллекта для ускорения процесса создания новых лекарственных препаратов и повышения эффективности программ фармацевтических исследований стала особенно востребованной в области хемоинформатики.

2018 г. ознаменовался впечатляющим числом проектов по сбору средств среди стартапов по поиску лекарств, полученных посредством использования искусственного интеллекта. Это свидетельствует о том, что работы по созданию нейронных сетей для идентификации потенциальных лекарств обладают серьезной привлекательностью для венчурных инвесторов. В настоящее время лондонская фармацевтическая компания BenevolentAI является лидером по сбору средств, достигнув в 2018 г. ошеломляющей отметки в 2 млрд долл. США (URL: https://www.linkedin.com/pulse/aimldl-drug-discovery-2018-year-review-andrii-buvailo). Компания

Atomwise, основанная в 2012 г. и ставшая пионером в использовании нейронных сетей для структурного проектирования лекарств, привлекла инвестиции в размере 45 млн долл. США для развития своей технологии открытия лекарств на основе алгоритмов глубокого обучения (URL: https://www.linkedin.com/pulse/aimldl-drug-discovery-2018-year-review-andrii-buvailo). Эта компания разработала нейронную сеть AtomNet и ежедневно тестирует с ее помощью 10 млн малых молекул для анализа их эффективности, прогнозирования токсичности и побочных эффектов с целью проверки на возможность использования в качестве лекарственных препаратов. Американская компания Insilico Medicine разрабатывает интеллектуальную систему, основанную на генеративных состязательных сетях, что позволит осуществлять процесс прогнозирования потенциальных лекарств от базового биологического моделирования и разработки биомаркеров до генерации молекул-лидеров, их оптимизации и доклинической проверки структур – кандидатов в лекарства (URL: https://www.linkedin.com/pulse/aimldl-drug-discovery-2018-year-review-andrii-buvailo).

В последние годы появилось большое число работ по применению методов машинного обучения для предсказания потенциальных ингибиторов ВИЧ-1 и резистентности вируса к анти-ВИЧ-препаратам (см., например, обзор [4]). Однако все эти исследования сконцентрированы на вирусных ферментах – обратной транскриптазе и протеазе. Соединения, блокирующие эти ферменты, не могут предотвращать проникновение вируса в клетку-мишень, что повышает внимание к ингибиторам ВИЧ-1, способным вмешиваться в ранние стадии жизненного цикла вируса путем блокирования процессов адсорбции и слияния мембран. Проникновение вирусного генома в клетку-хозяина – первый этап репликационного цикла ВИЧ-1 – представляет собой перспективную мишень для нескольких типов противовирусных препаратов, таких как ингибиторы связывания белка gp120 с первичным рецептором CD4, антагонисты корецепторов CCR5 и CXCR4 и ингибиторы слияния оболочки вируса с мембраной чувствительной клетки [5].

Цель настоящей работы – методами глубокого обучения создать генеративно-состязательную автоэнкодерную нейронную сеть для дизайна потенциальных ингибиторов ВИЧ-1, способных блокировать участок оболочки вируса, критический для его связывания с клеточным рецептором CD4. Для этого были проведены исследования, включающие:

– создание архитектуры состязательного автоэнкодера;

– формирование молекулярной библиотеки потенциальных лигандов белка gp120 ВИЧ-1 для обучения нейронной сети;

– молекулярный докинг лигандов с белком gp120 и расчет свободной энергии связывания;

– генерацию молекулярных дескрипторов (fingerprints) химических соединений обучающего набора данных;

– обучение нейронной сети;

– оценку результатов обучения и работы состязательного автоэнкодера.

Молекулярные дескрипторы предназначены для формального представления химических соединений в виде бинарных векторов фиксированной длины, что позволяет использовать такое представление для решения различных задач анализа и синтеза соединений методами машинного обучения.

Генеративно-состязательная нейронная сеть для идентификации потенциальных ингибиторов ВИЧ-1. Архитектура разработанного состязательного автоэнкодера состоит из двух нейросетей – автоэнкодера и дискриминатора, работающих во время обучения в соревновательном режиме. Такой режим позволяет настроить параметры автоэнкодера в режиме обучения и обеспечить получение качественных выходных данных на последующем этапе их генерирования. Задача дискриминатора состоит в том, чтобы отличать реальные данные от тех, которые генерирует автоэнкодер. Автоэнкодер представляет собой семислойную нейронную сеть, имеющую входной и выходной слои, латентный слой, а также четыре полносвязных слоя (рис. 1). На входной слой подаются молекулярные дескрипторы химических соединений, данные о которых проходят два полносвязных слоя (энкодер) и попадают на латентный слой, где к полученному результату добавляется численная оценка энергии связывания с молекулярной мишенью. Далее молекулярные дескрипторы проходят два полносвязных слоя (декодер) и попадают на выход, который, как и вход, представляет собой вектор молекулярного дескриптора. Работающая в таком режиме сеть уменьшает количество нейронов, поступающих на латентный

слой, который содержит сжатую информацию о векторе, поданном на вход сети, с последующим ее расширением на выходе. Латентный слой состоит их трех нейронов, два из которых получают значения от энкодера, а третий – значение энергии связывания с молекулярной мишенью. В рабочем режиме автоэнкодера на латентный слой, содержащий наиболее важную информацию об объекте, подаются случайные числа, которые затем проходят через декодер, генерирующий молекулярные дескрипторы молекул с требуемыми свойствами. Для генерации таких молекул важно, чтобы данные, поступающие на латентный слой после прохождения энкодера, имели нормальное распределение, которому обучены генератор случайных чисел и дискриминатор. Для обеспечения этого условия в процессе состязательного обучения энкодера и дискриминатора добивались того, чтобы энкодер был способен кодировать на латентный слой данные с нормальным распределением, а дискриминатор – отличать стандартное нормальное распределение (сгенерированные данные) от распределения, поступающего на латентный слой.

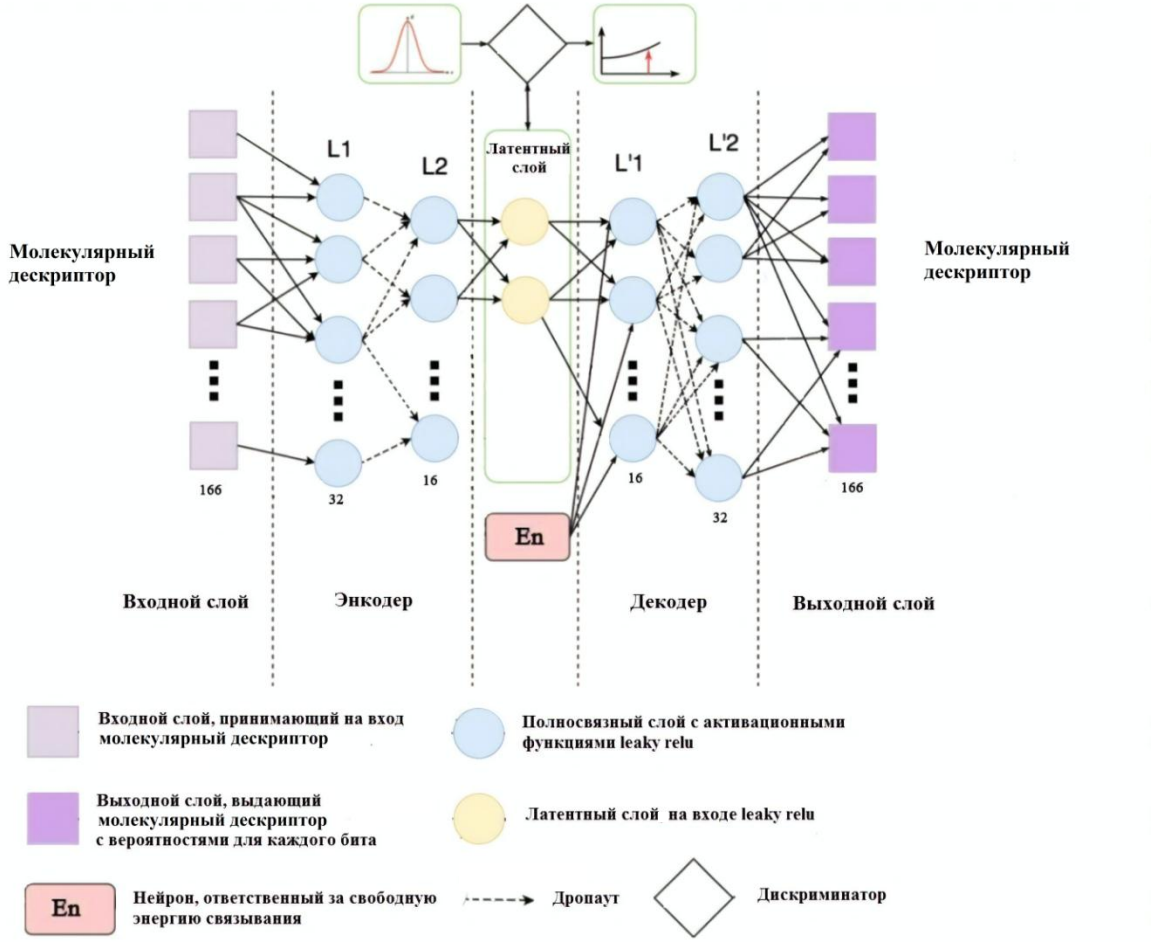


Рис. 1. Архитектура нейронной сети для генерации потенциальных ингибиторов ВИЧ-1, блокирующих CD4-связывающий сайт белка gp120 оболочки вируса

Разработанный состязательный автоэнкодер основан на модели нейронной сети, предназначенной для генерации химических соединений с противоопухолевой активностью [6], и имеет следующие особенности (рис. 1):

– на латентном слое используется нейрон, отвечающий за свободную энергию связывания. Он не взаимодействует с энкодером и подается только на вход декодера совместно с данными, полученными с помощью энкодера. Латентный слой состоит из трех нейронов;

– энкодер состоит из двух последовательных слоев L1 и L2 с 32 и 16 нейронами соответственно. Декодер включает два слоя – L'1 и L'2, содержащие 16 и 32 нейрона соответственно;

– дискриминатор состоит из четырех слоев, включающих 2, 16, 3 и 1 нейрон соответственно;

– на промежуточных слоях автоэнкодера используется активационная функция leaky relu [7]

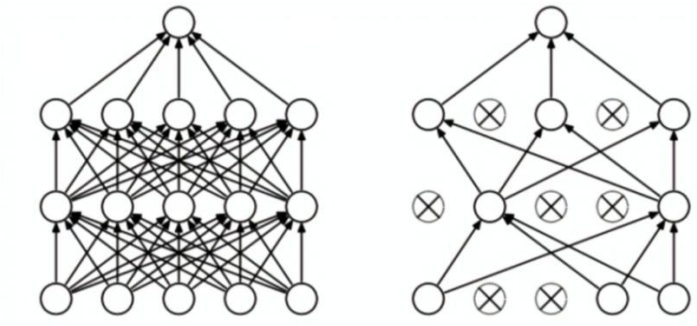
$$f(x) = \begin{cases} 0{,}01x \text{ при } x < 0, \\ x \text{ при } x \geq 0; \end{cases}$$

– на всех слоях дискриминатора используются сигмоидные активационные функции [8]

$$\sigma(x) = \frac{1}{1+e^{-x}};$$

– для дополнительного уровня защиты от переобучения между двумя полносвязными слоями энкодера и декодера добавлен слой дропаута, наличие которого позволяет нейронной сети полностью использовать свои параметры (веса) и выборочное случайное отключение во время обучения.

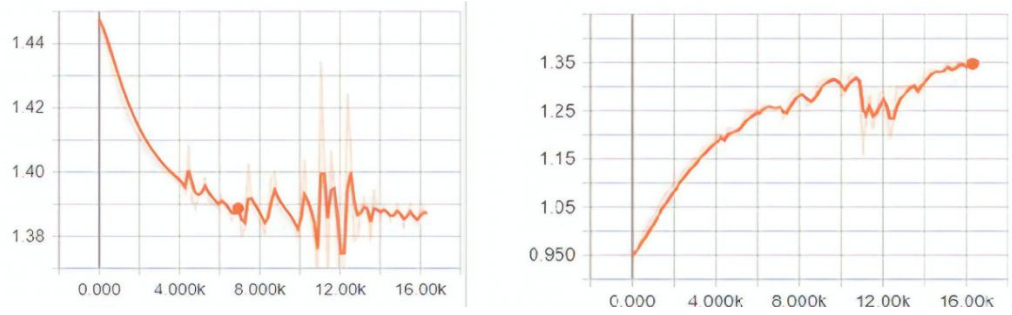
Основное назначение слоя дропаута заключается в том, чтобы вместо обучения одной сети обучить ансамбль из нескольких сетей, а затем усреднить полученные результаты. Схема работы слоя дропаута показана на рис. 2. Для обучения разработанного состязательного автоэнкодера использовался трехступенчатый итерационный процесс, который включал: 1) обучение дискриминатора различать заданное нормальное распределение от закодированного, полученного энкодером на латентном слое; 2) совместное обучение энкодера и декодера как автоэнкодера; 3) обучение энкодера сжимать данные таким образом, чтобы они представляли нормальное распределение.



а) *б)*

Рис. 2. Применение технологии дропаута: *а)* модель стандартной нейронной сети; *б)* модель нейронной сети с технологией дропаута, заключающейся в «выключении» из сети случайного набора нейронов, отмеченных на рисунке крестиком

Для дискриминационных моделей характерен более простой процесс обучения, чем для генеративных нейронных сетей. Поэтому при первых попытках обучить модель возникала ситуация, при которой функция потерь дискриминатора (ФПД) снижалась, а функция потерь энкодера росла (рис. 3).



а) *б)*

Рис. 3. Функции потерь дискриминатора (*а*) и энкодера (*б*) при более быстром обучении дискриминатора. На графиках представлены информативные части функций

Следует отметить, что при обучении нейронной сети сложно определить, действительно ли энкодер плохо обучается или он не способен «обмануть» дискриминатор. В связи с этим для улучшения процесса обучения были предприняты следующие меры:

– осуществлялось предварительное обучение дискриминатора до обучения всего автоэнкодера; предполагалось, что в этом случае дискриминатор будет отличать случайные числа, получаемые из нетренированного энкодера, от значений, соответствующих используемому нормальному распределению;

– в процессе обучения всей группы моделей дискриминатор тренировали не каждую эпоху*, а один раз в две эпохи, т. е. он обучался только в одну из двух эпох для модели автоэнкодера;

– для дискриминатора задавалась меньшая скорость обучения (learning rate), равная 0,001, в то время как для всего автоэнкодера она составляла величину, равную 0,005;

– в данные, сгенерированные из нормального распределения, добавлялся «небольшой шум», что затрудняло работу дискриминатора.

Данными изменениями была дополнена каждая эпоха (итерация) обучения, которая представляла собой трехступенчатый итерационный процесс:

1) энкодер и декодер обучались совместно как автоэнкодер;

2) дискриминатор обучался различать заданное нормальное распределение и закодированное «представление», полученное энкодером на латентном слое;

3) энкодер учился сжимать данные таким образом, чтобы они представляли собой нормальное распределение.

Дискриминатор и автоэнкодер обучались совместно в два этапа: реконструкции и регуляризации, выполняемые в каждом подмножестве из оригинальных данных. На этапе реконструкции (первой ступени итерации) автоэнкодер обновлял энкодер и декодер, чтобы минимизировать ошибку восстановления входных и выходных данных. На этапе регуляризации (второй ступени итерации) сначала обновлялась сеть дискриминатора, чтобы отличить истинные выборки (полученные с помощью генератора нормального распределения) от сжатых входных данных (данных на латентном слое, вычисленных автоэнкодером), а затем на третьей ступени итерации автоэнкодер обновлял свой энкодер, чтобы запутать сеть дискриминатора.

На рис. 4 изображены графики ФПД с учетом описанных выше изменений. Видно, что дискриминатор хорошо обучается классифицировать данные из нормального распределения, однако его способность правильно идентифицировать данные, полученные энкодером, падает.

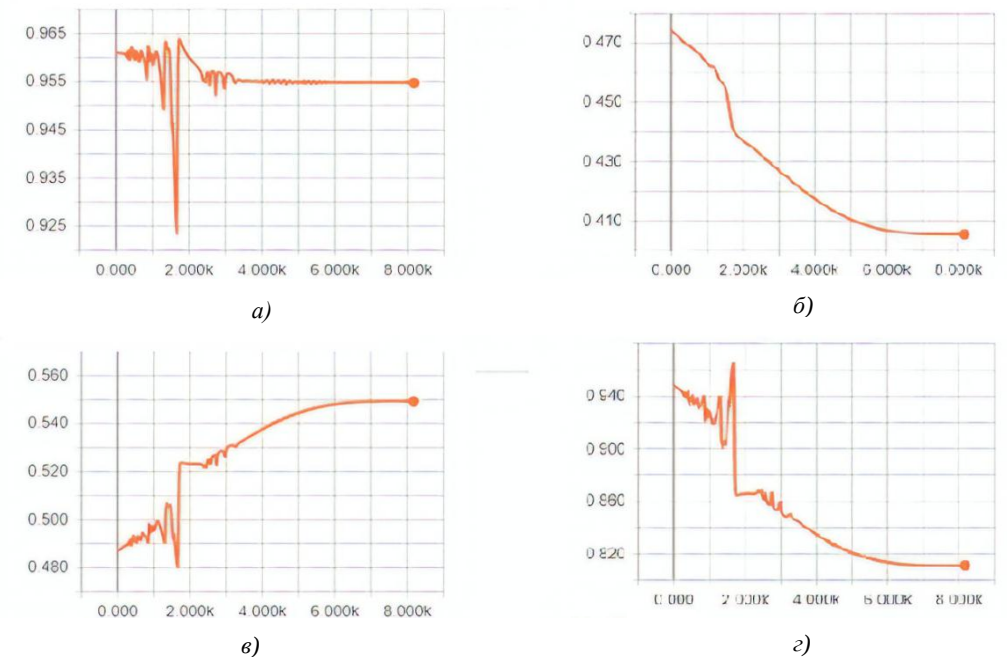
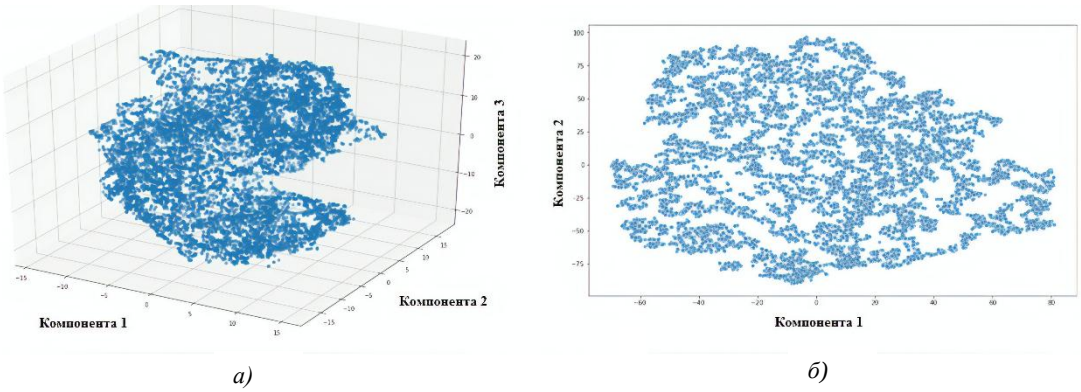


Рис. 4. Графики информативных частей ФПД (*а*), состоящей из ФПД для нормального распределения (*б*) и ФПД для закодированных данных (*в*), а также функция потерь энкодера (*г*)

*Эпоха – одна итерация в процессе обучения, включающая предъявление всех примеров из обучающего множества.

Для обучения автоэнкодера использовались следующие параметры:
количество эпох для главной версии модели, используемой для генерации, – 400;
скорость обучения всего автоэнкодера на первой ступени итерации – 0,005;
скорость обучения дискриминатора на второй ступени итерации – 0,001;
скорость обучения энкодера на третьей ступени итерации – 0,005;
параметр Batch size – 128;
оптимизатор – метод Adam [9].

В процессе обучения нейронной сети важно было убедиться, что в режиме генерации модель способна выдавать разные результаты для различных входных данных и производить множество молекулярных дескрипторов, а не генерировать их из небольшого числа возможных вариантов, поскольку существовала вероятность того, что такая ситуация отражает некий минимум исходных функций потерь. С целью снижения вероятности реализации такого сценария был использован алгоритм tSNE [10] для подвыборки из сгенерированных молекул (рис. 5), который представляет каждый сгенерированный молекулярный дескриптор двух- или трехмерной точкой таким образом, что похожие молекулярные дескрипторы отображаются близко расположенными точками, а непохожие дескрипторы – с большой вероятностью далеко отстоящими дуг от друга точками.



а) *б)*

Рис. 5. Результаты работы алгоритма tSNE для трех (*а*) и двух (*б*) компонент с подвыборкой из сгенерированных молекулярных дескрипторов

Создание молекулярной библиотеки для обучения автоэнкодера. Формирование обучающего набора данных выполнено в рамках подхода, использующего методологию клик-химии [11] для генерации наиболее вероятных структур-кандидатов биологически активных соединений. Для конструирования потенциальных лигандов с помощью программы DataWarrior (URL: http://www.openmolecules.org/help/basics.html) были созданы две молекулярные библиотеки. Первая библиотека включала отобранные из кластера Drug-Like базы данных ZINC [12, 13] небольшие молекулы (с молекулярной массой менее 250 Да) с азидной или алкиновой группой, содержащие ароматические фрагменты – элементы структуры, которые согласно данным об известных ингибиторах проникновения ВИЧ-1 [14, 15] играют ключевую роль для специфического взаимодействия с Phe43-полостью CD4-связывающего сайта белка gp120. Во вторую библиотеку были отобраны все низкомолекулярные соединения с молекулярной массой менее 250 Да, имеющие азидную или алкиновую группу. В результате работы программы DataWarrior первая библиотека включала 1388 соединений, а вторая библиотека – 3769. На следующем этапе эти соединения были использованы в качестве исходных реагентов для имитации реакции азид-алкинового циклоприсоединения с помощью программы AutoClickChem [16], которая рассматривала все возможные комбинации молекул из обеих библиотек. Это позволило получить набор из 1 655 301 гибридной молекулы, из которого 120 000 соединений, удовлетворяющие «правилу пяти» Липинского [17], были использованы для формирования обучающего набора данных. Оценку энергии связывания этих соединений с белком gp120 проводили методом молекулярного докинга – процедуры виртуального скрининга, позволяющей предсказать наиболее вероятные ориента-

ции лиганда в активном центре белка и рассчитать свободную энергию образования комплексов «лиганд-белок».

Генерация молекулярных дескрипторов MACCS (URL: http://www.dalkescientific.com/writings/NBN/fingerprints.html) в обучающем наборе данных осуществлялась с помощью программного пакета RDKit (URL: https://www.rdkit.org/) с открытым исходным кодом.

Молекулярный докинг лигандов из обучающего набора данных с белком gp120 выполнялся с помощью программы QuickVina 2 [18] с учетом конформационной подвижности лиганда. Трехмерная структура белка gp120 была выделена из комплекса этого гликопротеина с рецептором CD4 и антителом 17b (код 1GC1 из банка данных белков [19]). Атомы водорода добавлены к структуре белка gp120 с помощью программного пакета AutoDockTools. Ячейка для докинга представляла собой фрагмент белка gp120 с координатами $x \in$ (24 Å; 34 Å), $y \in$ (–15 Å; –5 Å), $z \in$ (78 Å; 88 Å), включающий Phe43-полость гликопротеина, т. е. объем ячейки составлял $10\times10\times10 = 1000$ Å^3. Для каждого лиганда генерировали девять моделей комплекса, лучших по значению оценочной функции. При этом параметр, характеризующий полноту поиска (охват конформационного пространства), был задан равным 50.

Оценка результатов обучения и работы автоэнкодера. Для тестирования работы автоэнкодера с помощью программного пакета RDKit была создана библиотека молекулярных дескрипторов MACCS (URL: http://www.dalkescientific.com/writings/ NBN/fingerprints.html) для 21 325 567 соединений из библиотеки Drug-Like базы данных ZINC [12, 13] и рассчитаны пять молекулярных дескрипторов для сгенерированных автоэнкодером молекул при пороговом значении энергии связывания с белком gp120, равном 5 ккал/моль. В результате виртуального скрининга созданной библиотеки для каждой из этих молекул с подобными молекулярными дескрипторами были найдены лиганды, которые показаны в таблице. При этом в качестве меры подобия молекулярных дескрипторов использовалось расстояние Хэмминга, определяемое в теории кодирования как число пар несовпадающих компонент сравниваемых векторов [20], и коэффициент Танимото, который вычислялся по формуле [21]

$$T(a, b) = \frac{N_c}{N_a+N_b-N_c},$$

где T – коэффициент Танимото, принимающий значения от 0 до 1; N_a – количество элементов в первом векторе; N_b – количество элементов во втором векторе; N_c – количество одинаковых элементов в двух векторах. В процессе скрининга библиотеки молекулярных дескрипторов из базы данных ZINC отбирались соединения, для которых коэффициент Танимото удовлетворял условию $T > 0{,}85$ [21]. В таблице молекулярные дескрипторы представлены строками из 166 бит, в которых каждый бит соответствует присутствию либо отсутствию определенного свойства или структурного фрагмента (URL: http://www.dalkescientific.com/writings/NBN/fingerprints.html). В векторах молекулярных дескрипторов, полученных после декодирования, 1 или 0 обозначает наличие либо отсутствие соответствующего структурного признака. Для каждого сгенерированного нейронной сетью лиганда приведены пять лучших по критериям R и T соединений из базы данных ZINC.

Идентифицированные в базе данных ZINC соединения подвергались процедуре докинга с белком gp120 и рассчитывалась энергия связывания с Phe43-полостью CD4-связывающего сайта оболочки ВИЧ. Молекулярный докинг проводился с помощью программы QuickVina 2 [18] с использованием вычислительного протокола, идентичного тому, что был применен при создании обучающего набора данных.

Анализ результатов молекулярного докинга найденных соединений с белком gp120 показал (таблица), что совместное использование нейронной сети с виртуальным скринингом библиотеки молекулярных дескрипторов позволяет идентифицировать лиганды с более низкой по сравнению с заданным пороговым значением энергией связывания. При этом идентифицированное в базе данных ZINC соединение с кодом ZINC000026430653 – аналог трех сгенерированных нейронной сетью лигандов – характеризуется величиной энергии связывания с белком gp120, сопоставимой со значением –9,5±0,1 ккал/моль, измеренным для комплекса CD4-gp120

методом изотермической титрационной калориметрии [22]. Эта величина, равная –8,8 ккал/моль, близка к значениям оценочной функции QuickVina 2 [18], полученным ранее [23–26] для высокоаффинных лигандов белка gp120, сконструированных методами молекулярного моделирования, а также для ингибиторов ВИЧ-1 NBD-11021 и NBD-14010, представляющих новое поколение полных функциональных антагонистов клеточного рецептора CD4 [27]. В частности, предсказанные QuickVina 2 значения свободной энергии Гиббса для ингибиторов NBD-11021 и NBD-14010 равны –8,4 и –8,6 ккал/моль соответственно.

Результаты тестирования нейронной сети

Молекулярные дескрипторы сгенерированных нейронной сетью лигандов	Коды соединений в базе данных ZINC	Расстояние Хэмминга R, критерий Танимото T	Энергия связывания, ккал/моль
00000000000000000000000000000000 00000000000000000000000100000000 01001000010000101011001000000 00010100010000000000010000000001 11011000010010101000010110010101 1010110101111110	ZINC000026430653	R = 3; T = 0,96	–8,8
	ZINC000037104033	R = 3; T = 0,96	–7,1
	ZINC000002786698	R = 4; T = 0,95	–7,0
	ZINC000055836809	R = 3; T = 0,96	–6,9
	ZINC000055843838	R = 4; T = 0,95	–6,5
00000000000000000000000000000000 00000000000000000000000100000000 01001000010000101011001000000 00011110010000000000010000000001 11011000010010101000010110010101 0010111101111110	ZINC000026430653	R = 5; T = 0,94	–8,8
	ZINC000037104033	R = 6; T = 0,93	–7,1
	ZINC000002786698	R = 6; T = 0,93	–7,0
	ZINC000163393594	R = 4; T = 0,95	–6,0
	ZINC000128895014	R = 4; T = 0,95	–5,9
00000000000000000000000000000000 00000000000000000000000100000000 01001000010000101011001000000 00011110010000000000010000000001 11011001010000001100010110010101 0010111101111110	ZINC000035245594	R = 6; T = 0,93	–6,6
	ZINC000163489237	R = 7; T = 0,92	–6,6
	ZINC000052221501	R = 7; T = 0,92	–6,6
	ZINC000600676089	R = 6; T = 0,93	–6,4
	ZINC000004006242	R = 7; T = 0,92	–5,9
00000000000000000000000000000000 00000000000000000000000100000000 01001000010000101011001000000 00010100010000000000010000000001 11011000010010001000010110010101 1010110101111110	ZINC000026430653	R = 4; T = 0,95	–8,8
	ZINC000002786698	R = 5; T = 0,94	–7,0
	ZINC000055836809	R = 4; T = 0,95	–6,8
	ZINC000037104033	R = 4; T = 0,95	–6,7
	ZINC000685198234	R = 4; T = 0,95	–6,0
00000000000000000000000000000000 00000000000000000000000100000000 01001000010000101011001000000 00011110010000000000010000000001 11011001010010101100010110010101 0010111111111110	ZINC000182934853	R = 7; T = 0,92	–7,4
	ZINC000771860139	R = 5; T = 0,94	–6,6
	ZINC000012991344	R = 7; T = 0,92	–6,0
	ZINC000128895014	R = 7; T = 0,92	–6,0
	ZINC000163393499	R = 7; T = 0,92	–6,0

Заключение. Результаты исследования свидетельствуют о том, что разработанная нейронная сеть представляет собой эффективную математическую модель для виртуального скрининга баз данных химических соединений, направленного на поиск малых молекул с высоким сродством к белку gp120 и разработку на их основе новых антиВИЧ-препаратов широкого спектра действия.

Разработанный автоэнкодер может быть использован для генерации молекулярных дескрипторов химических соединений, способных блокировать участок оболочки вируса, критический для его связывания с клеточным рецептором CD4. Анализ полученных результатов показывает, что совместное использование нейронной сети с виртуальным скринингом молекулярных библиотек формирует продуктивную платформу для идентификации базовых структур, перспективных для создания новых противовирусных препаратов, терапевтическое действие которых основано на ингибировании ранних стадий развития ВИЧ-инфекции.

References

1. Cherkasov A., Muratov E. N., Fourches D., Varnek A., Baskin I. I., …, Tropsha A. QSAR modeling: where have you been? Where are you going to? *Journal of Medicinal Chemistry*, 2014, vol. 201457, pp. 4977–5010.

2. Ali S. M., Hoemann M. Z., Aubé J., Georg G. I., Mitscher L. A., Jayasinghe L. R. Butitaxel analogues: Synthesis and structure-activity relationships. *Journal of Medicinal Chemistry*, 1997, vol. 40, pp. 236–241.

3. Vamathevan J., Clark D., Czodrowski P., Dunham I., Ferran E., …, Zhao S. Applications of machine learning in drug discovery and development. *Nature Reviews Drug Discovery*, 2019, vol. 18(6), pp. 463–477.

4. Dubey A. Machine learning approaches in drug development of HIV/AIDS. *International Journal of Molecular Biology: Open Access*, 2018, vol. 3(1), pp. 23–25.

5. Li W., Lu L., Li W., Jiang S. Small-molecule HIV-1 entry inhibitors targeting gp120 and gp41: a patent review (2010-2015). *Expert Opinion on Therapeutic Patents*, 2017, vol. 27, pp. 707–719.

6. Kadurin A., Aliper A., Kazennov A., Mamoshina P., Vanhaelen Q., Khrabrov K., Zhavoronkov A. The cornucopia of meaningful leads: Applying deep adversarial autoencoders for new molecule development in oncology. *Oncotarget*, 2017, vol. 8, pp. 10883–10890.

7. Xu B., Wang N., Chen T., Li M. *Empirical Evaluation of Rectified Activations in Convolutional Network*, 2015. Available at: https://arxiv.org/abs/1505.00853 (accessed 12.11.2019).

8. Rudoy G. I. The Choice of the Activation Function in the Prediction of Neural Networks. *Machine Learning and Data Analysis*, 2011, no. 1, pp. 16–39. Available at: https://arxiv.org/abs/1412.6980 (accessed 12.11.2019).

9. Kingma D., Ba J. *Adam: A Method for Stochastic Optimization*, 2014.

10. Van der Maaten L. Visualizing data using t-SNE. *Journal of Machine Learning Research*, 2008, vol. 9, pp. 2579–2605.

11. Kolb H. C., Finn M. G., Sharpless K. B. Click chemistry: Diverse chemical function from a few good reactions. *Angewandte Chemie International Edition*, 2001, vol. 40, no. 11, pp. 2004–2021.

12. Irwin J. J., Shoichet B. K. ZINC – a free database of commercially available compounds for virtual screening. *Journal of Chemical Information and Modeling*, 2005, vol. 45, no. 1, pp. 177–182.

13. Irwin J. J., Sterling T., Mysinger M. M., Bolstad E. S., Coleman R. G. ZINC: a free tool to discover chemistry for biology. *Journal of Chemical Information and Modeling*, 2012, vol. 52, no. 7, pp. 1757–1768.

14. Courter J. R., Madani N., Sodroski J., Schön A., Freire E., …, Smith A. B. 3rd. Structure-based design, synthesis and validation of CD4-mimetic small molecule inhibitors of HIV-1 entry: Conversion of a viral entry agonist to an antagonist. *Accounts of Chemical Research*, 2014, vol. 47, pp. 1228–1237.

15. Curreli F., Kwon Y. D., Zhang H., Scacalossi D., Belov D. S., …, Debnath A. K. Structure-based design of a small molecule CD4-antagonist with broad spectrum anti-HIV-1 activity. *Journal of Medicinal Chemistry*, 2015, vol. 58, pp. 6909–6927.

16. Durrant J. D., McCammon J. A. AutoClickChem: click chemistry in silico. *PLOS Computational Biology*, 2012, vol. 8, no. 3, e1002397. https://doi.org/10.1371/journal.pcbi.1002397

17. Lipinski C. A., Lombardo F., Dominy B. W., Feeney P. J. Experimental and computational approaches to estimate solubility and permeability in drug discovery and development settings. *Advanced Drug Delivery Reviews*, 2001, vol. 46, no. 1–3, pp. 3–26.

18. Alhossary A., Handoko S. D., Mu Y., Kwoh C. K. Fast, accurate, and reliable molecular docking with QuickVina 2. *Bioinformatics*, 2015, vol. 31, no. 13, pp. 2214–2216.

19. Kwong P. D., Wyatt R., Robinson J., Sweet R. W., Sodroski J., Hendrickson W. A. Structure of an HIV gp120 envelope glycoprotein in complex with the CD4 receptor and a neutralizing human antibody. *Nature*, 1998, vol. 393, pp. 648–659.

20. Blahut R. E. *Theory and Practice of Error Control Codes*. Addison-Wesley, 1983, 500 p.

21. Tanimoto T. T. *IBM Internal Report 17th*. IBM Corp., Armonk, New York, 1957.

22. Myszka D. G., Sweet R. W., Hensley P., Brigham-Burke M., Kwong P. D., …, Doyle M. L. Energetics of the HIV gp120-CD4 binding reaction. *Proceedings of the National Academy of Sciences*, 2000, vol. 97, pp. 9026–9031.

23. Andrianov A. M., Nikolaev G. I., Kornoushenko Y. V., Xu W., Jiang S., Tuzikov A. V. In silico identification of novel aromatic compounds as potential HIV-1 entry inhibitors mimicking cellular receptor CD4. *Viruses*, 2019, vol. 11, E746. https://doi.org/10.3390/v11080746

24. Andrianov A. M., Nikolaev G. I., Kornoushenko Y. V., Huang J., Jiang S., Tuzikov A. V. Virtual screening and identification of potential HIV-1 inhibitors based on cross-reactive neutralizing antibody N6. *Doklady of the National Academy of Sciences of Belarus*, 2019, vol. 63, no. 4, pp. 445–456.

25. Andrianov A. M., Nikolaev G. I., Kornoushenko Y. V., Karpenko A. D., Huang J., Jiang S., Tuzikov A. V. Identification of functional mimetics of the neutralizing anti-HIV antibody N6 by virtual screening and

molecular modeling N6. *Doklady of the National Academy of Sciences of Belarus*, 2019, vol. 63, no. 5, pp. 561–571.

26. Andrianov A. M., Nikolaev G. I., Kornoushenko Y. V., Huang J., Jiang S., Tuzikov A. V. In silico identification of high-affinity ligands of the HIV-1 gp120 protein, potential peptidomimetics of neutralizing antibody N6. *Mathematical Biology and Bioinformatics*, 2019, vol. 14, no. 2, pp. 430–449.

27. Curreli F., Kwon Y. D., Belov D .S., Ramesh R. R., Kurkin A. V., …, Debnath A. K. Synthesis, antiviral potency, in vitro ADMET, and X-ray structure of potent CD4 mimics as entry inhibitors that target the Phe43 cavity of HIV-1 gp120. *Journal of Medicinal Chemistry*, 2017, vol. 60, pp. 3124–3153.

Информация об авторах

Николаев Григорий Игоревич, научный сотрудник, Объединенный институт проблем информатики Национальной академии наук Беларуси, Минск, Беларусь.
E-mail: reshaemvsem@gmail.com

Шульдов Никита Андреевич, студент, Белорусский государственный университет, факультет прикладной математики и информатики, Минск, Беларусь.
E-mail: nickshuldov29@gmail.com

Анищенко Арсений Игоревич, студент, Белорусский государственный университет, факультет прикладной математики и информатики, Минск, Беларусь.
E-mail: BatsilaBox3@gmail.com

Тузиков Александр Васильевич, член-корреспондент, доктор физико-математических наук, профессор, директор, Объединенный институт проблем информатики Национальной академии наук Беларуси, Минск, Беларусь.
E-mail: tuzikov@newman.bas-net.by

Андрианов Александр Михайлович, доктор химических наук, главный научный сотрудник, Институт биоорганической химии Национальной академии наук Беларуси, Минск, Беларусь.
E-mail: alexande.andriano@yandex.ru

Information about the authors

Grigory I. Nikolaev, Researcher, The United Institute of Informatics Problems of the National Academy of Sciences of Belarus, Minsk, Belarus.
E-mail: reshaemvsem@gmail.com

Nikita A. Shuldov, Student, Belorussian State University, Faculty of Applied Mathematics and Computer Science, Minsk, Belarus.
E-mail: nickshuldov29@gmail.com

Arseny I. Anishenko, Student, Belorussian State University, Faculty of Applied Mathematics and Computer Science, Minsk, Belarus.
E-mail: BatsilaBox3@gmail.com

Alexander V. Tuzikov, Corresponding Member, Dr. Sci. (Phys.-Math.), Professor, Director, The United Institute of Informatics Problems of the National Academy of Sciences of Belarus, Minsk, Belarus.
E-mail: tuzikov@newman.bas-net.by

Alexander M. Andrianov, Dr. Sci. (Chem.), Chief Researcher, Institute of Bioorganic Chemistry of the National Academy of Sciences of Belarus, Minsk, Belarus.
E-mail: alexande.andriano@yandex.ru

ISSN 1816-0301 (Print)
ISSN 2617-6963 (Online)

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ

MATHEMATICAL MODELING

УДК 004.942
https://doi.org/10.37661/1816-0301-2020-17-1-18-28

Поступила в редакцию 24.02.2020
Received 24.02.2020

Принята к публикации 26.02.2020
Accepted 26.02.2020

Моделирующая среда для анализа алгоритмов трехмерной реконструкции объектов видеоэндоскопических исследований

А. Ф. Чернявский, Е. А. Головатая✉, В. С. Садов

Белорусский государственный университет, Минск, Беларусь
✉E-mail: katerina-golovataya@yandex.ru

Аннотация. Трехмерная реконструкция по результатам видеоэндоскопических обследований является перспективным направлением для поддержки медицинской диагностики и планирования терапии широкого спектра патологий. Тем не менее значительную сложность представляет оценка результатов такой реконструкции и проверка соответствия полученной трехмерной модели исходной сцене. В качестве решения этой проблемы предлагается использовать моделирующую среду для эмуляции процесса получения исходных видеоэндоскопических данных по сгенерированной сцене. Рассматривается задача трехмерного моделирования пищевода с использованием среды Autodesk 3ds Max и движка визуализации Arnold, а также задача процедурной генерации текстур для модели. Описывается генерация по подобию с использованием пространственно-периодических генеративно-состязательных моделей на основе сверточных нейронных сетей. Для сравнения результата реконструкции со сценой, сгенерированной при помощи предложенной моделирующей среды, вводится критерий оптимальности, с помощью которого сравниваются отдельные этапы алгоритма трехмерной реконструкции при оптимизации по методу связок.

Ключевые слова: моделирование, трехмерная реконструкция, генеративно-состязательные модели, генерация текстур, критерий оптимальности

Для цитирования. Чернявский, А. Ф. Моделирующая среда для анализа алгоритмов трехмерной реконструкции объектов видеоэндоскопических исследований / А. Ф. Чернявский, Е. А. Головатая, В. С. Садов // Информатика. – 2020. − Т. 17, № 1. – С. 18–28. https://doi.org/10.37661/1816-0301-2020-17-1-18-28

Modelling environment for analyzing the algorithms for 3D reconstruction of videoendoscopic research objects

Aleksandr F. Chernyavsky, Katsiaryna A. Halavataya✉, Vasili S. Sadau

Belarusian State University, Minsk, Belarus
✉E-mail: katerina-golovataya@yandex.ru

Abstract. Three-dimensional reconstruction based on the results of video endoscopic examination is a promising area for supporting medical diagnostics and treatment planning for a wide range of pathologies. Nevertheless, the assessment of the results of such reconstruction and verification of the correspondence of the obtained three-dimensional model to the original scene is significantly challenging. As a solution to this problem, the possibility of using a modelling environment to emulate the process of obtaining source video endoscopic data from the generated scene is suggested. The problem of three-dimensional modelling of the esophagus using the Autodesk 3ds Max environment and the Arnold visualization engine is considered. The paper describes the

procedural generation of textures for the model and proposes the using Periodic Spatial Generative Adversarial Network models based on convolutional neural networks. To compare the result of reconstruction with a scene, generated using the proposed modelling environment, an optimality criterion is introduced, by which the individual stages of the three-dimensional reconstruction algorithm are compared when the model is optimized using the bundle adjustment method.

Keywords: modelling, three-dimensional reconstruction, generative-competitive models, texture generation, optimality criterion

For citation. Chernyavsky A. F., Halavataya K. A., Sadau V. S. Modelling environment for analyzing the algorithms for 3D reconstruction of videoendoscopic research objects. *Informatics*, 2020, vol. 17, no. 1, pp. 18−28 (in Russian). https://doi.org/10.37661/1816-0301-2020-17-1-18-28

Введение. Одним из важных направлений в медицинской диагностике и терапии является дополнительная постобработка данных, которые могут быть получены в ходе различных обследований в цифровом виде. Значительный интерес с точки зрения компьютерной обработки представляют медицинские изображения, в частности данные, полученные по результатам видеоэндоскопических обследований. Медицинская видеоэндоскопия имеет широкий спектр применения для диагностики различных патологий внутренних органов человека. При этом важнейшими задачами являются первичное обнаружение объектов исследований (патологий, новообразований и т. п.), а также их детальный анализ для постановки корректного диагноза и выработки стратегии дальнейшего лечения. К основным показателям, которые необходимо оценить по видеопоследовательности, относятся размеры и пространственные характеристики найденных объектов, класс образований, а также динамика их развития с течением времени. Одним из перспективных направлений в построении репрезентативных представлений исходных данных для дальнейшего анализа является трехмерная реконструкция по итогам видеоэндоскопических обследований, в результате которой по отдельным участкам исходной видеопоследовательности строится полноцветная трехмерная модель. Использование такой модели упрощает оценку пространственных характеристик, облегчает визуальную экспертную диагностику, а также позволяет осуществлять моделирование различных терапевтических мероприятий.

Значительную сложность представляет задача оценки полученных результатов трехмерной реконструкции. Во многих случаях результирующую трехмерную модель достаточно сложно строго сопоставить с исходными объектами, по которым проводилась реконструкция, поскольку это требует определения всех их пространственных характеристик и сопоставимо по сложности с самой трехмерной реконструкцией. Оценка может осуществляться только по отдельным измерениям и только для тех объектов, пространственные характеристики которых известны заранее или могут быть легко определены. Для видеоэндоскопических изображений соответствующая информация в общем виде недоступна. При этом сами алгоритмы трехмерной реконструкции могут включать оптимизации для работы с определенным видом данных, поэтому оценка их работы при использовании других объектов и сцен является некорректной.

Оценка корректности результатов трехмерной реконструкции может использоваться для определения не только репрезентативности полученной модели относительно исходных данных, но и влияния отдельных этапов и оптимизаций самого метода трехмерной реконструкции на качество полученного результата.

Для решения описанных проблем в работе предлагается использовать моделирующую среду. Главное назначение моделирующей среды состоит в генерации трехмерного окружения, основные характеристики которого совпадают с характеристиками исследуемых объектов, после чего в рамках этого окружения производится моделирование процесса захвата изображений или видеоряда аналогично входным данным для исследуемого алгоритма. После построения трехмерной модели с применением алгоритма трехмерной реконструкции эту модель можно сравнить с исходной моделью, сгенерированной моделирующей средой. Результаты такого сравнения позволяют сделать вывод о состоятельности используемого алгоритма, а также оценить относительное влияние отдельных этапов алгоритма и используемых оптимизаций на качество конечной реконструкции.

Моделирование окружения на основе анатомических особенностей. Моделирующая среда для оценки алгоритмов трехмерной реконструкции подразумевает использование совокупности методов генерации трехмерных сцен в соответствии с определенным шаблоном. В частности, оценка по моделирующей среде должна проводиться на тех данных, к работе с которыми оптимизирован исследуемый алгоритм. В контексте задачи трехмерной реконструкции по результатам видеоэндоскопических исследований моделирующая среда должна генерировать сцену, приближенную к захвату видеопоследовательности на основании анатомических особенностей внутренних органов человека. В работе рассматривается возможность генерации окружения для моделирования гастроэндоскопии, основанной на эталонной модели пищевода человека.

Построение искусственных моделей внутренних органов находит широкое применение для обучения медицинского персонала. Полученные модели могут в дальнейшем использоваться для разработки интерактивных симуляторов и других видов обучающих программ, а также совместно с технологиями 3D-печати для планирования сложных процедур и оперативных вмешательств [1].

Большинство существующих моделей внутренних органов основано на их представлении с точки зрения анализа анатомии человека. В частности, модели желудочно-кишечного тракта, в том числе и пищевода, как правило, представлены структурой и текстурами их поверхностей снаружи, в то время как для моделирования процесса получения видеоэндоскопических данных требуются модели, поверхности и текстуры для которых определены изнутри аналогично прохождению дистального конца эндоскопа. К примеру, была рассмотрена возможность использования данных, предоставленных открытой платформой BioDigital Human (URL: https://www.biodigital.com), занимающейся свободной и коммерческой реализацией трехмерных моделей отдельных участков внутренних органов человека. Большинство моделей желудочно-кишечного тракта в соответствующей базе демонстрируют только особенности его строения снаружи, а некоторые модели съемки изнутри ориентированы на моделирование специфических видов образований в очень небольшом участке. Кроме того, использующиеся текстуры имеют достаточно низкое разрешение, что приводит к ненадлежащему качеству первичного изображения, которое было бы репрезентативно относительно реальных видеоэндоскопических данных. В этой связи возникает необходимость построения эталонной модели пищевода вручную на основании анатомических особенностей отдельных участков.

Для построения исходной модели и реализации динамики с течением времени использовалась среда Autodesk 3ds Max. В качестве базового примитива для моделирования поверхности пищевода может применяться цилиндрическая поверхность с несколькими изгибами. С целью эмуляции движения стенок пищевода при прохождении эндоскопа реализовывается сужение и расширение согласно периодическому закону с небольшой амплитудой. Для реалистичного моделирования самой поверхности и отражения света проходящего источника освещения использовался многоуровневый смешанный шейдер, реализованный на основе шейдера эмиссии для колеровки, шейдера подповерхностного рассеивания (subsurface scattering), шейдера глянцевого эффекта на основе двунаправленной функции распределения рассеивания (glossy bidirectional scattering distribution function shader) и шейдера преломления нормали в соответствии со случайной величиной с гауссовым распределением. Тем не менее равномерный материал на основе многоуровневого шейдера не может применяться для моделирования всей внутренней поверхности пищевода из-за наличия дополнительных особенностей – сосудистой структуры, отдельных выступов, а также образований. Традиционным подходом к добавлению таких особенностей на моделируемые трехмерные поверхности является использование статической текстуры. Однако существенным недостатком статического текстурирования является периодичность полученной поверхности. Одним из возможных решений этой проблемы может быть использование процедурной генерации текстур, при которой каждый участок поверхности текстурируется в соответствии с некоторым процессом, являющимся в общем случае случайным в определенных пределах [2].

Методы генерации текстур. Задача генерации текстур состоит в проведении такой процедуры, которая способна построить произвольную текстуру поверхности, не используя при этом шаблонную текстуру напрямую. Другими словами, генерация текстур подразумевает случайное или псевдослучайное создание отдельного участка текстуры на основании не шаблонного изображения, а некоторых его характерных особенностей. Таким образом, процедурно генерируемые текстуры должны быть похожи на шаблонную, но не должны с ней совпадать.

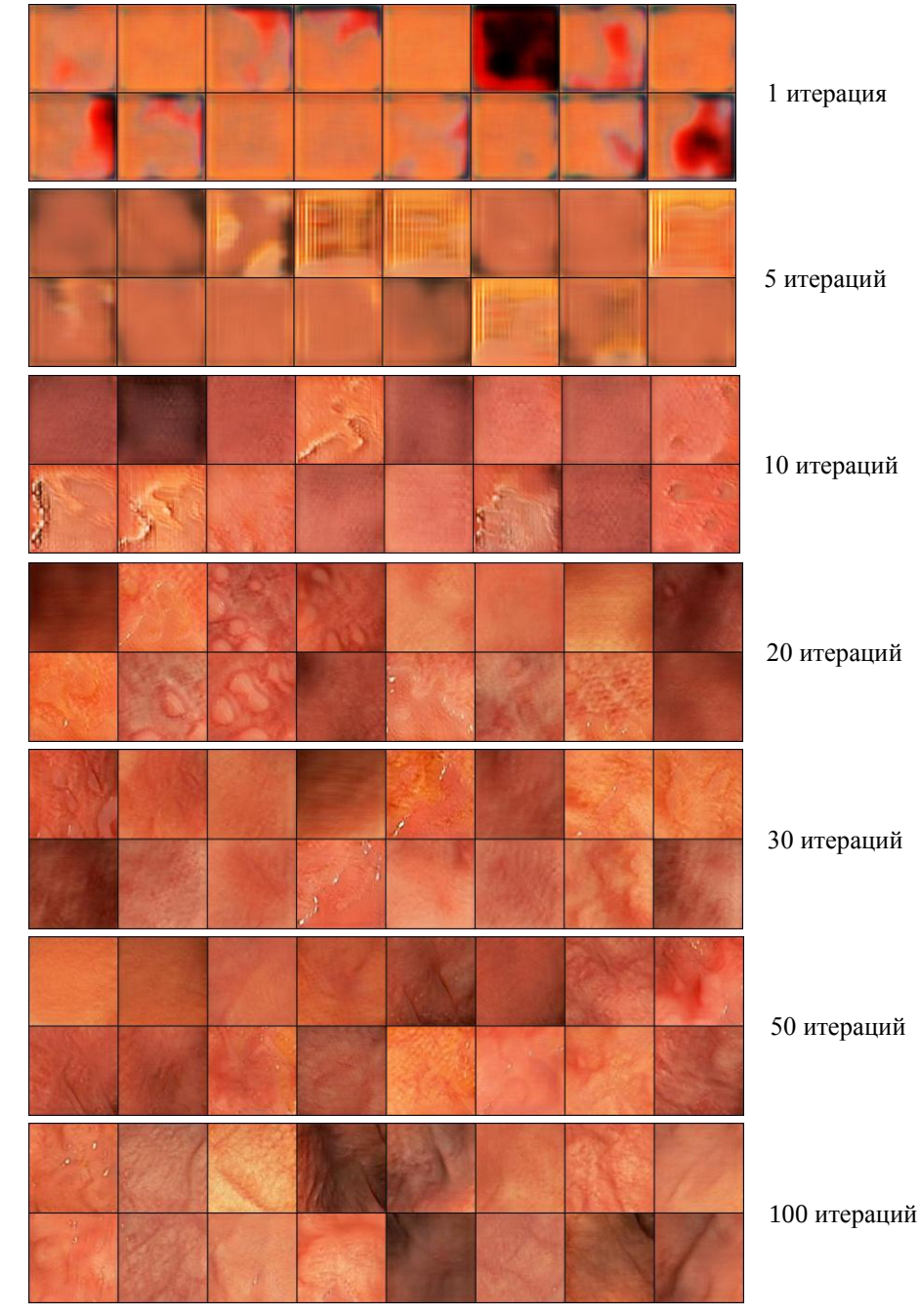
Методы генерации текстур можно разделить на два вида: основанные на анализе пикселов (pixel-based) и основанные на анализе участков (patch-based).

Методы на основе анализа пикселов заключаются в применении некоторой схемы отбора, в соответствии с которой по последовательностям пикселов анализируемой текстуры строится частотная модель используемых в ней яркостей, а также периодичностей отдельных цветовых составляющих по длине. Повторное сэмплирование полученной величины в дальнейшем может использоваться для попиксельной генерации текстуры, в которой статистическое распределение яркостей пикселов в зависимости от их отклонения от начальной точки будет полностью соответствовать статистическому распределению яркостей исходной текстуры, на основании которой должна производиться генерация. Во многих случаях данные методы, предоставляют механическую процедуру для рандомизации отдельных пикселов исходной текстуры с сохранением статистических свойств в частотной области. Однако такие перестановки, как правило, показывают плохой результат на строго периодических структурах, где переходы между отдельными сгенерированными участками могут быть пропущены, что, в свою очередь, ведет к появлению заметных артефактов и «разрывов» на сгенерированной поверхности. Полученная процедура генерации является, по сути, вырожденной формой реализации выборки по непараметрической марковской сети переходов яркостей пикселов, сформированной в порядке обхода при помощи анализа исходной текстуры.

Методы на основе анализа участков реализуются частичным переносом исходной текстуры, при этом координаты отдельных участков для переноса определяются последовательно по некоторому случайному закону с заданным характером распределения. Для обеспечения плавных переходов между полученными участками могут использоваться различные алгоритмы, основанные на оценке взаимного перекрытия участков друг с другом. Перестановки осуществляются таким образом, чтобы минимизировать разницу между участками на перекрытии, после чего итоговая текстура может быть получена усреднением или параметрическим отбором. В отличие от метода на основе анализа пикселов методы на основе анализа участков хорошо подходят для анализа значительно периодических структур, поскольку сэмплирование исходной текстуры может осуществляться произвольно исходя из требований параметрического отбора, т. е. может быть сформулировано в виде задачи оптимизации.

В последнее время значительное распространение получил также подход с использованием генеративно-состязательных нейросетевых моделей на основе сверточных нейронных сетей. Как правило, такие сети используются для задачи переноса стиля (style transfer). Для этого весá или значения активаций нейронов более поверхностных слоев при подаче на сверточную сеть целевого изображения заменяются соответствующими значениями весов или активаций этих же нейронов, которые получены при подаче на сверточную сеть изображения с эталонным стилем. С другой стороны, при использовании такой сети в качестве генеративной в генеративно-состязательных моделях дискриминатор может быть обучен на преобразование высокоуровневых абстрактных описаний отдельных участков изображения в текстурированные участки, сформированные на низкоуровневых особенностях используемой сети, которые описаны с помощью матрицы Грэма. Наиболее популярной нейросетевой архитектурой для решения данной задачи на сегодняшний день является сверточная нейронная сеть VGG-19 [3].

Для текстурирования поверхности пищевода в разработанной моделирующей среде используется генеративная модель на основе пространственно-периодических генеративно-состязательных нейронных сетей (Periodic Spatial Generative Adversarial Networks, PSGAN) [4]. Эта модель основана на проекции некоторого псевдослучайного входного вектора в пространство входных признаков в сверточной сети для генератора с искусственным расширением полученного изображения по горизонтали и вертикали с применением генеративной модели.



а)

б)

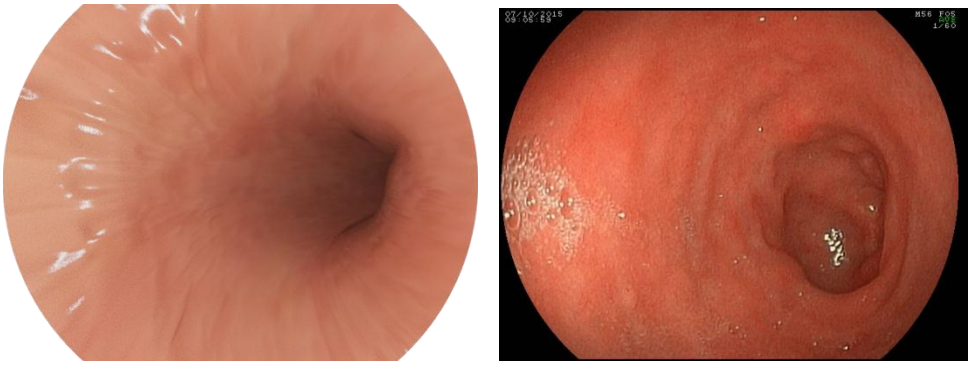
Рис. 1. Генерация текстур на основе пространственно-периодических генеративно-состязательных нейронных сетей: *а)* примеры выхода генератора на различных итерациях обучения; *б)* примеры периодических текстур высокого разрешения, сгенерированных обученной сетью

Аналогичным образом дискриминатор генеративно-состязательной сети оценивает реалистичность сгенерированных данных посредством анализа отдельных участков изображения, а не всего изображения целиком, после чего обратная связь с генератором позволяет разрабатывать структуры с определенной периодичностью по входным данным. Дополнительно в дискриминатор может быть введен метод детектирования кратной периодичности, чтобы обеспечить более уникальный и равномерный результат на выходе генератора.

В качестве входных данных для генератора использовались участки 100×100 пикселов, извлеченные и ректифицированные вручную из видеопоследовательности, полученной в результате видеоэндоскопического обследования. С помощью алгоритма рекурсивной точечной заливки с исходных изображений были устранены блики, поскольку эмуляция бликов и эффекта отражения света от источника в моделирующей среде обеспечивается не самой текстурой, а наложенным на нее шейдером с отражением, описанным ранее. Полученные результаты генерации текстур оценивались визуально.

Примеры сгенерированных текстур на различных итерациях обучения генератора и дискриминатора показаны на рис. 1. Видно, что уже после 30 итераций генеративная модель смогла создавать базовые текстуры с достаточным качеством для использования в трехмерном моделировании внутренних органов человека. Особенностью генерации является тот факт, что сами текстуры сформированы в результате анализа видеоэндоскопических изображений, полученных в результате реального обследования. Таким образом, при помощи пространственно-периодических генеративно-состязательных нейронных сетей можно осуществить генерацию по подобию любого фактического видеоэндоскопического обследования для формирования текстур, максимально реплицирующих особенности внутренних органов именно этого исследования.

Моделирование параметров камеры и ее движения. Моделирование процесса первичного захвата информации при помощи камеры на дистальном конце эндоскопа осуществлялось средствами Autodesk 3ds Max и движка визуализации Arnold [5]. В стандартной конфигурации широкоугольные камеры моделируются при помощи камер типа «рыбий глаз» (fisheye camera), которые, в свою очередь, моделируют поступающий в камеру свет как результат отражения от единичной сферы с абсолютно отражающей поверхностью в объектив камеры, расположенной в противоположном от сцены направлении. Основным параметром такой камеры является угол обзора, увеличение которого приводит к более выраженным дисторсионным искажениям. Для имитации эффекта появления бликов от источника освещения, сонаправленного с осью камеры, используется псевдослучайный шум для искажения карты нормалей с дополнительным точечным источником освещения. Для имитации размытия из-за движения камеры применяется шейдер размытия от движения (motion blur) камеры. Чтобы увеличить силу размытия, эмулируется захват изображения камерой в режиме высокой экспозиции (от 100 мс и выше), благодаря чему могут формироваться условия съемки, похожие на захват изображения камерой при проведении видеоэндоскопического обследования. Пример полученной модели показан на рис. 2.



а) *б)*

Рис. 2. Видеоэндоскопическое изображение, полученное: *а)* в результате генерации на основе моделирующей среды; *б)* при проведении реального обследования

Сравнение и оценка качества алгоритмов трехмерной реконструкции на данных видеоэндоскопических систем. Моделирующая среда и трехмерная модель, сгенерированная на ее основе, могут использоваться в качестве эталонных для дальнейшего сравнения результатов трехмерной реконструкции. Тем не менее возникает необходимость выработки критерия, определяющего, насколько результат трехмерной реконструкции соответствует исходной модели. Поскольку моделирование процесса захвата позволяет отображать лишь малую часть модели при последующей реконструкции, дискретизация моделей на вокселы и поточечное сравнение не являются информативными. Кроме того, значительное влияние на результат такого сравнения оказывает тот факт, что полезной информацией в модели, полученной после трехмерной реконструкции, является не объемная геометрия и внутреннее наполнение соответствующих объектов, а корректная реконструкция наблюдаемых в исходной модели поверхностей. Для решения этой проблемы в работе предлагается оценка системы уравнений, получаемой в процессе трехмерной реконструкции после оптимизации по методу связок [6]. С помощью константных координат тестовых точек координатная система пространства моделирования при трехмерной реконструкции может быть соотнесена с координатной системой модели, сгенерированной с помощью моделирующей среды. Это позволяет сравнивать координаты отдельных точек на проекциях (изображениях) как с реальными координатами исходной модели, так и с предсказанными координатами по результатам трехмерной реконструкции. Кроме того, поскольку моделирующая среда также контролирует процесс управления камерой и захвата первичных изображений, для каждого из полученных кадров известными являются параметры внутреннего и внешнего ориентирования камеры: координаты и ориентация камеры, фокусное расстояние и параметры системы съемки.

В качестве критерия оптимальности на основе моделирующей среды используется среднеквадратическое отклонение положения ключевой точки в исходном трехмерном пространстве, среднеквадратическое отклонение положения камеры в трехмерном пространстве и среднеквадратическое отклонение угла поворота камеры с различными весами. При известных координатах ключевых точек $\left(X_i^*, Y_i^*, Z_i^*\right)$ и их проекциях на различных изображениях, координатах положений камеры $\left(X_{0j}^*, Y_{0j}^*, Z_{0j}^*\right)$ и углах поворота камеры $\left(\omega_j^*, \varphi_j^*, \beta_j^*\right)$ их значения могут быть сопоставлены с вычисленными в результате реконструкции координатами ключевых точек $\left(X_i, Y_i, Z_i\right)$, положениями камеры $\left(X_{0_j}, Y_{0j}, Z_{0j}\right)$ и углами поворота $\left(\omega_j, \varphi_j, \beta_j\right)$. Итоговая оценка модели может быть задана величиной ошибки модели

$$E = w_1 E_{kp} + w_2 E_c + w_3 E_a, \tag{1}$$

где w_1, w_2, w_3 – весовые коэффициенты; E_{kp} – среднеквадратическая ошибка определения положения ключевой точки, вычисляемая для N_p ключевых точек по фактическим координатам ключевых точек $\left(X_i^*, Y_i^*, Z_i^*\right)$ и их координатам, полученным в результате реконструкции $\left(X_i, Y_i, Z_i\right)$:

$$E_{kp} = \frac{1}{N_p}\sqrt{\sum_{i=1}^{N_p}\left(\left(X_i - X_i^*\right)^2 + \left(Y_i - Y_i^*\right)^2 + \left(Z_i - Z_i^*\right)^2\right)}; \tag{2}$$

E_c – среднеквадратическая ошибка определения положения камеры, вычисляемая для N_c камер по фактическим координатам положений камеры $\left(X_{0j}^*, Y_{0j}^*, Z_{0j}^*\right)$ и координатам положений камеры, полученными по методу связок $\left(X_{0_j}, Y_{0j}, Z_{0j}\right)$:

$$E_c = \frac{1}{N_c}\sqrt{\sum_{j=1}^{N_c}\left(\left(X_{0j} - X_{0j}^*\right)^2 + \left(Y_{0j} - Y_{0j}^*\right)^2 + \left(Y_{0j} - Y_{0j}^*\right)^2\right)}; \tag{3}$$

E_a – среднеквадратическая ошибка определения угла наклона камеры, рассчитываемая для N_c камер по фактическим углам наклона $\left(\omega_j^*, \varphi_j^*, \beta_j^*\right)$ и углам, вычисленным в процессе реконструкции $\left(\omega_j, \varphi_j, \beta_j\right)$:

$$E_a = \frac{1}{N_c}\sqrt{\sum_{j=1}^{N_c}\left(\left(\omega_j - \omega_j^*\right)^2 + \left(\varphi_j - \varphi_j^*\right)^2 + \left(\beta_j - \beta_j^*\right)^2\right)}. \quad (4)$$

Оценка ошибки (1)–(4) фактически является нормированной оценкой среднеквадратической ошибки обратной проекции точки в виде L2-нормы вектора ошибок. Преимущество такой оценки заключается в простоте вычисления при наличии фактических данных о восстановленной среде.

К недостаткам предложенной оценки можно отнести невозможность оценить корректность модели при построении после этапа уплотнения облака точек. Поскольку все координаты ключевых точек, участвующих в реконструкции, должны быть учтены и определены непосредственно решением системы уравнений по методу связок, координаты всех других точек, добавленных в модель после уплотнения, невозможно соотнести с исходным трехмерным объектом в пространстве. Аналогично сложной является задача сравнения поверхности модели, сгенерированной при помощи моделирующей среды, и поверхности, полученной в результате реконструкции. Поэтому такой метод может использоваться только для оценки реконструкции и для подбора параметров на этапах выборки кадров, сопоставления ключевых точек, составления и решения системы уравнений по методу связок.

Хотя абсолютные значения оценки (1) не дают возможность оценить итоговое качество реконструкции, можно оценить влияние тех или иных гиперпараметров метода реконструкции на результирующую ошибку. В качестве основных оцениваемых гиперпараметров рассматриваются алгоритмы поиска и сопоставления ключевых точек (детекторы и дескрипторы), а также модель построения проекции для формирования уравнений коллинеарности. В результате оценки была проанализирована модель центральной проекции с коррекцией дисторсии и обрезкой кадра и модель сферической широкоугольной проекции [7]. В качестве детекторов и дескрипторов были рассмотрены гистограммный дескриптор SIFT [8], детектор FAST [9] с бинарным дескриптором BRIEF [10], бинарный дескриптор ORB [11], а также предложенные в работе [12] сегментные детектор и дескриптор.

На рис. 3 показаны нормированные на максимум значения ошибки для различных комбинаций дескрипторов и детекторов ключевых точек при использовании стандартной центральной проекции и сферической широкоугольной проекции, а также количество ключевых точек, взятое для построения модели. Для оценки применялись 10 различных моделей, сгенерированных описанной ранее моделирующей средой, с различными параметрами текстурирования и геометрии сцены. В качестве исходных данных для оптимизации по методу связок использовались видеопоследовательности длиной 5 с и частотой кадров 30 Гц.

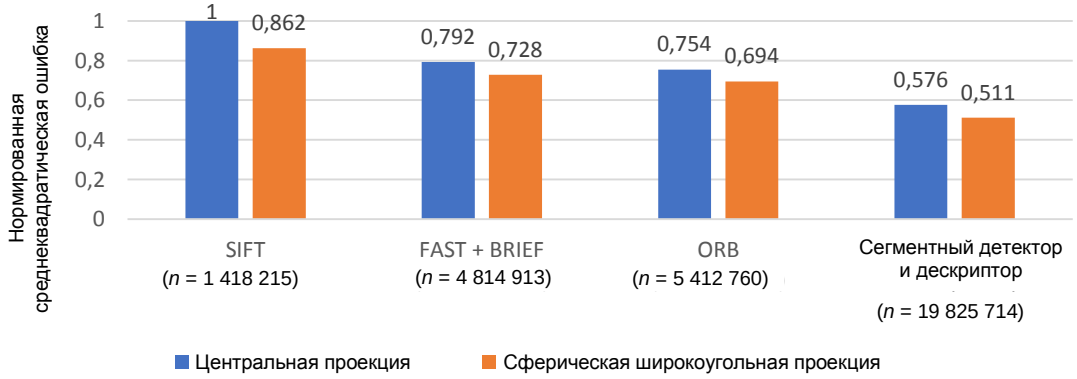


Рис. 3. Нормированное значение критерия (1) при использовании различных видов алгоритмов работы с локальными признаками

В качестве весов в оценке (1) использовались значения $w_1 = 1$, $w_2 = 0{,}8$, $w_3 = 0{,}5$. Эти значения весов выбраны исходя из того, что для итоговой модели положение и ориентация камеры не являются информативными, а их некорректное определение с большой вероятностью будет влиять на правильность определения положения точек, поэтому веса соответствующих ошибок могут быть ниже.

По полученным значениям ошибки обратной проекции видно, что сегментный алгоритм детектирования и описания ключевых точек обеспечивает значительно меньшую суммарную ошибку, чем популярные алгоритмы SIFT, детектор FAST с дескриптором BRIEF и дескриптор ORB. В частности, в сравнении с алгоритмом ORB по всем моделям снижение ошибки определения координат ключевых точек и параметров ориентирования камеры на видеоэндоскопических изображениях составляет 32,2 ± 9,4 % (95%-й доверительный интервал). Значительные отличия обусловливаются также тем фактом, что сегментные детектор и дескриптор были способны выделить и сопоставить намного большее количество точек на эндоскопических изображениях (n = 19 852 714) по сравнению с другими алгоритмами благодаря адаптивному подбору параметров.

Модель сферической широкоугольной проекции на исследуемых изображениях показывает лучший результат при использовании любого из дескрипторов, поскольку в ней может быть учтено значительно больше параметров самой системы съемки. Снижение ошибки определения координат ключевых точек и параметров ориентирования камеры по сравнению с центральной проекцией по всем исследованным моделям составляет 11,2 ± 2,8 % (95%-й доверительный интервал).

Заключение. Оценка результатов трехмерной реконструкции по видеопоследовательностям представляет собой сложную задачу, поскольку не существует универсального способа сопоставления полученной модели с исходными сценами. Сравнение отдельных измерений длины или площади объектов является эффективным способом оценки качества реконструкции, но во многих задачах, в том числе и при трехмерной реконструкции по результатам видеоэндоскопических обследований, определение пространственных характеристик снимаемой сцены крайне затруднено. Это обусловливает необходимость разработки альтернативных способов оценки точности трехмерной реконструкции. В качестве одного из таких способов в работе предложена возможность использования моделирующей среды. Рассмотрены особенности построения трехмерных виртуальных сред с применением среды моделирования Autodesk 3ds Max и движка визуализации Arnold, на основании которых спроектирована моделирующая среда для имитации процесса захвата первичных данных при проведении видеоэндоскопических обследований. Особое внимание уделено задаче генерации текстур высокого разрешения. Приведены основные подходы к процедурной генерации текстур по подобию. Для моделирующей среды выбран подход с использованием пространственно-периодических генеративно-состязательных моделей на основе сверточных нейронных сетей, рассмотрен процесс обучения сети для генерации изображения по подобию исходя из результатов видеоэндоскопических обследований.

На основании разработанной моделирующей среды предложен способ оценки корректности результатов трехмерной реконструкции и введен критерий оптимальности полученной модели путем сравнения координат ключевых точек и параметров внутреннего и внешнего ориентирования камер, полученных с помощью данных моделирующей среды, и соответствующих оценок в рамках трехмерной реконструкции по методу связок. Предложенный критерий использован для сравнения известной модели центральной проекции с обрезкой изображения для коррекции дисторсии и модели сферической широкоугольной проекции, а также для сравнения различных известных алгоритмов поиска и сопоставления локальных признаков с сегментным детектором и дескриптором. Показано, что в соответствии с предложенным критерием модель сферической широкоугольной проекции, сегментный детектор и дескриптор обеспечивают наименьшую ошибку определения координат ключевых точек и параметров ориентирования камеры при их использовании для трехмерной реконструкции по данным видеоэндоскопических систем.

Список использованных источников

1. Usefulness of the 3D virtual visualization surgical planning simulation and 3D model for endoscopic endonasal transsphenoidal surgery of pituitary adenoma: technical report and review of literature / A. Shinomiya [et al.] // Interdisciplinary Neurosurgery. – 2018. – Vol. 13. – P. 13–19. https://doi.org/10.1016/j.inat.2018.02.002

2. Gatys, L. A. Texture synthesis using convolutional neural networks / L. A. Gatys, A. S. Ecker, M. Bethge // Advances in Neural Information Processing Systems. – 2015. – Vol. 28. – P. 262–270.

3. Mamgain, P. Autodesk 3ds Max 2019: a Detailed Guide to Arnold Renderer / P. Mamgain. – Padexi Academic, 2018. – 192 p.

4. Simonyan, K. Very deep convolutional networks for large-scale image recognition / K. Simonyan, A. Zisserman // Intern. Conf. on Learning Representations 2014 (ICLR 2014), Banff, Canada, 14–16 Apr. 2014. – Banff, 2014. – P. 1–14.

5. Bergmann, U. Learning texture manifolds with the periodic spatial GAN / U. Bergmann, N. Jetchev, R. Vollgraf // Proc. of the 34th Intern. Conf. on Machine Learning, Sydney, Australia, 6–11 Aug. 2017. – Sydney, 2017. – Vol. 70. – P. 469–477.

6. Bundle adjustment in the large / S. Agarwal [et al.] // Proc. of the 11th European Conf. on Computer Vision (ECCV 2010), Heraklion, Greece, 5–11 Sept. 2010. – Heraklion, 2010. – P. 29–42.

7. Головатая, Е. А. Модель формирования изображений для трехмерной реконструкции сцен по данным видеоэндоскопических исследований / Е. А. Головатая, В. С. Садов // Вестн. Полоц. гос. ун-та. Сер. С. Фундам. науки. – 2019. – № 12. – С. 43–49.

8. Lowe, D. G. Distinctive image features from scale-invariant keypoints / D. G. Lowe // Intern. J. of Computer Vision. – 2004. – Vol. 60, no. 2. – P. 91–110.

9. Rosten, E. Machine learning for high-speed corner detection / E. Rosten, T. Drummond // Proc. of the 9th European Conf. on Computer Vision (ECCV 2006), Graz, Austria, 7–13 May 2006. – Graz, 2006. – P. 430–443.

10. BRIEF: binary robust independent elementary features / M. Calonder [et al.] // Proc. of the 11th European Conf. on Computer Vision (ECCV 2010), Heraklion, Greece, 5–11 Sept. 2010. – Heraklion, 2010. – P. 778–792.

11. ORB: an efficient alternative to SIFT or SURF / E. Rublee [et al.] // IEEE Intern. Conf. on Computer Vision (ICCV 2011), Barcelona, 6–13 Nov. 2011. – Barcelona, 2011. – P. 2564–2571.

12. Halavataya, K. Optimizing local feature description and matching for realtime video sequence object detection / K. Halavataya, V. Sadov // Open Semantic Technologies for Intelligent Systems : Research Papers Collection / BSUIR. – Minsk, 2019. – P. 269–272.

References

1. Shinomiya A., Shindo A., Kawanishi M., Miyake K., Nakamura T., ..., Tamiya T. Usefulness of the 3D virtual visualization surgical planning simulation and 3D model for endoscopic endonasal transsphenoidal surgery of pituitary adenoma: technical report and review of literature. *Interdisciplinary Neurosurgery*, 2018, vol. 13, pp. 13–19. https://doi.org/10.1016/j.inat.2018.02.002

2. Gatys L. A., Ecker A. S., Bethge M. Texture synthesis using convolutional neural networks. *Advances in Neural Information Processing Systems*, 2015, vol. 28, pp. 262–270.

3. Mamgain P. *Autodesk 3ds Max 2019: a Detailed Guide to Arnold Renderer*. Padexi Academic, 2018, 192 p.

4. Simonyan K., Zisserman A. Very deep convolutional networks for large-scale image recognition. *International Conference on Learning Representations 2014 (ICLR 2014), Banff, Canada, 14–16 April 2014*. Banff, 2014, pp. 1–14.

5. Bergmann U., Jetchev N., Vollgraf R. Learning texture manifolds with the periodic spatial GAN. *Proceedings of the 34th International Conference on Machine Learning, Sydney, Australia, 6–11 August 2017*. Sydney, 2017, vol. 70, pp. 469–477.

6. Agarwal S., Snavely N., Seitz S. M., Szelisk R. Bundle adjustment in the large. *Proceedings of the 11th European Conference on Computer Vision (ECCV 2010), Heraklion, Greece, 5–11 September 2010*. Heraklion, 2010, pp. 29–42.

7. Halavataya K. A., Sadau V. S. Model formirovaniya izobrazheniy dlya trekhmernoy rekonstrukcii scen po dannym videoendoscopicheskyh issledovanii [Image formation model for three-dimensional reconstruction of scenes according to video endoscopic studies]. Vestnik Polotskogo gosudarstvennogo universiteta. Ser. S.

Fundamental'nyye nauki [*Vestnik of Polotsk State University. Ser. C. Basic Sciences*], 2019, no. 12, pp. 43–49 (in Russian).

8. Lowe, D. G. Distinctive image features from scale-invariant keypoints. *International Journal of Computer Vision*, 2004, vol. 60, no. 2, pp. 91–110.

9. Rosten E., Drummond T. Machine learning for high-speed corner detection. *Proceedings of the 9th European Conference on Computer Vision (ECCV 2006), Graz, Austria, 7–13 May 2006*. Graz, 2006, pp. 430–443.

10. Calonder M., Lepetit V., Strecha Ch., Fua P. BRIEF: binary robust independent elementary features. *Proceedings of the 11th European Conference on Computer Vision (ECCV 2010), Heraklion, Greece, 5–11 September 2010*. Heraklion, 2010, pp. 778–792.

11. Rublee E., Rabaud V., Konolige K., Bradski G. ORB: an efficient alternative to SIFT or SURF. *IEEE International Conference on Computer Vision (ICCV 2011), Barcelona, 6–13 November 2011*. Barcelona, 2011, pp. 2564–2571.

12. Halavataya K., Sadov V. Optimizing local feature description and matching for realtime video sequence object detection. *Open Semantic Technologies for Intelligent Systems*. Minsk, 2019, pp. 269–272.

Информация об авторах

Чернявский Александр Федорович, академик Национальной академии наук Беларуси, доктор технических наук, профессор, заведующий научно-исследовательской лабораторией специализированных вычислительных систем, Научно-исследовательское учреждение «Институт прикладных физических проблем им. А. Н. Севченко» Белорусского государственного университета, Минск, Беларусь.
E-mail: CheryAF@bsu.by

Головатая Екатерина Александровна, аспирант, старший преподаватель кафедры интеллектуальных систем, факультет радиофизики и компьютерных технологий, Белорусский государственный университет, Минск, Беларусь.
E-mail: katerina-golovataya@yandex.ru

Садов Василий Сергеевич, кандидат технических наук, доцент, профессор кафедры интеллектуальных систем, факультет радиофизики и компьютерных технологий, Белорусский государственный университет, Минск, Беларусь.
E-mail: sadov@bsu.by

Information about the authors

Aleksandr F. Chernyavsky, Academician of the National Academy of Sciences of Belarus, Dr. Sci. (Eng.), Professor, Head of the Research Laboratory of Specialized Computing Systems, A. N. Sevchenko Institute of Applied Physical Problems of the Belarusian State University, Minsk, Belarus.
E-mail: CheryAF@bsu.by

Katsiaryna A. Halavataya, Postgraduate Student, Senior Lecturer, Department of Intelligent Systems, Faculty of Radiophysics and Computer Technologies, Belarusian State University, Minsk, Belarus.
E-mail: katerina-golovataya@yandex.ru

Vasili S. Sadau, Cand. Sci. (Eng.), Associate Professor, Professor of the Department of Intelligent Systems, Faculty of Radiophysics and Computer Technologies, Belarusian State University, Minsk, Belarus.
E-mail: sadov@bsu.by

ISSN 1816-0301 (Print)
ISSN 2617-6963 (Online)

УДК 001.891.573
https://doi.org/10.37661/1816-0301-2020-17-1-29-38

Поступила в редакцию 03.12.2019
Received 03.12.2019

Принята к публикации 16.01.2020
Accepted 16.01.2020

Анализ системы обслуживания с повторными вызовами, неоднородными приборами и марковским процессом поступления

Лю Мэй

Белорусский государственный университет, Минск, Беларусь
E-mail: liumei19910101@126.com

Аннотация. Анализируется многолинейная система массового обслуживания с повторными попытками и разнородными приборами. Запросы поступают в систему в соответствии с марковским процессом прибытия. Прибывающие первичные запросы и запросы, которые повторяют попытки попасть на обслуживание с орбиты, занимают свободный прибор с самой высокой скоростью обслуживания, если таковой имеется. В противном случае, если все приборы заняты, запросы переходят на орбиту бесконечной емкости, с которой осуществляют повторные попытки попасть на обслуживание. Общая интенсивность потока повторных попыток бесконечно возрастает с увеличением числа запросов на орбите. Время обслуживания запроса имеет экспоненциальное распределение с интенсивностью, зависящей от номера прибора. Поведение системы описывается многомерной цепью Маркова с непрерывным временем, которая принадлежит классу асимптотически квазитеплицевых цепей Маркова. Это позволяет вывести простое и прозрачное условие эргодичности и вычислить стационарное распределение вероятностей состояний цепи. Представленные численные результаты иллюстрируют динамику некоторых показателей эффективности системы и важность учета корреляции в процессе поступления запросов.

Ключевые слова: система массового обслуживания, разнородные приборы, марковский процесс прибытия, повторные вызовы, асимптотически квазитеплицевая цепь Маркова

Для цитирования. Мэй, Лю. Анализ системы обслуживания с повторными вызовами, неоднородными приборами и марковским процессом поступления / Лю Мэй // Информатика. – 2020. − Т. 17, № 1. – С. 29–38. https://doi.org/10.37661/1816-0301-2020-17-1-29-38

Analysis of retrial queue with heterogeneous servers and Markovian arrival process

Liu Mei

Belarusian State University, Minsk, Belarus
E-mail: liumei19910101@126.com

Abstract. Multi-server retrial queueing system with heterogeneous servers is analyzed. Requests arrive to the system according to the Markovian arrival process. Arriving primary requests and requests retrying from orbit occupy an available server with the highest service rate, if there is any available server. Otherwise, the requests move to the orbit having an infinite capacity. The total retrial rate infinitely increases when the number of requests in orbit increases. Service periods have exponential distribution. Behavior of the system is described by multi-dimensional continuous-time Markov chain which belongs to the class of asymptotically quasi-toeplitz Markov chains. This allows to derive simple and transparent ergodicity condition and compute the stationary probabilities distribution of chain states. Presented numerical results illustrate the dynamics of some system effectiveness indicators and the importance of considering of correlation in the requests arrival process.

Keywords: retrial queue, heterogeneous servers, markovian arrival process, retrials, asymptotically quasi-toeplitz Markov chain

For citation. Mei Liu. Analysis of retrial queue with heterogeneous servers and Markovian arrival process. *Informatics*, 2020, vol. 17, no. 1, pp. 29−38 (in Russian). https://doi.org/10.37661/1816-0301-2020-17-1-29-38

Введение. Теория систем массового обслуживания с повторными вызовами является важной частью теории очередей, которая учитывает влияние повторных попыток попасть на обслуживание. Пропускная способность системы ограничена, и некоторые запросы не могут быть приняты к обслуживанию сразу по прибытии из-за временной недоступности пропускной способности. В отличие от очередей с буферами, где такие запросы помещаются в буфер и затем выбираются для обслуживания в соответствии с некоторыми дисциплинами, и очередей с потерями, в которых запросы теряются, в системах с повторными попытками данные запросы перемещаются в некое виртуальное место, называемое орбитой, и пытаются получить доступ к прибору через случайные промежутки времени. Ввиду своей высокой практической значимости системы обслуживания с повторными вызовами привлекают большое внимание исследователей. Область применения теории очередей с повторными вызовами включает в себя различные телекоммуникационные системы с дисциплинами множественного доступа, базы данных, центры обработки вызовов и т. д. Современное состояние исследований в области систем обслуживания с повторными вызовами изложено в работах [1, 2].

Из-за неоднородного по состоянию поведения цепей Маркова, которые описывают поведение систем обслуживания с повторными вызовами, их анализ значительно более сложен, чем анализ очередей с буферами или потерями. Наибольшие трудности возникают при анализе многолинейных систем обслуживания с повторными вызовами даже в самых простых предположениях о процессах поступления, обслуживания и повторных попыток. Например, система $M/M/N$ с классической политикой повторных попыток исследована в книге [2]. Трудности существенно возрастают, если вводятся более реалистичные предположения о процессах прибытия и обслуживания. В работе [3] изучается система обслуживания с повторными вызовами типа $BMAP/PH/N$. Здесь $BMAP$ (англ. batch Markovian arrival process) обозначает групповой марковский процесс прибытия, представленный в статье [4] как потенциально полезный дескриптор коррелированных групповых потоков в современных телекоммуникационных сетях. Дополнительная информация о $BMAP$ и результаты исследования систем с таким потоком даны в [5, 6]. В настоящей статье предполагается, что процесс поступления – это марковский процесс прибытия MAP, который является частным случаем $BMAP$, когда не допускается групповое поступление. Аббревиатура PH (англ. phase type distribution) обозначает распределение фазового типа [7]. Этот класс распределений довольно широк и включает, в частности, экспоненциальное, эрланговское и коксовское распределения, а также их варианты.

При рассмотрении многолинейных систем обычно предполагается, что приборы однородны и произвольный незанятый прибор задействуется с равной вероятностью для обслуживания, когда приходит новый запрос. Гораздо меньше исследованы очереди с разнородными приборами, которые являются более интересными объектами для исследования. Часто возникают довольно нетривиальные проблемы оптимизации, связанные с назначением приборов прибывающим запросам в зависимости от соотношения средних скоростей обслуживания и затрат на их использование. Проблема оптимального распределения запросов между гетерогенными серверами с целью минимизации среднего числа запросов в обычной системе обслуживания (без учета повторных вызовов) рассматривалась в работах [8–14]. Было показано, что оптимальная стратегия принадлежит к классу монотонных стратегий, т. е. пороговых стратегий, которые используют медленный прибор только тогда, когда длина очереди превышает определенный порог. В статье [15] показано, что для систем с повторными вызовами и классической политикой повторных попыток пороговая стратегия также оптимальна, и предложен алгоритм, который позволяет построить оптимальные стратегии для широкого класса систем массового обслуживания. Аналогичный анализ приведен в [15] для случая постоянной (не зависящей от числа запросов на орбите) частоты повторных попыток.

Многолинейные системы с повторными вызовами, в которых серверы являются однородными, а вновь прибывающий запрос выбирает произвольный незанятый прибор с равной вероятностью и обращается к какому-то конкретному прибору, рассматривались, например, в работах [16, 17].

В настоящей статье анализируется многолинейная система с повторными попытками типа $MAP/\hat{M}_N/N$. Символы $\hat{M}_N$ означают, что распределение времени обслуживания является экспоненциальным с различной скоростью на разных приборах. Предполагается, что приборы пронумерованы в порядке уменьшения скорости обслуживания, т. е. прибор с номером 1 самый быстрый, а прибор с номером N – самый медленный. Согласно известным результатам о структуре оптимального управления (см., например, [15]) лицо, принимающее решение, имеет возможность наблюдать за количеством запросов на орбите и активирует новый, более медленный сервер, если это число превышает определенный порог. Предположим следующее: а) число запросов на орбите не наблюдается, что имеет место в большинстве реальных систем, потому что орбита – это виртуальное место и в действительности ожидающие запросы расположены в некоторой, возможно очень широкой, области; б) дисциплина обслуживания является консервативной. Это означает, что если запрос с орбиты делает попытку попасть на обслуживание и не все приборы заняты, то такой запрос будет принят к обслуживанию. Проблема выбора конкретного прибора из множества доступных в данный момент приборов довольно сложная. Ее решению должно предшествовать формулирование некоторого экономического критерия, включающего, например, затраты на ожидание запросов на орбите (время пребывания в системе) и затраты на использование доступных приборов в единицу времени. В рамках данной статьи экономические аспекты не учитываются (это планируется сделать в дальнейших исследованиях), а изучается следующая дисциплина выбора прибора: в первую очередь задействуется самый быстрый из свободных приборов. Смена прибора в процессе обслуживания любого запроса не допускается.

Описание модели. Рассматривается система массового обслуживания с N приборами. Первичные запросы приходят в систему в соответствии с MAP. Поступление запросов в MAP-потоке происходит под управлением неприводимой цепи Маркова ν_t, $t \ge 0$, с непрерывным временем и конечным пространством состояний $\{0,1,\ldots,W\}$. Поведение MAP-потока полностью характеризуется квадратными матрицами (D_0, D_1) порядка $\overline{W} = W + 1$. При этом матрица $D(1) = D_0 + D_1$ является инфинитезимальным генератором цепи Маркова ν_t. Интенсивность λ поступления запросов в MAP определяется как $\lambda = \boldsymbol{\theta} D_1 \mathbf{e}$, где $\boldsymbol{\theta}$ – вектор-строка стационарного распределения цепи Маркова ν_t, $t \ge 0$. Вектор $\boldsymbol{\theta}$ будет единственным решением системы линейных алгебраических уравнений $\boldsymbol{\theta} D(1) = \mathbf{0}$, $\boldsymbol{\theta}\mathbf{e} = 1$. Коэффициент c_{var} вариации интервалов между прибытием клиентов определяется как $c_{var} = 2\lambda\boldsymbol{\theta}(-D_0)^{-1}\mathbf{e} - 1$, коэффициент корреляции c_{cor} последовательных интервалов между прибытиями – как $c_{cor} = (\lambda\boldsymbol{\theta}(-D_0)^{-1} D_1 (-D_0)^{-1}\mathbf{e} - 1)/c_{var}^2$.

Распределение времени обслуживания предполагается экспоненциальным. Приборы имеют разные скорости обслуживания: $\mu_1, \mu_2, \ldots, \mu_N$.

Предположение 1. Серверы нумеруются таким образом, что выполняются неравенства $\mu_1 > \mu_2 > \ldots > \mu_N$. В будущем полученные результаты могут быть использованы для решения проблемы оптимальной нумерации серверов с учетом не только скоростей работы приборов, но и затрат на их использование.

Если входящий запрос застает все приборы незанятыми, он обслуживается на первом приборе. Если первый прибор занят, то запрос ищет незанятый сервер с минимальным номером. Найдя такой прибор, запрос начинает обслуживание на нем. Если же все приборы заняты, то запрос уходит на орбиту. Число мест на орбите (емкость орбиты) не ограничено. Запросы генерируют повторные попытки попасть на обслуживание до тех пор, пока их не обслужат. Предположительно, общий поток повторных попыток таков, что вероятность генерации повторной

попытки в интервале $(t, t+\Delta t)$ равна $\alpha_i \Delta t + o(\Delta t)$, когда количество запросов на орбите равно i, $i > 0$, $\alpha_0 = 0$. Явная зависимость интенсивностей α_i от i не фиксируется. Предполагается, что интенсивность потока повторных попыток возрастает неограниченно: $\lim\limits_{i\to\infty} \alpha_i = \infty$. Это справедливо, в частности, для классической стратегии повторов, где $\alpha_i = i\alpha$, и линейной стратегии, где $\alpha_i = i\alpha + \gamma$.

Целью работы является получение условия существования стационарного распределения вероятностей состояния системы, нахождение этого распределения и краткий анализ проблемы оптимизации работы системы.

Процесс состояний системы. Введем следующие обозначения:

i_t – количество запросов на орбите, $i_t \geq 0$;

$\xi_t^{(n)}$ – состояние n-го прибора, $n = \overline{1, N}$:

$$\xi_t^{(n)} = \begin{cases} 0, & \text{если } n\text{-й прибор свободен,} \\ 1, & \text{если } n\text{-й прибор занят;} \end{cases}$$

ν_t – состояние управляющего процесса MAP, $\nu_t = \overline{0, W}$,

в произвольный момент времени t, $t > 0$.

Рассмотрим многомерный стохастический процесс с непрерывным временем:

$$\zeta_t = \{i_t, \xi_t^{(1)}, \ldots, \xi_t^{(N)}, \nu_t\}, \ t \geq 0.$$

Видно, что данный процесс является неприводимой цепью Маркова. Предположим, что существуют стационарные вероятности этой цепи Маркова:

$$\pi(i, r^{(1)}, \ldots, r^{(N)}, \nu) = \lim_{t\to\infty} P\{i_t = i, \xi_t^{(1)} = r^{(1)}, \ldots, \xi_t^{(N)} = r^{(N)}, \nu_t = \nu\}, \ i \geq 0, \ r^{(n)} = \overline{0,1}, \ n = \overline{0, N}, \ \nu = \overline{0, W}.$$

Условие существования стационарных вероятностей будет приведено ниже.

Пронумеровав состояния цепи Маркова $\zeta_t, t \geq 0$, в лексикографическом порядке, сформируем вектор-строку

$$\boldsymbol{\pi}(i, r^{(1)}, \ldots, r^{(N)}) = (\pi(i, r^{(1)}, \ldots, r^{(N)}, 0), \ldots, \pi(i, r^{(1)}, \ldots, r^{(N)}, W))$$

стационарных вероятностей $\pi(i, r^{(1)}, \ldots, r^{(N)}, \nu)$ и вектор-строку $\boldsymbol{\pi}_i$, состоящую из векторов $\boldsymbol{\pi}(i, r^{(1)}, \ldots, r^{(N)}), i \geq 0$. Отметим, что размер векторов $\boldsymbol{\pi}_i$ рассчитывается как $K = (W+1)2^N$. Определим также бесконечномерный вектор вероятностей $\boldsymbol{\pi} = (\boldsymbol{\pi}_0, \boldsymbol{\pi}_1, \boldsymbol{\pi}_2, \ldots)$.

Дополнительно введем следующие обозначения:

I – тождественная матрица соответствующего размера (при необходимости размер определяется нижним индексом);

O_n – нулевая матрица размера n;

$\otimes$ и $\oplus$ – символы Кронекерова произведения и суммы матриц, $S^{\otimes l} = \underbrace{S \otimes \cdots \otimes S}_{l}$, $l \geq 1$;

J – квадратная матрица размера 2^N, определяемая как $J = \mathrm{diag}\{0, \ldots, 0, 1\}$;

$\mathrm{diag}\{\ldots\}$ – диагональная матрица с диагональными элементами, указанными в скобках;

$\bar{I} = (I - J) \otimes I_{\bar{W}}$;

E^0 – матрица размера 2^N со всеми нулевыми элементами, кроме элементов $\left(E^0\right)_{r,r} = -\sum\limits_{k=1}^{N} n_k \mu_k$ для $r = \sum\limits_{k=1}^{N} n_k 2^{N-k}$;

E^- – матрица размера 2^N со всеми нулевыми элементами, кроме элементов $\left(E^-\right)_{r,r'} = \mu_l$ для $r = \sum_{k=1}^{N} n_k 2^{N-k}$, $r' = \sum_{k=1,k\neq l}^{N} n_k 2^{N-k}$, $l = \arg\{n_l = 1\}$;

E^+ – матрица размера 2^N со всеми нулевыми элементами, кроме элементов $\left(E^+\right)_{r,r'} = 1$ для $r = \sum_{k=1}^{q-1} 2^{N-k} + \sum_{k=q+1}^{N} n_k 2^{N-k}$, $r' = \sum_{k=1}^{q} n_k 2^{N-k} + \sum_{k=q+1}^{N} n_k 2^{N-k}$, $q = \arg\min_q \left\{n_q = 0\right\}$;

$\tilde{I} = E^+ \otimes I_{\bar{w}}$.

Лемма. Если существует вектор $\boldsymbol{\pi}$ стационарных вероятностей цепи Маркова ζ_t, $t \geq 0$, то он удовлетворяет уравнению равновесия

$$\boldsymbol{\pi}\mathbf{Q} = \mathbf{0},$$

где $\mathbf{0}$ – бесконечная вектор-строка, состоящая из нулей, а матрица $\mathbf{Q}$, которая является генератором цепи ζ_t, $t \geq 0$, имеет следующую структуру:

$$\mathbf{Q} = \begin{pmatrix} \mathbf{Q}_{00} & \mathbf{Q}_{01} & 0 & 0 & \cdots \\ \mathbf{Q}_{10} & \mathbf{Q}_{11} & \mathbf{Q}_{12} & 0 & \cdots \\ 0 & \mathbf{Q}_{21} & \mathbf{Q}_{22} & \mathbf{Q}_{23} & \cdots \\ 0 & 0 & \mathbf{Q}_{32} & \mathbf{Q}_{33} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}. \quad (1)$$

Блоки $\mathbf{Q}_{ij}$, $i,\ j \geq 0,\ j = \left\{\max\{0, i-1\}, i, i+1\right\}$, матрицы $\mathbf{Q}$ имеют размер K и определяются следующим образом:

$$\mathbf{Q}_{i,i+1} = J \otimes D_1,\ \mathbf{Q}_{i,i-1} = \alpha_i \tilde{I}, \mathbf{Q}_{i,i} = \mathbf{Q}_{ii}{}^0 + \mathbf{Q}_{ii}{}^- + \mathbf{Q}_{ii}{}^+,$$

где $\mathbf{Q}_{ii}{}^0 = I_{2^N} \otimes D_0 + E^0 \otimes I_{\bar{w}} - \alpha_i \bar{I}, \mathbf{Q}_{ii}{}^- = E^- \otimes I_{\bar{w}}, \mathbf{Q}_{ii}{}^+ = E^+ \otimes D_1$.

Доказательство. Пронумеруем все возможные комбинации состояний $(r^{(1)}, \ldots, r^{(N)})$ таким образом, чтобы комбинация $\{n_1, n_2, \ldots, n_N\}$, $n_k = 0,1$, $k = \overline{1,N}$, имела порядковый номер $\sum_{k=1}^{N} n_k 2^{N-k}$.

Матрица E^0 является диагональной, и ее диагональные элементы $\left(E^0\right)_{r,r}$, взятые с противоположным знаком, задают интенсивности выхода цепи Маркова из состояния $(i, n_1, \ldots, n_N, \nu)$. Такой выход возможен за счет окончания обслуживания на одном из приборов, интенсивность выхода равна $\sum_{k=1}^{N} n_k \mu_k$.

Матрица E^- задает интенсивности переходов цепи Маркова, когда один из занятых приборов заканчивает обслуживание. При этом учитываются изменения номера комбинации из-за изменения соответствующего ненулевого значения компоненты n_l на нулевое значение. Интенсивность такого перехода равна μ_l.

Матрица E^+ задает вероятности переходов цепи Маркова, когда первый свободный прибор начинает обслуживание. При этом учитывается изменение номера комбинации из-за замены соответствующего нулевого значения компоненты n_q на ненулевое значение.

Таким образом, справедливость леммы подтверждена.

Следствие. *Марковская цепь* ζ_t *принадлежит классу асимптотически квазитеплицевых цепей Маркова.*

Доказательство. Согласно определению асимптотически квазитеплицевых цепей Маркова, приведенному в работе [18], необходимо доказать существование пределов

$$Y_0 = \lim_{i\to\infty} R_i^{-1}\mathbf{Q}_{i,i-1},\ Y_2 = \lim_{i\to\infty} R_i^{-1}\mathbf{Q}_{i,i+1},\ Y_1 = \lim_{i\to\infty} R_i^{-1}\mathbf{Q}_{ii} + I,$$

где R_i – диагональная матрица с диагональными элементами, определенными как модули соответствующих диагональных элементов матрицы $\mathbf{Q}_{ii}$, $i \ge 0$. Легко проверить, что R_i является матрицей с диагональными блоками $T_i^{(n)}$, $n = \overline{0,N}$:

$$T_i^{(n)} = \begin{cases} \Lambda \oplus Z_n + \alpha_i I_{\bar{W}\cdot 2^{N-n-1}},\ n = \overline{0,N-1}; \\ \Lambda + \sum_{k=1}^{N} \mu_k I_{\bar{W}},\ n = N, \end{cases}$$

где Λ, Z_n – диагональные матрицы с диагональными элементами, определяемыми диагональными элементами матриц $-D_0, \Delta_{N-n-1}, n = \overline{0,N}$.

С помощью прямых расчетов можно убедиться в справедливости следующих формул:

$$Y_0 = \tilde{I}_\beta, Y_1 = \begin{pmatrix} O & O & \cdots & O & O \\ O & O & \cdots & O & O \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ O & O & \cdots & O & O \\ \Gamma_1 & \Gamma_2 & \cdots & \Gamma_N & \Psi \end{pmatrix},\ Y_2 = \begin{pmatrix} O & O & \cdots & O & O \\ O & O & \cdots & O & O \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ O & O & \cdots & O & O \\ O & O & \cdots & O & \Phi \end{pmatrix},$$

где

$$\Gamma_n = \mu_n \mathbf{b_1}^{\otimes(N-n)} \otimes C,\ n = \overline{1,N},\ C = (\Lambda + \sum_{k=1}^{N} \mu_k I_{\bar{W}})^{-1};$$

$$\Psi = C(D_0 - \sum_{k=1}^{N} \mu_k I_{\bar{W}}) + I,\ \Phi = CD_1.$$

Следствие доказано.

Условие эргодичности и условие неэргодичности цепи.

Теорема. *Цепь Маркова* ζ_t *эргодична, если выполняется неравенство*

$$\lambda < \sum_{k=1}^{N} \mu_k, \tag{2}$$

и неэргодична, если выполняется неравенство

$$\lambda > \sum_{k=1}^{N} \mu_k, \tag{3}$$

где λ *– фундаментальная скорость MAP.*

Доказательство теоремы следует из работы [18] с учетом полученного вида матриц Y_0, Y_1, Y_2. Условие эргодичности (2) интуитивно понятно. Обычно условие эргодичности состоит в том, что в перегруженной системе скорость поступления запросов меньше, чем скорость обслуживания. В рассматриваемой модели, когда она перегружена, т. е. на орбите находится очень много запросов, все приборы непрерывно заняты. Таким образом, общая скорость обслуживания равна $\sum_{k=1}^{N} \mu_k$.

В дальнейшем будем считать, что условие (2) выполнено. Тогда существуют векторы стационарных вероятностей $\boldsymbol{\pi}_i$, $i \geq 0$, определенные выше. Они удовлетворяют системе уравнений равновесия $\boldsymbol{\pi}\mathbf{Q} = \mathbf{0}$ и условию нормировки $\boldsymbol{\pi}\mathbf{e} = 1$. Эта система бесконечна, и ее решение довольно сложное. Система может быть решена с использованием алгоритма, разработанного в [18], и более эффективного алгоритма, предложенного в [19].

Показатели эффективности работы системы. Среднее количество запросов на орбите вычисляется как

$$L_{orbit} = \sum_{i=1}^{\infty} i\boldsymbol{\pi}_i\mathbf{e}.$$

Вероятность того, что n-й прибор в произвольный момент занят, рассчитывается по формуле

$$P_{busy}^{(n)} = \sum_{i=0}^{\infty} \sum_{(r^{(1)},\ldots,r^{(N)})\in\mathcal{R},\, r^{(n)}=1} \boldsymbol{\pi}(i,\, r^{(1)},\, \ldots,\, r^{(N)})\mathbf{e},\ n = \overline{1, N}.$$

Предположим, что функционал качества работы системы, задающий ее средние расходы в единицу времени, определяется как

$$E = aL_{orbit} + \sum_{n=1}^{N} c_n P_{busy}^{(n)},$$

где a – штраф за единицу времени ожидания одного запроса на орбите, c_n – штраф за единицу времени использования n-го прибора.

Предположение 2. В дополнение к сделанному выше (без ограничения общности) предположению 1, что приборы перенумерованы в таком порядке, что интенсивности обслуживания удовлетворяют неравенствам $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_N$, предположим выполнение и соотношения $\frac{c_1}{\mu_1} \leq \frac{c_2}{\mu_2} \leq \cdots \leq \frac{c_N}{\mu_N}$. Предположение 2 выглядит обоснованным в практических ситуациях, поскольку оно означает, что более быстрый сервер имеет также меньшую стоимость эксплуатации на единицу скорости обслуживания. При выполнении предположения 2 численные эксперименты подтверждают справедливость следующего правила.

Правило c/μ: прибор с меньшим значением отношения c/μ должен иметь меньший номер, т. е. более высокий приоритет на обслуживание поступающего запроса.

Численные результаты. Чтобы проиллюстрировать результаты выполнения алгоритмов расчета стационарных вероятностей и показателей эффективности, а также показать влияние корреляции на характеристики системы в процессе поступления, рассмотрим кратко следующий пример.

Пусть изначально входящий поток *MAP* характеризуется матрицами

$$D_0 = \begin{pmatrix} -1,35164 & 0 \\ 0 & -0,04387 \end{pmatrix},\ D_1 = \begin{pmatrix} 1,34265 & 0,00899 \\ 0,02443 & 0,01944 \end{pmatrix}$$

и имеет интенсивность $\lambda = 1$. В дальнейшем интенсивность потока будет варьироваться путем умножения матриц D_0 и D_1 на соответствующую константу.

Процесс поступления имеет коэффициент корреляции длин двух последовательных интервалов между поступлениями запросов $c_{cor} = 0,2$ и коэффициент вариации длин интервалов между прибытиями запросов $c_{var} = 13,4$.

Представим также результаты расчета для модели, в которой поток прихода запросов определяется как стационарный пуассоновский процесс с той же интенсивностью поступления.

Предположим, что общее количество серверов $N = 3$, а скорости обслуживания на приборах $\mu_1 = 4,\ \mu_2 = 3$ и $\mu_3 = 1$ соответственно. Интенсивности выполнения повторных попыток определяются как $\alpha_0 = 0,\ \alpha_i = i\alpha,\ \alpha = 1,\ i > 0$. Штраф за единицу времени ожидания одного запроса на орбите $a = 7$, штрафы за единицу времени использования приборов соответственно $c_1 = 10,\ c_2 = 8,\ c_3 = 5$. При этом $\frac{c_1}{\mu_1} = 2,5,\ \frac{c_2}{\mu_2} = 2,67,\ \frac{c_3}{\mu_3} = 5.$

В табл. 1 комбинация (1, 2, 3) дает минимальное значение критерия *E* при любом значении λ. С ростом величины λ значения критерия *E* при различных комбинациях нумерации приборов сближаются, поскольку возрастает вероятность того, что все приборы заняты и возможность их выбора исчезает.

Таблица 1

Значения критерия *E* при различных комбинациях нумерации приборов и различных значениях λ

Комбинация	$\lambda = 1$	$\lambda = 2$	$\lambda = 3$	$\lambda = 4$	$\lambda = 5$	$\lambda = 6$	$\lambda = 7$
(1, 2, 3)	2,69	6,42	12,90	26,07	57,22	141,55	425,88
(1, 3, 2)	3,02	7,10	13,88	27,32	58,69	143,17	427,62
(2, 3, 1)	3,22	7,52	14,62	28,54	60,52	145,55	430,60
(2, 1, 3)	2,79	6,63	13,30	26,78	58,33	143,03	427,76
(3, 1, 2)	3,74	7,85	14,75	28,47	60,23	145,07	429,92
(3, 2, 1)	3,81	8,07	15,20	29,24	61,40	146,61	431,85

В табл. 2 приведены значения критерия E с M стационарным пуассоновским процессом поступления запросов при различных комбинациях нумерации приборов и различных значениях λ. Пусть здесь изначально M – это входящий поток, характеризующийся матрицами $D_0 = -\lambda$ и $D_1 = \lambda$.

Таблица 2

Значения критерия E с M стационарным пуассоновским процессом поступления запросов

Комбинация	$\lambda = 1$	$\lambda = 2$	$\lambda = 3$	$\lambda = 4$	$\lambda = 5$	$\lambda = 6$	$\lambda = 7$
(1, 2, 3)	2,62	5,79	10,27	17,40	30,15	57,22	141,38
(1, 3, 2)	2,92	6,49	11,29	18,72	31,77	59,13	143,57
(2, 3, 1)	3,13	6,89	11,94	19,73	33,31	61,47	147,27
(2, 1, 3)	2,73	6,00	10,61	17,95	31,04	58,63	143,72
(3, 1, 2)	3,83	7,44	12,27	19,82	33,13	60,96	146,24
(3, 2, 1)	3,90	7,63	12,63	20,44	34,12	62,48	148,65

Согласно данным табл. 3 и 4 при невыполнении предположения 2 правило c/μ может перестать действовать. Жирным шрифтом выделены минимальные значения критерия *E*.

Таблица 3

Значения критерия *E* при различных комбинациях нумерации приборов и штрафах за единицу времени использования первого прибора при $\lambda = 1$

Комбинация	$c_1 = 10{,}8,\ c_2 = 8,\ c_3 = 5$	$c_1 = 10{,}9,\ c_2 = 8,\ c_3 = 5$	$c_1 = 11,\ c_2 = 8,\ c_3 = 5$
(1, 2, 3)	**2,838**	2,857	2,876
(1, 3, 2)	3,172	3,191	3,210
(2, 3, 1)	3,242	3,244	3,247
(2, 1, 3)	2,845	**2,851**	**2,858**
(3, 1, 2)	3,826	3,838	3,849
(3, 2, 1)	3,838	3,841	3,845

Таблица 4

Значения критерия E при различных комбинациях нумерации приборов и штрафах за единицу времени использования второго прибора при $\lambda = 1$

Комбинация	$c_1 = 10,\ c_2 = 15{,}5,\ c_3 = 5$	$c_1 = 10,\ c_2 = 15{,}6,\ c_3 = 5$	$c_1 = 10,\ c_2 = 16,\ c_3 = 5$
(1, 2, 3)	**3,200**	3,207	3,235
(1, 3, 2)	3,201	**3,203**	**3,213**
(2, 3, 1)	4,974	4,997	5,091
(2, 1, 3)	4,537	4,560	4,653
(3, 1, 2)	4,001	4,014	4,028
(3, 2, 1)	4,882	4,897	4,954

Заключение. В статье проанализирована система обслуживания с повторными вызовами, разнородными приборами и *MAP*-процессом поступления запросов. Полученные результаты могут найти применение при решении различных задач оптимизации, связанных, в частности, с порядком использования имеющихся обслуживающих приборов, а также в случае фазового распределения времен обслуживания запросов на приборах системы и в случае системы с ненадежными приборами.

References

1. Artalejo J. R., Gomez-Corral A. *Retrial Queueing Systems: a Computational Approach*. Springer, Berlin – Heidelberg, 2008, 318 p.
2. Falin G. I., Templeton J. G. C. *Retrial Queues*. Chapman & Hall, London, 1997, 328 p.
3. Breuer L., Dudin A. N., Klimenok V. I. A retrial $BMAP/PN/N$ system. *Queueing Systems*, 2002, vol. 40, pp. 433–457.
4. Lucantoni D. New results on the single server queue with a batch Markovian arrival process. *Communication in Statistics-Stochastic Models*, 1991, vol. 7, pp. 1–46.
5. Chakravarthy S. R. The batch Markovian arrival process: a review and future work. In Krishnamoorthy A., Raju N., Ramaswami V. (eds.). *Advances in Probability Theory and Stochastic Processes*, Notable Publications Inc., New Jersey, 2001, pp. 21–29.
6. Vishnevskii V. M., Dudin A. N. Queueing systems with correlated arrival flows and their applications to modeling telecommunication networks. *Automation and Remote Control*, 2017, vol. 78, pp. 1361–1403.
7. Neuts M. *Matrix-Geometric Solutions in Stochastic Models*. The Johns Hopkins University Press, Baltimore, 1981, 352 p.
8. Efrosinin D. V. *Controlled Queueing Systems with Heterogeneous Servers.* Trier University, Germany, 2004, 229 p.
9. Lin W., Kumar P. R. Optimal control of a queueing system with two heterogeneous servers. *IEEE Transactions on Automatic Control*, 1984, vol. 29, pp. 696–703.
10. Luh H. P., Viniotis I. *Optimality of Threshold Policies for Heterogeneous Server Systems*. Raleign, North Carolina State University, 1990.
11. Nobel R., Tijms H. C. Optimal control of a queueing system with heterogeneous servers. *IEEE Transactions on Automatic Control*, 2000, vol. 45, no. 4, pp. 780–784.
12. Rosberg Z., Makowski A. M. Optimal routing to parallel heterogeneous servers-small arrival rates. *Transactions on Automatic Control*, 1990, vol. 35, no. 7, pp. 789–796.
13. Rykov V. V. Monotone control of queueing systems with heterogeneous servers. *Queueing Systems*, 2001, vol. 37, pp. 391–403.
14. Rykov V. V., Efrosinin D. V. Numerical analysis of optimal control polices for queueing systems with heterogeneous servers. *Information Processes*, 2002, vol. 2, no. 2, pp. 252–256.
15. Efrosinin D., Breuer L. Threshold policies for controlled retrial queues with heterogeneous servers. *Annals of Operations Research*, 2006, vol. 41, no. 1, pp. 139–162.
16. Falin G. Stability of the multiserver queue with addressed retrials. *Annals of Operations Research*, 2012, vol. 196, no. 1, pp. 241–246.
17. Mushko V. V. Multiserver queue with addressed retrials. *Annals of Operations Research*, 2006, vol. 141, pp. 283–301.
18. Klimenok V., Dudin A. Multi-dimensional asymptotically quasi-Toeplitz Markov chains and their application in queueing theory. *Queueing Systems*, 2006, vol. 54, no. 4, pp. 245–259.

19. Dudin S., Dudina O. Retrial multi-server queueing system with PHF service time distribution as a model of a channel with unreliable transmission of information. *Applied Mathematical Modelling*, 2019, vol. 65, pp. 676–695.

Информация об авторе

Лю Мэй, аспирантка кафедры теории вероятностей и математической статистики факультета прикладной математики и информатики, Белорусский государственный университет, Минск, Беларусь.
E-mail: liumei19910101@126.com

Information about the author

Liu Mei, Postgraduate Student of Department of Probability Theory and Mathematical Statistics of Faculty of Applied Mathematics and Computer Science, Belarusian State University, Minsk, Belarus.
E-mail: liumei19910101@126.com

ISSN 1816-0301 (Print)
ISSN 2617-6963 (Online)

УДК 517.5
https://doi.org/10.37661/1816-0301-2020-17-1-39-46

Поступила в редакцию 01.07.2019
Received 01.07.2019

Принята к публикации 23.10.2019
Accepted 23.10.2019

Локальные преобразования с сингулярным вейвлетом

В. М. Романчак

Белорусский национальный технический университет, Минск, Беларусь
E-mail: Romanchak@bntu.by

Аннотация. Рассматривается локальное вейвлет-преобразование с сингулярным базисным вейвлетом. С помощью последовательности локальных вейвлет-преобразований решается задача непараметрической аппроксимации функции. Традиционно считается, что вейвлет должен иметь среднее значение, равное нулю. Ранее автором рассматривались сингулярные вейвлеты, для которых среднее значение не равно нулю. Например, в качестве вейвлета использовались дельтообразные функции, которые участвуют в оценках Парзена – Розенблатта и Надарая – Ватсона. Для сингулярных вейвлетов была построена последовательность вейвлет-преобразований для всей числовой оси и конечного интервала.
В работе предлагается последовательность локальных вейвлет-преобразований, дается определение локального вейвлет-преобразования и доказываются теоремы, которые формулируют его свойства. Для подтверждения эффективности алгоритма приводится пример аппроксимации функции с помощью суммы дискретных локальных вейвлет-преобразований.

Ключевые слова: вейвлет-преобразование, сингулярный вейвлет, окно Парзена − Розенблатта, непараметрическая аппроксимация, ядерная оценка Надарая – Ватсона

Для цитирования. Романчак, В. М. Локальные преобразования с сингулярным вейвлетом / В. М. Романчак // Информатика. – 2020. − Т. 17, № 1. – С. 39–46. https://doi.org/10.37661/1816-0301-2020-17-1-39-46

Local transformations with a singular wavelet

Vasily M. Romanchak

Belarusian National Technical University, Minsk, Belarus
E-mail: Romanchak@bntu.by

Abstract. The paper considers a local wavelet transform with a singular basis wavelet. The problem of nonparametric approximation of a function is solved by the use of the sequence of local wavelet transforms. Traditionally believed that the wavelet should have an average equal to zero. Earlier, the author considered singular wavelets when the average value is not equal to zero. As an example, the delta-shaped functions, participated in the estimates of Parzen – Rosenblatt and Nadara – Watson, were used as a wavelet. Previously, a sequence of wavelet transforms for the entire numerical axis and finite interval was constructed for singular wavelets.
The paper proposes a sequence of local wavelet transforms, a local wavelet transform is defined, the theorems that formulate the properties of a local wavelet transform are proved. To confirm the effectiveness of the algorithm an example of approximating the function by use of the sum of discrete local wavelet transforms is given.

Keywords: wavelet transform, singular wavelets, the Parzen – Rosenblatt window method, nonparametric estimator, Nadaraya − Watson kernel regression

For citation. Romanchak V. M. Local transformations with a singular wavelet. *Informatics*, 2020, vol. 17, no. 1, pp. 39−46 (in Russian). https://doi.org/10.37661/1816-0301-2020-17-1-39-46

Введение. С целью обоснования методов непараметрической аппроксимации строят различные математические модели. Для этого в прикладных работах рассматриваются ядерные оценки [1−4] и теория вейвлетов [4−6]. Вейвлет-преобразования с сингулярным вейвлетом расширяют возможности теории вейвлетов и ядерных оценок типа Надарая – Ватсона [7−10]. Вейвлет-преобразования можно применять для построения рекуррентной последовательности с целью аппроксимации функции. В настоящей работе для этого рассматривается локальное интегральное вейвлет-преобразование с сингулярным вейвлетом.

Обозначим $\psi(t)$ базисный вейвлет [6]. В вейвлете варьируются значения параметра масштабирования a и параметра сдвига b:

$$\frac{1}{a}\psi\left(\frac{t-b}{a}\right). \tag{1}$$

Пусть для вейвлета $\psi(t)$ выполняется условие на бесконечности

$$\left|\psi(t)\right| \le \frac{q}{1+t^2}, \tag{2}$$

где q, $q > 0$, – некоторая константа, и для функции $\psi(t)$ существует конечное среднее значение

$$C_\psi = \int_{-\infty}^{\infty} \psi(t)\,dt, \ \left|C_\psi\right| < \infty. \tag{3}$$

Из условий (2) и (3) следует, что $\psi(t) \in L^1(R)$. Обычно считается, что базисный вейвлет должен иметь среднее значение, равное нулю: $C_\psi = 0$. Чтобы определить локальное вейвлет-преобразование, понадобятся вейвлеты со средним значением, не равным нулю, – сингулярные вейвлеты [7].

Регуляризованное вейвлет-преобразование для бесконечного промежутка определяется формулой [9]

$$W(f - f(b))(b,a) = \frac{1}{a}\int_{-\infty}^{\infty}(f(t) - f(b))\psi\left(\frac{t-b}{a}\right)dt, \tag{4}$$

где $b \in R$. В качестве вейвлета в преобразовании (4) можно взять дельтообразные функции [2]. Например, вейвлетом может быть функция плотности стандартного нормального распределения. Если для вейвлета $\psi(t)$ среднее значение $C_\psi = 0$, то регуляризованное вейвлет-преобразование (4) совпадает с вейвлет-преобразованием

$$W(f)(b,a) = \frac{1}{a}\int_{-\infty}^{\infty} f(t)\psi\left(\frac{t-b}{a}\right)dt. \tag{5}$$

В работе [10] рассматривается вейвлет-преобразование с сингулярным вейвлетом на конечном интервале

$$Wf(b,a) = \frac{1}{aC(b,a)}\int_A^B f(t)\psi\left(\frac{t-b}{a}\right)dt$$

и регуляризованное вейвлет-преобразование

$$W(f - f(b))(b,a) = \frac{1}{aC(b,a)}\int_A^B (f(t) - f(b))\psi\left(\frac{t-b}{a}\right)dt,$$

где $b \in [A, B]$, $C(b, a) \neq 0$, $0 < a < a_0$, $\psi(t)$ − сингулярный вейвлет.

Целью настоящей работы является обоснование алгоритма локальной аппроксимации. Показано, что локальное вейвлет-преобразование может применяться в методе сингулярных вейвлетов. Это позволяет локально аппроксимировать функцию, заданную на бесконечном или конечном интервале.

Локальное вейвлет-преобразование. Будем считать, что вейвлет $\psi(t)$ удовлетворяет условиям на бесконечности (2) и имеет ненулевое среднее. Следовательно, $\psi(t) \in L^1(R)$.

Для определенности считаем, что постоянная $C_\psi > 0$. Пусть функция $f(t)$ принадлежит пространству L^1. Локальное вейвлет-преобразование зададим формулой

$$Wf(b,a) = \frac{1}{aC_M} \int_{b-aM}^{b+aM} f(t)\psi\left(\frac{t-b}{a}\right)dt, \tag{6}$$

где $C_M = \frac{1}{a}\int_{b-aM}^{b+aM} \psi\left(\frac{t-b}{a}\right)dt = \int_{-M}^{M} \psi(u)du$, $b \in R$, $a > 0$, $\psi(t)$ – сингулярный вейвлет, C_M – нормирующая постоянная.

Если $M \to \infty$ и параметр a фиксирован, то локальное вейвлет-преобразование (6) стремится к вейвлет-преобразованию для бесконечного интервала (5), поэтому будут использоваться одинаковые обозначения для того и другого вейвлет-преобразования. Аналогично для регуляризованного локального вейвлет-преобразования применяется обозначение

$$W(f - f(b))(b,a) = \frac{1}{aC_M} \int_{b-aM}^{b+aM} (f(t) - f(b))\psi\left(\frac{t-b}{a}\right)dt, \tag{7}$$

где $b \in R$, $C_M > 0$, $a > 0$.

Лемма. Если функция $f(x)$ принадлежит пространству L^1 и непрерывна в точке $x \in R$, то функция $F(x) = W(f - f(x))(x, a)$ непрерывна в точке $x \in R$ и принадлежит пространству L^1.

Доказательство. Запишем функцию $F(x)$, используя формулу (7), в виде выражения

$$F(x) = \frac{1}{aC_M} \int_{x-aM}^{x+aM} (f(t) - f(x))\psi\left(\frac{t-x}{a}\right)dt. \tag{8}$$

Выполнив замену переменных $x = au + t$ в выражении (8), получим равенство

$$F(x) = -f(x) + \frac{1}{C_M} \int_{-M}^{M} f(x+au)\psi(u)du, \tag{9}$$

где $C_M = \int_{-M}^{M} \psi(u)du$, $C_M > 0$. Пусть $F(x)$ – непрерывная в точке $x \in R$ функция и для определенности $\Delta x > 0$ (случай $\Delta x < 0$ рассматривается аналогично). Обозначим приращение функции $F(x)$ как $\Delta F = F(x+\Delta x) - F(x)$ и получим неравенство

$$|\Delta F| \le |f(x+\Delta x) - f(x)| + \frac{1}{C_M} \int_{-M}^{M} |f(x+\Delta x+au) - f(x+au)|\psi(u)du. \tag{10}$$

Докажем, что выражение ΔF можно сделать сколь угодно малым. Пусть $\omega_x(\delta) = = \sup_{|\Delta x| \le \delta} |f(x+\Delta x) - f(x)|$, где x и $x+\Delta x \in R$. Тогда выполняется неравенство

$$|\Delta F| \le \omega_x(\Delta x) + \omega_x(\Delta x)\frac{1}{C_M} \int_{-\infty}^{\infty} |\psi(t)|dt \le \varepsilon$$

для достаточно малого Δx $\psi(t) \in L^1(R)$.

Таким образом, показана непрерывность функции $F(x) = W(f - f(x))(x, a)$ в точке x. Теперь докажем, что $F(x) \in L^1$. На основании (9) получим

$$\int_{-\infty}^{\infty}|F(x)|dx \le \int_{-\infty}^{\infty}|f(x)|dx + \frac{1}{C_M}\left|\int_{-\infty}^{\infty}\int_{-M}^{M} f(x+au)\psi(u)dudx\right| \le$$

$$\le \int_{-\infty}^{\infty}|f(x)|dx + \frac{1}{C_M}\left|\int_{-M}^{M}\psi(u)\int_{-\infty}^{\infty} f(x+au)dxdu\right| \le$$

$$\le \int_{-\infty}^{\infty}|f(x)|dx + \frac{1}{C_M}\left|\int_{-M}^{M}\psi(u)du\right|\int_{-\infty}^{\infty}|f(\tau)|d\tau = 2\int_{-\infty}^{\infty}|f(x)|dx.$$

Из леммы следует, что последовательное применение вейвлет-преобразования приводит к последовательности непрерывных в точке x функций из пространства L^1. Пусть $\psi(t)$ – вейвлет, среднее значение которого $C_\psi > 0$. Покажем, что можно аппроксимировать функцию $f(x)$ с помощью последовательности регуляризованных локальных вейвлет-преобразований

$$F^{k+1}(x) = F^k(x) - WF^k(x, a_k), \tag{11}$$

где

$$WF^k(x, a_k) = \frac{1}{C_M}\int_{x-a_kM}^{x+a_kM} F^k(t)\psi\left(\frac{t-x}{a_k}\right)dt, \tag{12}$$

$F^0(x) = f(x)$ − начальное значение, $F^k(x) \in L^1$, $k = 0, 1, 2, \ldots, K$, M – фиксированная постоянная, $M > 0$, $C_M > 0$, $F^k(x)$ – регуляризованное локальное вейвлет-преобразование (7) (с точностью до знака, $F^{k+1}(x) = -W(F^k - F^k(x))(x, a_k)$).

Теорема 1. *Если функция $f(x) \in L^1$ и непрерывна в точке $x \in [A, B]$, то справедливо вейвлет-разложение*

$$f(x) = \sum_{k=0}^{K-1} WF^k(x, a_k) + F^K(x), \tag{13}$$

где a_k − произвольные положительные действительные числа;

$F^0(x) = f(x)$;

$F^k(x) \in L^1$, $F^k(x)$ − последовательность рекуррентных вейвлет-преобразований (11);

$F^K(x)$ – остаточный член;

k – порядковый номер вейвлет-преобразования, $0 \le k \le K$;

K – порядок приближения, $K \ge 1$.

Доказательство проиллюстрируем на примере приближения второго порядка, $K = 2$. Выберем M так, чтобы выполнялось $C_M > 0$. В этом случае согласно рекуррентным формулам (11) справедливы равенства

$$F^1(x) = F^0(x) - WF^0(x, a_0),$$

$$F^2(x) = F^1(x) - WF^1(x, a_1).$$

Складывая данные равенства, получим $F^2(x) = F^0(x) - WF^0(x, a_0) - WF^1(x, a_1)$. Учитывая, что $F^0(x) = f(x)$, будет выполняться выражение

$$f(x) = WF^0(x, a_0) + WF^1(x, a_1) + F^2(x). \tag{14}$$

Таким образом доказано, что равенство (13) выполняется тождественно для случая $K = 1$. Для произвольного порядка K формула (13) доказывается аналогично.

Формула остаточного члена. Вначале определим разности k-го порядка Δ^k в узлах z, z_0, $z_1, \ldots, z_k$ по формулам

$$\Delta f(z, z_0) = f(z) - f(z + z_0), \tag{15}$$

$$\Delta^2 f(z, z_0, z_1) = \Delta f(z, z_0) - \Delta f(z + z_1, z_0), \tag{16}$$

$$\Delta^k f(z, z_0, z_1, ..., z_{k-1}) = \Delta^{k-1} f(z, z_0, z_1, ..., z_{k-2}) - \Delta^{k-1} f(z + z_{k-1}, z_0, ..., z_{k-2}).$$

Из формулы (11) при $k = 0$ получим равенство

$$F^1(x) = \frac{1}{C_M} \int_{-M}^{M} (f(x) - f(x + au))\psi(u)du. \tag{17}$$

С учетом разности первого порядка (15) справедливо выражение

$$F^1(x) = \frac{1}{C_M} \int_{-M}^{M} \Delta^1 f(x, a_0 u_0)\psi(u_0)du. \tag{18}$$

Для функции $F^2(x)$ из формулы (11) при $k = 1$ получим равенство

$$F^2(x) = \frac{1}{C_M} \int_{-M}^{M} \Delta^1 F_1(x, a_1 u_1)\psi(u_1)du_0. \tag{19}$$

Используя разность второго порядка (16) и выражение (18), запишем равенство (19) как соотношение

$$F^2(x) = \frac{1}{C_M^2} \int_{-M}^{M} \int_{-M}^{M} \Delta^2 f(x, a_0 u_0, a_1 u_1)\psi(u_0)\psi(u_1)du_0 du_1.$$

Аналогично для функции $F^k(x)$ справедливо представление

$$F^k(x) = \frac{1}{C_M^k} \int_{-M}^{M} \int_{-M}^{M} ... \int_{-M}^{M} \Delta^k f(x, a_0 u_0, a_1 u_1, ..., a_{k-1} u_{k-1})\psi(u_0)\psi(u_1)...\psi(u_{k-1})du_0 du_1 ... du_{k-1}. \tag{20}$$

Теорема 2 (достаточное условие равномерной сходимости). *Пусть по формуле (11) определена последовательность вейвлет-преобразований $F^k(x)$ с неотрицательным вейвлетом $\psi(u)$. Если для функции $f(x) \in L^1$ в некоторых точках $x \in R$ выполняется условие Липшица $|f(x) - f(x+\Delta x)| < L|\Delta x|$, где L – постоянная, то последовательность $F^k(x)$ равномерно стремится к нулю в этих точках для $a_k = a_0 q^k$, $k = 0, 1, \ldots$, $0 < q < 1/2$.*

Доказательство. Если для функции $f(x)$ в точке x выполняется условие Липшица, то для разности первого порядка $\Delta f(x, a_0 u_0) = f(x) - f(x + a_0 u_0)$ получим неравенство

$$|\Delta f(x, a_0 u_0)| \le a_0 L |u_0| .$$

Аналогично для разности второго порядка справедливо неравенство

$$|\Delta^2 f(x, a_0 u_0, a_1 u_1)| \le |f(x) - f(x + a_1 u_1)| + |f(x + a_0 u_0 + a_1 u_1) - f(x + a_0 u_0)| \le 2^1 a_1 L |u_1|.$$

В общем случае для разности k +1-го порядка выполняется неравенство

$$\Delta^k f(x, a_0 u_0, a_1 u_1, ..., a_{k-1} u_{k-1}) \le 2^{k-1} a_{k-1} L |u_{k-1}|. \tag{21}$$

Для функции $F^k(x)$, заданной формулой (20), используя соотношение (21), получим неравенство

$$|F^k(x)| \le \frac{2^{k-1}}{C_M^k} \int_{-M}^{M} \int_{-M}^{M} ... \int_{-M}^{M} a_{k-1} |u_{k-1}| \psi(u_0)\psi(u_1)...\psi(u_{k-1})du_0 du_1 ... du_{k-1} \le 2^{k-1} a_{k-1} LM.$$

Итак, доказано, что $\left|F^k(x)\right| \le 2^{k-1} a_{k-1} LM$, где $k = 0, 1, 2, \ldots$ Следовательно, если $a_k = a_0 q^k$, где $0 < q < 1/2$, $a_0 > 0$, то последовательность $F^k(x)$ равномерно стремится к нулю. Функция $F^K(x)$ является остаточным членом последовательности (13). Поэтому вейвлет-разложение (13) можно использовать для аппроксимации функции $f(x)$.

Аппроксимация дельта-вейвлетами (13) может служить обоснованием численного алгоритма аппроксимации. Однако можно определить дискретное вейвлет-преобразование и самостоятельно. В этом случае требуется дополнительное исследование, целесообразность которого подтвердим с помощью примера аппроксимации непрерывной функции, заданной на дискретном множестве точек. Пусть точки x_i, $i = 1, \ldots, n$, принадлежат интервалу $[-1, 1]$ и известны значения функции $y_i = f(x_i)$ в этих точках.

Алгоритм дискретной аппроксимации:

1. Присваиваем начальные значения y_i коэффициентам вейвлет-преобразования нулевого порядка: $W_i^0 = y_i$, $i = 1, \ldots, n$.

2. Вычисляем коэффициенты локального регуляризованного вейвлет-преобразования, используя дискретный аналог формулы (11):

$$W_j^k = W_j^{k-1} - \frac{\sum\limits_{S(i)} W_i^{k-1} \psi\left(\dfrac{x_i - x_j}{a_{k-1}}\right)}{\sum\limits_{S(i)} \psi\left(\dfrac{x_i - x_j}{a_{k-1}}\right)}, \tag{22}$$

где $k = 1, \ldots, K$, W_i^k – значения коэффициентов вейвлета k-го порядка в точке x_i, $j = 1, \ldots, n$, $a_k = \alpha 2^{-k}$, α – постоянная. В формуле (22) $S(i)$ означает суммирование выражений под знаком суммы по всем значениям переменной i, для которых выполняется неравенство $\left|x_i - x_j\right| \le a_{k-1} M$.

3. Восстанавливаем функцию $f_K(x) \approx f(x)$ во всех точках интервала $[-1, 1]$, используя аналог формулы (13):

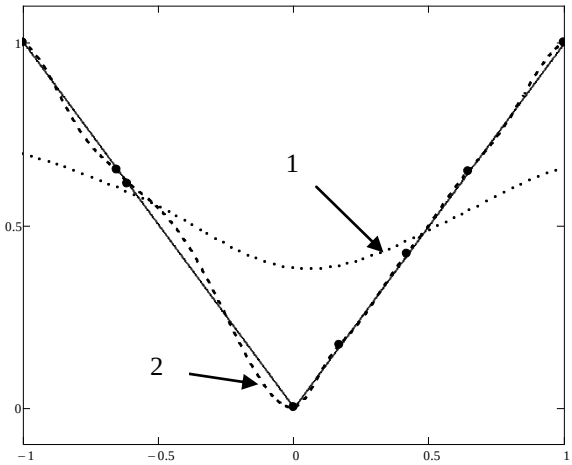
$$f_K(x) = \sum_{k=0}^{K} \frac{\sum\limits_{S(i)} W_i^k \psi\left(\dfrac{x_i - x}{a_k}\right)}{\sum\limits_{S(i)} \psi\left(\dfrac{x_i - x}{a_k}\right)}. \tag{23}$$

Рассмотрим частный случай: $\psi(t) = \dfrac{1}{1+t^2}$, $x_i \in [-1, 1]$, $y_i = |x_i|$. Выбраны значения параметров $M = 32$, $a_0 = 1$. Значения коэффициентов вейвлетов W_i^k, найденные по формуле (22), представлены в таблице. Номеру строки m, $m = 1, 2, \ldots, 6$, соответствует номер преобразования $k = m - 1$. Номер столбца i, $i = 1, 2, \ldots, 8$, совпадает с номером точки x_i.

Коэффициенты вейвлетов W_i^k

1,00	0,61	0,17	0,00	0,65	0,65	0,42	1,00
0,31	0,02	–0,22	–0,38	0,11	0,05	–0,03	0,35
0,14	–0,01	–0,06	–0,19	0,06	0,00	0,01	0,14
0,03	–0,01	0,01	–0,06	0,01	0,00	0,01	0,02
0,00	–0,01	0,01	–0,01	0,00	0,01	0,00	0,00
0,00	–0,00	0,00	–0,00	0,00	0,00	–0,00	–0,00

Значения аппроксимирующей функции были рассчитаны по формуле (23). На рисунке изображены график функции $f_K(x)$, $x \in [-1, 1]$, для $K = 2$ и $K = 6$, график функции $y = |x|$ и точки, в которых заданы значения функции $y_i = |x_i|$, $i = 1, 2, \ldots, 8$.



Аппроксимация функции $y = |x|$: 1 − график $f_2(x)$, 2 − график $f_6(x)$

Аппроксимацию функцией $f_2(x)$ можно интерпретировать как результат сглаживания данных, аппроксимацию функцией $f_6(x)$ − как интерполяцию (квазиинтерполяцию). Используя приближения разного порядка K, можно получить различные степени сглаживания функции или при необходимости интерполировать экспериментальные данные. Применение сингулярных вейвлетов позволяет аппроксимировать функцию в случае неравномерного расположения узлов. Результаты расчета подтверждают целесообразность продолжения исследования дискретного варианта вейвлет-преобразования.

Заключение. В работе получены новые результаты теории сингулярных вейвлетов. Впервые рассматривается определение локального преобразования с сингулярным вейвлетом. Проведено исследование сходимости последовательности преобразований с сингулярным вейвлетом. Сформулировано и доказано достаточное условие равномерной сходимости последовательности вейвлет-преобразований. Локальное вейвлет-преобразование можно использовать для аппроксимации функциональных зависимостей. Приведен пример сглаживания и квазиинтерполяции дискретно заданной функции с нерегулярным расположением узлов на конечном промежутке.

Список использованных источников

1. Хардле, В. Прикладная непараметрическая регрессия : пер. с англ. / В. Хардле. − М. : Мир, 1993. – 349 с.

2. Parzen, E. On estimation of a probability density function and mode / E. Parzen // The Annals of Mathematical Statistics. – 1962. – Vol. 33, no. 3. – P. 1065−1076.

3. Watson, G. S. Smooth regression analysis / G. S. Watson // Sankhya: The Indian Journal of Statistics, Ser. A. −1964. − Vol. 26. − P. 359–372.

4. Надарая, Э. А. Об оценке регрессии / Э. А. Надарая // Теория вероятностей и ее применение. − 1964. − Т. 9, № 1. − С. 157–159.

5. Чуи, К. Введение в вейвлеты : пер. с англ. / К. Чуи. − М. : Мир, 2001. – 412 с.

6. Добеши, И. Десять лекций по вейвлетам : пер. с англ. / И. Добеши. – Ижевск : НИЦ «Регулярная и хаотическая динамика», 2001. − 464 с.

7. Серенков, П. С. Система сбора данных о качестве как техническая основа функционирования эффективных систем менеджмента качества / П. С. Серенков, В. М. Романчак, В. Л. Соломахо // Докл. Нац. акад. наук Беларуси. – 2006. – Т. 50, № 4. – С. 100–104.

8. Романчак, В. М. Аппроксимация экспертных оценок сингулярными вейвлетами / В. М. Романчак, П. М. Лаппо // Вестник Гродненского гос. ун-та. Сер. 2. Математика. Физика. Информатика, вычислительная техника и управление. – 2017. – Т. 7, № 1. − С. 132−139.

9. Романчак, В. М. Аппроксимация сингулярными вейвлетами / В. М. Романчак // Системный анализ и прикладная информатика. – 2018. – № 2. − С. 23–28.

10. Романчак, В. М. Сингулярные вейвлеты на конечном интервале / В. М. Романчак // Информатика. – 2018. – Т. 15, № 4. − С. 39–49.

References

1. Härdle W. *Applied Nonparametric Regression*. Cambridge, Cambridge University Press, 1992, 434 p.

2. Parzen E. On estimation of a probability density function and mode. *The Annals of Mathematical Statistics*, 1962, vol. 33, no. 3, pp. 1065−1076.

3. Watson G. S. Smooth regression analysis. *Sankhya: The Indian Journal of Statistics, Ser. A*, 1964, vol. 26, pp. 359–372.

4. Nadaraya E. A. Ob ocenke regressii [About a regression assessment]. Teorija verojatnostej i ee primenenie [*Probability Theory and Its Application*], 1964, vol. 9, no. 1, pp. 157–159 (in Russian).

5. Chui C. *An Introduction to Wavelets*. San Diego, Academic Press, 1992, 266 p.

6. Daubechies I. *Ten Lectures on Wavelets*. Philadelphia, Society for Industrial and Applied Mathematics, 1992, 377 p.

7. Serenkov P. S., Romanchak V. M., Solomakho V. L. Sistema sbora dannyh o kachestve kak tehnicheskaja osnova funkcionirovanija jeffektivnyh sistem menedzhmenta kachestva [System of collection of data on quality as technical basis of functioning of effective systems of quality management]. Doklady Nacional'noj akademii nauk Belarusi [*Doklady of the National Academy of Sciences of Belarus*], 2006, vol. 50, no. 4, pp. 100−104 (in Russian).

8. Romanchak V. M., Lappo P. M. Approksimacija jekspertnyh ocenok singuljarnymi vejvletami [Approximation of expert estimates by singular wavelets]. Vestnik Grodnenskogo gosudarstvennogo universiteta. Ser. 2. Matematika. Fizika. Informatika, vychislitel'naja tehnika i upravlenie [*Bulletin of the Grodno State University. Series 2: Mathematics. Physics. Informatics, Computer Science and Management*], 2017, vol. 7, no. 1, pp. 132−139 (in Russian).

9. Romanchak V. M. Approksimacija singuljarnymi vejvletami [Approximation by singular wavelets]. Sistemnyj analiz i prikladnaja informatika [*Systems Analysis and Applied Informatics*], 2018, no. 2, pp. 23–28 (in Russian).

10. Romanchak V. M. Singuljarnye vejvlety na konechnom intervale [Singular wavelets on a finite interval]. Informatika [*Informatics*], 2018, vol. 15, no. 4, pp. 39−49 (in Russian).

Информация об авторе

Романчак Василий Михайлович, кандидат технических наук, доцент кафедры инженерной математики, Белорусский национальный технический университет, Минск, Беларусь.
E-mail: Romanchak@bntu.by

Information about the author

Vasily M. Romanchak, Cand. Sci. (Eng.), Associate Professor of the Department of Engineering Mathematics, Belarusian National Technical University, Minsk, Belarus.
E-mail: Romanchak@ bntu.by

ISSN 1816-0301 (Print)
ISSN 2617-6963 (Online)

АВТОМАТИЗАЦИЯ ЛОГИЧЕСКОГО ПРОЕКТИРОВАНИЯ

COMPUTER-AIDED LOGICAL DESIGN

УДК 004.33.054
https://doi.org/10.37661/1816-0301-2020-17-1-47-62

Поступила в редакцию 02.10.2019
Received 02.10.2019

Принята к публикации 14.11.2019
Accepted 14.11.2019

Формирование адресных последовательностей с заданной переключательной активностью

В. Н. Ярмолик[1]✉, Н. А. Шевченко[2]

[1]Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь
✉E-mail: yarmolik10ru@yahoo.com

[2]Гимназия имени Лихтенберга, Дармштадт, Германия

Аннотация. Показывается актуальность тестирования современных вычислительных систем, и в первую очередь их запоминающих устройств. Исследования основаны на применении универсального метода генерирования адресных последовательностей с заданными свойствами для многократных маршевых тестов оперативных запоминающих устройств. В качестве математической модели используется модификация экономичного способа Антонова и Салеева для формирования последовательностей Соболя. Для указанной модели приводится структурная схема ее аппаратурной реализации, основу которой составляет запоминающее устройство для хранения направляющих чисел. Множество этих чисел образует порождающую матрицу. Отмечается, что вид порождающей матрицы определяет основные свойства генерируемых последовательностей. Получены математические выражения, позволяющие оценить предельные значения переключательной активности самой последовательности и определенных ее разрядов. Предлагаются методики синтеза генераторов адресной последовательности с заданной переключательной активностью как отдельных ее разрядов, так и последовательности в целом. Рассматриваются примеры использования предлагаемых методик. Обосновывается применимость изложенных результатов для синтеза генераторов тестовых последовательностей с заданной переключательной активностью при тестировании запоминающих устройств и формировании управляемых вероятностных тестовых последовательностей. Приводятся результаты практической реализации генераторов адресных последовательностей и оцениваются их основные характеристики.

Ключевые слова: тестирование вычислительных систем, многократное тестирование, адресные последовательности, модифицированные последовательности Соболя, переключательная активность

Для цитирования. Ярмолик, В. Н. Формирование адресных последовательностей с заданной переключательной активностью / В. Н. Ярмолик, Н. А. Шевченко // Информатика. – 2020. − Т. 17, № 1. – С. 47–62. https://doi.org/10.37661/1816-0301-2020-17-1-47-62

Generation of address sequences with a given switching activity

Vyacheslav N. Yarmolik[1]✉, Nikolai A. Shevchenko[2]

[1]Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus
✉Email: yarmolik10ru@yahoo.com

[2]Lichtenberg Gymnasium, Darmstadt, Germany

Abstract. The relevance of testing modern computing systems and, first of all, their storage devices is shown. The studies are based on the use of a universal method for generating the address sequences with desired properties for multiple March tests of random access memory devices. The modification of economical method

of Antonov and Saleev is used as mathematical model to form Sobol sequences. For this model a structural diagram of its hardware implementation is presented, where the storage device for storing direction numbers is used as the basis. The set of multitudes makes up the generating matrix. It is noted that the form of the generating matrix determines the basic properties of the generated sequences. Mathematical expressions are obtained that make it possible to estimate the limiting values of switching activity, both of the sequence itself and of its individual bits. A technique is proposed for the synthesis of generators of address sequences with a given switching activity both of its individual bits and of the sequence as a whole. Examples of the application of the proposed methods are considered. The applicability of the presented results to the synthesis of test sequence generators with a given switching activity for the purpose of testing storage devices and the formation of controlled random test sequences is substantiated. The results of the practical implementation of address sequence generators are presented and their main characteristics are evaluated.

Keywords: testing of computing systems, multiple testing, address sequences, modified Sobol sequences, switching activity

For citation. Yarmolik V. N., Shevchenko N. A. Generation of address sequences with a given switching activity. *Informatics*, 2020, vol. 17, no. 1, pp. 47−62 (in Russian). https://doi.org/10.37661/1816-0301-2020-17-1-47-62

Введение. Одной из актуальных проблем современных вычислительных систем, таких как встроенные системы (embedded systems), системы на кристалле (systems-on-a-chip) и сети на кристалле (nets-on-a-chip), является тестирование их запоминающих устройств, удельный вес которых достигает 90 % занимаемой системой площади кристалла [1, 2]. При многократном тестировании запоминающих устройств несомненный интерес вызывают детерминированные последовательности, имеющие различные свойства и применяемые для формирования как тестовых, так и адресных последовательностей запоминающих устройств [3–5]. При этом наиболее часто используемой характеристикой данных последовательностей является так называемая переключательная активность (switching activity), которая влияет на переключательную активность тестируемых цифровых устройств [6–8].

Определяющее значение переключательная активность имеет в области проектирования цифровых устройств с низким потреблением энергии [9, 10], в том числе при разработке и применении средств их тестирования и самотестирования [11, 12]. Большое количество исследований в данной области направлено на получение оценок значений переключательной активности полюсов проектируемых устройств, которые позволяют прогнозировать их энергопотребление [9, 13]. Обратная задача, а именно задача синтеза цифровых устройств с заданной интегральной переключательной активностью (как правило, минимальной), чрезвычайно сложна и решается путем выбора наилучшего результата из небольшого числа возможных вариантов построения устройства [9, 13].

В области тестового диагностирования современных вычислительных систем переключательная активность также имеет огромное значение, поскольку от нее зависит эффективность тестовых процедур, которая определяется как временем тестирования, так и полнотой покрытия неисправностей. При этом, как правило, для уменьшения длины теста и увеличения полноты его покрытия существенным является не только увеличение переключательной активности объекта тестирования в целом, но и возможность управления этой характеристикой в заданных диапазонах. Решение подобных задач в основном ориентируется на построение генераторов тестов с низким потреблением энергии [11], перестановку тестовых наборов [12], применение различных оценок этой характеристики [7, 8] и схемотехнических подходов при реализации методов контролепригодного синтеза [14, 15].

Между тем исследование вопросов синтеза различного рода устройств с заданными значениями переключательной активности для тестирования вычислительных систем находится лишь в начальной стадии. В частности, методы синтеза генераторов адресных последовательностей, рассмотренные в ряде источников [3, 4, 16], позволяют строить подобные устройства, описываемые фиксированными значениями переключательной активности. Вопрос решения задачи синтеза устройств для генерирования тестовых последовательностей с заданной переключательной активностью при тестировании запоминающих устройств и формировании управляемых вероятностных тестовых последовательностей остается практически открытым.

Генератор адресных последовательностей. Под адресной последовательностью понимают упорядоченную последовательность m-разрядных двоичных векторов $A(n) = a_{m-1}a_{m-2}a_{m-3} \ldots a_2a_1a_0$, $a_i \in \{0,1\}$, $i \in \{0, 1, 2, \ldots, m-1\}$ и $n \in \{0, 1, 2, \ldots, 2^m-1\}$, однократно принимающих все возможные значения $\{0, 1, 2, \ldots, 2^m-1\}$ [3, 4, 17]. Подобные последовательности имеют период, равный 2^m, и их часто называют пересчетными (counting sequences) последовательностями, последовательностями де Брюйна (de Bruijn sequences) либо (по аналогии с M-последовательностями) последовательностями максимальной длины [17]. Существует большое множество различных разновидностей последовательностей максимальной длины, среди которых выделяют такие их подмножества, как детерминированные, псевдослучайные и квазислучайные последовательности [3, 4, 17]. Хорошо апробированы и применяются на практике пересчетные (счетчиковые) последовательности, последовательности Грея и анти-Грея, последовательности с максимальной переключательной активностью, с заданным расстоянием Хэмминга, $ЛП_\tau$-последовательности, M-последовательности и ряд других [3, 4, 17]. Каждая из них описывается своим уникальным алгоритмом, предполагающим специфическую реализацию. Поэтому попытка реализации какого-то подмножества адресных последовательностей требует большой аппаратурной избыточности.

С целью существенного уменьшения аппаратурных затрат для генерирования большого множества адресных последовательностей в работе [4] рассмотрена математическая модель универсального генератора адресных последовательностей. В качестве основы данной модели используется метод формирования последовательностей Соболя [18].

В работе [18] показано, что значение координат n-го элемента последовательности Соболя вычисляется как поразрядная сумма по модулю два до $m = \lfloor \log_2 n \rfloor$ операндов в зависимости от количества ненулевых компонент двоичного представления $b_{m-1}(n)b_{m-2}(n)\ldots b_1(n)b_0(n)$ числа n. Количество операндов может быть снижено до одного при использовании экономичного способа Антонова и Салеева, основанного на представлении числа n в коде Грея [4, 19, 20]. Тогда формирование n-го элемента $A(n)$ последовательности Соболя осуществляется в соответствии с соотношением

$$A(n) = A(n-1) \oplus \mathrm{v}_i, \quad n = \overline{0, 2^m - 1}, \quad i = \overline{0, m-1}, \tag{1}$$

в котором к предыдущему элементу $A(n-1)$ последовательности Соболя добавляется только одно модифицированное направляющее число v_i, $i \in \{0, 1, 2, \ldots, m-1\}$ [19, 20]. Значение индекса i направляющего числа v_i, используемого в качестве слагаемого в выражении (1), зависит от так называемой последовательности переключений T_{m-1} отраженного кода Грея. Например, для $m = 4$ эта последовательность имеет вид $T_3 = 0, 1, 0, 2, 0, 1, 0, 3, 0, 1, 0, 2, 0, 1, 0$. Формально последовательность переключений T_{m-1} определяет индекс i изменяемого разряда при переходе от n_{g-1} к n_g, где индекс g числа n_g означает представление в коде Грея исходного числа $n = b_{m-1}(n)\, b_{m-2}(n) \ldots b_1(n)\, b_0(n)$. Число n в коде Грея может быть получено согласно известному соотношению $n_g = g_{m-1}(n)\, g_{m-2}(n) \ldots g_1(n)\, g_0(n) = b_{m-1}(n)\, b_{m-2}(n) \ldots b_1(n)\, b_0(n) \oplus 0\, b_{m-1}(n)\, b_{m-2}(n) \ldots b_2(n)\, b_1(n)$ [21]. Сумма по модулю два последовательных значений n_g и n_{g-1} кода Грея определяет индекс i направляющего числа v_i, используемого в выражении (1). Последовательность значений индекса чисел v_i представляет собой T_{m-1}. Процедура получения последовательности переключений T_{m-1} для $m = 4$ в виде аппаратной структуры изображена на рис. 1.

Наиболее сложным блоком данного устройства является синхронный двоичный счетчик (Binary Counter), который при подаче синхронизирующего сигнала (Clk) выполняет операцию увеличения своего состояния на единицу (+1). Таким образом формируется пересчетная последовательность $n = b_3(n)\, b_2(n)\, b_1(n)\, b_0(n)$ (табл. 1).

Значения разрядов кода Грея для $m = 4$ определяются в соответствии с соотношениями $g_3(n) = b_3(n)$, $g_2(n) = b_2(n) \oplus b_3(n)$, $g_1(n) = b_1(n) \oplus b_2(n)$ и $g_0(n) = b_0(n) \oplus b_1(n)$, полученными согласно выражению $n_g = g_3(n)\, g_2(n)\, g_1(n)\, g_0(n) = b_3(n)\, b_2(n)\, b_1(n)\, b_0(n) \oplus 0\, b_3(n)\, b_2(n)\, b_1(n)$. Последовательность переключений T_3 определяет индекс $i \in \{0, 1, 2, 3\}$ изменяемого разряда при переходе от кода $n_{g-1} = g_3(n-1)\, g_2(n-1)\, g_1(n-1)\, g_0(n-1)$, который хранится на D-триггерах (см. рис. 1), к коду $n_g = g_3(n)\, g_2(n)\, g_1(n)\, g_0(n)$. Соответственно, на выходах $i = 0$, $i = 1$, $i = 2$ и $i = 3$ устройства

формируются управляющие сигналы, определяющие последовательность выборки так называемых направляющих чисел (direction numbers) $v_i = \beta_{m-1}(i)\beta_{m-2}(i)\ldots\beta_0(i)$, $i \in \{0, 1, 2, \ldots, m-1\}$ [4]. При этом из табл. 1 видно, что в каждый такт работы устройства только на одном из его выходов формируется сигнал, который определяет индекс i направляющего числа v_i, используемого в очередной итерации для получения $A(n)$ (см. (1)).

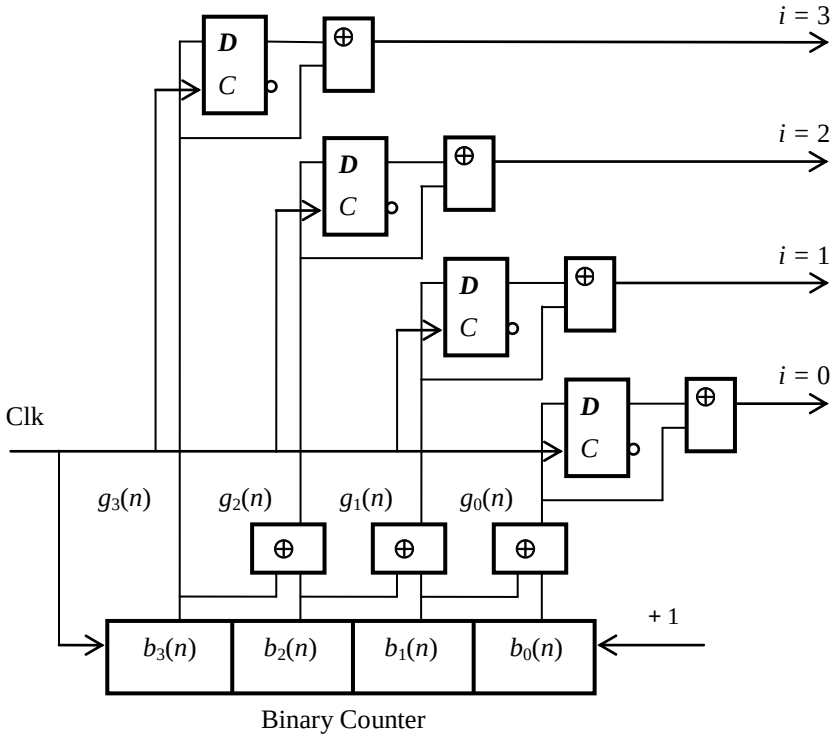


Рис. 1. Устройство для генерирования последовательности переключений T_{m-1} при $m = 4$

Таблица 1

Процедура генерирования последовательности переключений T_3

n	$n = b_3(n)b_2(n)b_1(n)b_0(n)$	$n_g = g_3(n)g_2(n)g_1(n)g_0(n)$	$n_g \oplus n_{g-1}$	T_3
0	0 0 0 0	0 0 0 0	0 0 0 0	
1	0 0 0 1	0 0 0 1	0 0 0 1	0
2	0 0 1 0	0 0 1 1	0 0 1 0	1
3	0 0 1 1	0 0 1 0	0 0 0 1	0
4	0 1 0 0	0 1 1 0	0 1 0 0	2
5	0 1 0 1	0 1 1 1	0 0 0 1	0
6	0 1 1 0	0 1 0 1	0 0 1 0	1
7	0 1 1 1	0 1 0 0	0 0 0 1	0
8	1 0 0 0	1 1 0 0	1 0 0 0	3
9	1 0 0 1	1 1 0 1	0 0 0 1	0
10	1 0 1 0	1 1 1 1	0 0 1 0	1
11	1 0 1 1	1 1 1 0	0 0 0 1	0
12	1 1 0 0	1 0 1 0	0 1 0 0	2
13	1 1 0 1	1 0 1 1	0 0 0 1	0
14	1 1 1 0	1 0 0 1	0 0 1 0	1
15	1 1 1 1	1 0 0 0	0 0 0 1	0

В работе [18] показано, что для всех возможных направляющих чисел некоторые их разряды принимают фиксированные значения. Так, всегда $\beta_{m-1-i}(i) = 1$, $i = \overline{0, m-1}$, и $\beta_{m-1-j}(i) = 0$ для $j > i$, а $\beta_{m-1-i}(i)$ для $j < i$ принимают произвольные значения в зависимости от выбранного направляющего числа [18, 20]. Это значит, что для всех возможных последовательностей Соболя $v_0 = 100\ldots00$, $v_1 = \beta_{m-1}(1)10\ldots00$, где $\beta_{m-1}(1)$ принимает значение 0 либо 1, $v_2 = \beta_{m-1}(2)\,\beta_{m-2}(2)10\ldots00$ и т. д. [20]. В общем случае числа v_i можно представить в виде нижней треугольной матрицы с единичной диагональю [4]:

$$V = \begin{vmatrix} 1 & 0 & 0 & \ldots & 0 \\ \beta_{m-1}(1) & 1 & 0 & \ldots & 0 \\ \beta_{m-1}(2) & \beta_{m-2}(2) & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \beta_{m-1}(m-1) & \beta_{m-2}(m-1) & \beta_{m-3}(m-1) & \ldots & 1 \end{vmatrix}. \qquad (2)$$

Предложенная математическая модель может быть расширена для случая последовательностей, относящихся не только к множеству квазислучайных числовых последовательностей [4]. В общем случае в качестве порождающей матрицы направляющих чисел V может быть использована любая двоичная квадратная матрица размерности $m \times m$ вида

$$V = \begin{vmatrix} \beta_{m-1}(0) & \beta_{m-2}(0) & \beta_{m-3}(0) & \ldots & \beta_0(0) \\ \beta_{m-1}(1) & \beta_{m-2}(1) & \beta_{m-3}(1) & \ldots & \beta_0(1) \\ \beta_{m-1}(2) & \beta_{m-2}(2) & \beta_{m-3}(2) & \ldots & \beta_0(2) \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \beta_{m-1}(m-1) & \beta_{m-2}(m-1) & \beta_{m-3}(m-1) & \ldots & \beta_0(m-1) \end{vmatrix}, \qquad (3)$$

построенная из m линейно независимых двоичных векторов $v_i = \beta_{m-1}(i)\,\beta_{m-2}(i)\,\ldots\,\beta_0(i)$, $i = \overline{0, m-1}$.

Отметим, что нижняя треугольная матрица с единичной диагональю (2) по определению имеет максимальный ранг и является базисом линейного векторного пространства. Это объясняется тем, что такая матрица состоит из m линейно независимых двоичных векторов. Поэтому любая подобная матрица позволяет генерировать всевозможные двоичные векторы размерности m.

Таким образом, основу генератора адресных последовательностей составляет устройство для хранения направляющих чисел $v_i = \beta_{m-1}(i)\,\beta_{m-2}(i)\,\ldots\,\beta_0(i)$, $i = \overline{0, m-1}$, порождающей матрицы V (3), а структура генератора состоит из трех последовательно подключенных функциональных блоков (рис. 2).

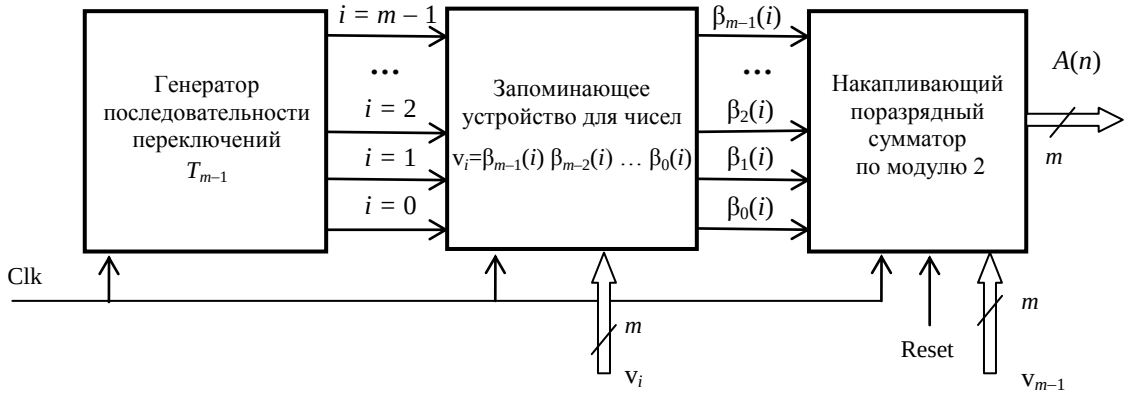


Рис. 2. Генератор адресных последовательностей

Первым блоком устройства генерирования адресов является генератор последовательности переключений T_{m-1}, которая определяет последовательность выборки направляющих чисел матрицы V (3). Как отмечалось ранее, в каждый такт функционирования только на одном выходе генератора последовательности переключений формируется разрешающий сигнал, определяющий выбранное направляющее число его индексом i. Например, это реализуется для конкретного случая, когда $m = 4$ (см. рис. 1 и табл. 1). Вторым и главным блоком генератора адресов является запоминающее устройство, состоящее из m ячеек, каждая из которых имеет m разрядов, что позволяет хранить в таком запоминающем устройстве m двоичных векторов v_i, состоящих их m бит. Содержимое запоминающего устройства, представляющее собой направляющие числа $\mathrm{v}_i = \beta_{m-1}(i)\ \beta_{m-2}(i)\ \ldots\ \beta_0(i)$, $i = \overline{0, m-1}$, порождающей матрицы V (3), по сути, и определяет вид адресной последовательности $A(n)$.

Третий блок генератора адресных последовательностей реализует соотношение (1) и представляет собой накапливающий поразрядный сумматор по модулю два накопленной суммы с очередным направляющим числом, поступившим из запоминающего устройства. В сумматоре предусмотрена возможность задания нулевого начального адреса $A(0) = 0\ 0\ 0\ \ldots\ 0$ путем реализации обнуления всех разрядов сумматора сигналом Reset. Кроме того, начальным адресам может быть задан вектор $\mathrm{v}_{m-1} = \beta_{m-1}(m-1)\ \beta_{m-2}(m-1)\ \beta_{m-3}(m-1)\ \ldots\ \beta_0(m-1)$. Использование данного вектора в качестве начального значения $A(0) = \beta_{m-1}(m-1)\ \beta_{m-2}(m-1)\ \beta_{m-3}(m-1)\ \ldots\ \beta_0(m-1)$ позволяет формировать последовательность $A(n)$ в обратном порядке по отношению к последовательности, сгенерированной для $A(0) = 0\ 0\ 0\ \ldots\ 0$.

Несомненным достоинством показанного на рис. 2 генератора адресных последовательностей является простота его программной и аппаратной реализации. В то же время подобный генератор позволяет формировать достаточно широкий спектр адресных последовательностей, некоторые из которых представлены и проанализированы в статье [4].

Частотные свойства адресных последовательностей. Для формирования всевозможных двоичных m-разрядных векторов на базе матрицы V (3) обязательным условием является ее максимальный ранг, который обеспечивается линейной независимостью двоичных векторов $\mathrm{v}_i = \beta_{m-1}(i)\ \beta_{m-2}(i)\ \ldots\ \beta_0(i)$, $i = \overline{0, m-1}$.

Количество M двоичных матриц размерности $m \times m$ с максимальным рангом, или количество базисов векторного пространства размерности m над конечным полем F_2, определяется из соотношения [22, 23]

$$M = (2^m - 2^0)(2^m - 2^1)(2^m - 2^2)\ldots(2^m - 2^{m-1}) = \prod_{j=0}^{m-1}(2^m - 2^j) = 2^{m(m-1)/2}\prod_{i=1}^{m}(2^i - 1). \quad (4)$$

В то же время общее количество M_t произвольных двоичных матриц размерности $m \times m$ вычисляется согласно соотношению

$$M_t = 2^{m^2}. \quad (5)$$

В табл. 2 приведены численные значения общего количества двоичных матриц M_t, а также числа M матриц максимального ранга для ряда значений m.

Таблица 2

Численные значения характеристик M_t, M и M/M_t

m	2	3	4	5	6	10	20	30
M_t	2^4	2^9	2^{16}	2^{25}	2^{36}	$\approx 3{,}7\cdot 10^{29}$	$\approx 7{,}46\cdot 10^{119}$	$\approx 2{,}44\cdot 10^{270}$
M	6	168	$\approx 2\cdot 10^4$	$\approx 1\cdot 10^7$	$\approx 2\cdot 10^{10}$	$\approx 12{,}7\cdot 10^{29}$	$\approx 25{,}8\cdot 10^{119}$	$\approx 8{,}45\cdot 10^{270}$
M/M_t	0,375	0,328	0,308	0,298	0,293	0,2892	0,288 79	0,288 78

Величина M/M_t позволяет оценить вероятность того, что матрица, сгенерированная случайным образом, когда ее компонента $\beta_j(i) \in \{0,1\}$, $i = \overline{0, m-1}$, $j = \overline{0, m-1}$, формируется равновероятно равной 0 либо 1, состоит из линейно независимых строк, т. е. имеет максимальный ранг. Для больших значений m эта вероятность может быть оценена величиной

$$\lim_{m\to\infty} M/M_t = \lim_{m\to\infty} 2^{-m(m+1)/2} \prod_{i=1}^{m} (2^i - 1) \approx 0{,}2887880951\ldots \tag{6}$$

Отметим, что полученная оценка значения данной вероятности позволяет констатировать возможность формирования случайным образом матрицы V (3) с последующей проверкой ее ранга, поскольку вероятность того, что ранг этой матрицы будет максимален, достаточно высока.

Из выражения (6) видно, что общее количество различных m-разрядных двоичных последовательностей, которые можно сформировать на основании соотношения (1), огромно. Оно включает в себя последовательности Соболя, Грея, последовательности с максимальной переключательной активностью и др.

Для оценки свойств последовательностей Соболя $A(n) = a_{m-1}\, a_{m-2}\, a_{m-3} \ldots a_1\, a_0$, используемых в качестве адресной последовательности в работе [20], была введена метрика $F(a_j)$, $j \in \{0, 1, 2, \ldots, m-1\}$, определяющая количество переключений (изменений) j-го разряда a_j кода последовательности $A(n)$. В большинстве литературных источников метрика $F(a_j)$ имеет название переключательной активности (switching activity) [7, 8, 14, 16]. В общем случае для произвольного значения j величина данной метрики определяется по формуле [4]

$$F(a_j) = \sum_{i=0}^{m-1} \beta_j(i)\, 2^{m-1-i}. \tag{7}$$

Значения метрики $F(a_j)$ были исследованы для конкретных видов адресных последовательностей, таких как квазислучайные последовательности Соболя, пересчетные адресные последовательности, модифицированные квазислучайные и пересчетные последовательности, а также последовательности с максимальной переключательной активностью [4].

Основываясь на переключательной активности $F(a_j)$ разрядов последовательности $A(n)$, введем для нее интегральную меру переключательной активности $F(A)$, вычисляемой согласно выражению

$$F(A) = \sum_{j}^{m-1} \sum_{i=0}^{m-1} \beta_j(i)\, 2^{m-1-i} = \sum_{i}^{m-1} 2^{m-1-i} \sum_{j=0}^{m-1} \beta_j(i), \tag{8}$$

где вторая сумма является количеством единиц в i-й строке матрицы (3), представляющей собой вес Хэмминга $w(\mathrm{v}_i)$ двоичного вектора $\mathrm{v}_i = \beta_{m-1}(i)\, \beta_{m-2}(i) \ldots \beta_0(i)$, $i = \overline{0, m-1}$.

Оценим предельные значения приведенных метрик переключательной активности адресных последовательностей, которые формируются на основании порождающих матриц вида (3), определенных в работе [4]. В качестве порождающей матрицы может быть использована любая квадратная матрица $m \times m$, состоящая из m линейно независимых двоичных векторов.

Как следует из линейной независимости двоичных векторов v_i, j-й столбец матрицы не может быть нулевым. Поэтому минимальное значение $F(a_j)$, $j \in \{0, 1, 2, \ldots, m-1\}$, достигается тогда, когда только $\beta_j(m-1) = 1$, а остальные $\beta_j(i) = 0$, $i \in \{0, 1, 2, \ldots, m-2\}$. В этом случае значение j-го разряда адресной последовательности изменится только один раз. Следовательно, $\min F(a_j) = 1$. Важно отметить, что достижение минимального значения $F(a_j)$ возможно для любого j-го разряда, но только одного из них. Это ограничение также следует из линейной независимости строк и, соответственно, столбцов порождающей матрицы V (3).

Максимальное значение $F(a_j)$, $j \in \{0, 1, 2, \ldots, m-1\}$, так же, как и минимальное, достигается для любого, но только одного разряда адресной последовательности. Это обеспечивается формированием j-го единичного столбца матрицы (3), $\beta_j(i) = 1$, $i \in \{0, 1, 2, \ldots, m-1\}$. Тогда справедливо равенство

$$\max F(a_j) = \sum_{i=0}^{m-1} 2^{m-1-i} = 2^{m-1} + 2^{m-2} + \cdots + 2^1 + 2^0 = 2^m - 1. \quad (9)$$

Анализ характеристики $F(a_j)$ позволяет сформулировать следующее свойство адресных последовательностей, генерируемых на основании соотношения (1) с применением порождающей матрицы V (3).

Свойство 1. *Переключательная активность разрядов* $F(a_j)$, $j \in \{0, 1, 2, \ldots, m-1\}$, *адресной последовательности* $A(n) = a_{m-1}\, a_{m-2}\, a_{m-3} \ldots a_1\, a_0$ *принимает значения в диапазоне от* 1 *до* 2^m-1, *причем каждый из* m *разрядов имеет свою уникальную переключательную активность.*

Следствием данного свойства является отличие переключательных активностей и (или) перераспределение переключательных активностей для двух различных адресных последовательностей.

Переключательная активность $F(A)$ (см. (8)) адресной последовательности $A(n) = a_{m-1}\, a_{m-2}\, a_{m-3} \ldots a_1\, a_0$, $n \in \{0, 1, 2, \ldots, 2^m-1\}$, принимает минимальное значение для последовательностей кода Грея [4, 20, 21]. Для матрицы, состоящей из m отличающихся строк, каждая из которых содержит по одной единице, согласно (8) имеем $\min F(A) = 2^m-1$. Максимальная оценка $F(A)$ также однозначно определяется видом порождающей матрицы [4], первая строка которой состоит из единиц, а остальные строки содержат по одному нулю. Тогда выполняется равенство

$$\max F(A) = m2^{m-1} + (m-1)\sum_{i=1}^{m-1} 2^{m-i-1} = m2^m - 2^{m-1} - m + 1. \quad (10)$$

На практике чаще всего используются средние значения $F_{av}(A)$ и $F_{av}(a_j)$ рассмотренных ранее метрик переключательной активности $F(A)$ и $F(a_j)$ (см. (7)), которые показывают среднее значение переключений при формировании одного тестового набора. Значения средних величин переключательной активности $F_{av}(A)$ и $F_{av}(a_j)$ находятся путем деления $F(A)$ и $F(a_j)$ на 2^m-1. Диапазон возможных значений указанных характеристик определяется их максимальными и минимальными значениями:

$$\begin{aligned} \min\ F_{av}(a_j) &= \min\ F(a_j)/(2^m-1) = 1/(2^m-1), \\ \max\ F_{av}(a_j) &= \max\ F(a_j)/(2^m-1) = 1, \\ \min\ F_{av}(A) &= \min\ F(A)/(2^m-1) = 1, \\ \max\ F_{av}(A) &= \max\ F(A)/(2^m-1) = m-1/2+1/(2^{m+1}-2). \end{aligned} \quad (11)$$

Для ряда значений m предельные величины рассмотренных характеристик приведены в табл. 3.

Таблица 3

Значения переключательной активности для некоторых значений m

m	2	3	4	5	6	…	20	…	M
$\min F_{av}(a_j)$	0,333	0,142	0,066	0,032	0,016	…	0,000	…	$1/(2^m-1)$
$\max F_{av}(a_j)$	1	1	1	1	1	…	1	…	1
$\min F_{av}(A)$	1	1	1	1	1	…	1	…	1
$\max F_{av}(A)$	1,666	2,571	3,533	4,516	5,507	…	19,500	…	$m-1/2+1/(2^{m+1}-2)$

Анализ численных значений переключательной активности адресных последовательностей, представленных в табл. 3, показывает широкий диапазон возможных величин этой характеристики для произвольной последовательности. Отметим, что для ряда классических последовательностей значения переключательной активности были определены в работах [4, 20], однако

методика синтеза адресных последовательностей с требуемой переключательной активностью, в том числе и для предельных значений, отсутствует.

Синтез адресных последовательностей с заданной переключательной активностью. Эффективность тестовых последовательностей во многом определяется их свойствами, максимально адаптированными к объекту тестирования. Как отмечалось ранее, в случае адресных последовательностей весьма эффективными характеристиками являются как переключательная активность $F(a_j)$, $j \in \{0, 1, 2, \ldots, m-1\}$, определяющая количество переключений (изменений) j-го разряда a_j кода последовательности $A(n)$, так и интегральная переключательная активность $F(A)$. На практике чаще всего используются средние величины $F_{av}(A)$ и $F_{av}(a_j)$ указанных характеристик, которые принимают значения из заданных диапазонов, определенных минимальными и максимальными значениями (см. табл. 3).

Методика синтеза генератора последовательностей A(n) с заданной переключательной активностью ее $k \le m$ разрядов. Предположим, что необходимо синтезировать устройство для заданного значения m, формирующее последовательность $A(n) = a_{m-1}a_{m-2}\,a_{m-3}\ldots a_2a_1a_0$, $a_i \in \{0,1\}$, $i \in \{0, 1, 2, \ldots, m-1\}$ и $n \in \{0, 1, 2, \ldots, 2^m-1\}$, в которой для $k \le m$ разрядов $a_{\alpha 1}, a_{\alpha 2}, a_{\alpha 3}, \ldots, a_{\alpha k}$ определены конкретные значения средней переключательной активности $F_{av}(a_{\alpha 1})$, $F_{av}(a_{\alpha 2})$, $F_{av}(a_{\alpha 3})$, …, $F_{av}(a_{\alpha k})$. Отметим, что значения переключательных активностей $F(a_{\alpha 1})$, $F(a_{\alpha 2})$, $F(a_{\alpha 3})$, …, $F(a_{\alpha k})$ должны удовлетворять свойству 1.

Результатом синтеза будет являться устройство, структурная схема которого подробно описана в предыдущем разделе и показана на рис. 2. Большинство параметров и элементов устройства определяются величиной m, поэтому синтез устройства, по сути, будет заключаться в нахождении для него соответствующей порождающей матрицы V (3). Методика синтеза генератора последовательностей $A(n)$ с заданной переключательной активностью ее $k \le m$ разрядов включает следующие этапы:

1. На основании средних значений переключательной активности разрядов $F_{av}(a_{\alpha 1})$, $F_{av}(a_{\alpha 2})$, $F_{av}(a_{\alpha 3})$, …, $F_{av}(a_{\alpha k})$ вычисляются значения переключательных активностей $F(a_{\alpha 1})$, $F(a_{\alpha 2})$, $F(a_{\alpha 3})$, …, $F(a_{\alpha k})$. Результат умножения $F_{av}(a_{\alpha c})$, $c \in \{1, 2, 3, \ldots, k\}$, на 2^m-1 округляется до ближайшего целого значения, т. е. $F(a_{\alpha c}) = \mathrm{int}[F_{av}(a_{\alpha c})\cdot(2^m-1)]$. При округлении необходимо учитывать ограничение $F(a_{\alpha 1}) \ne F(a_{\alpha 2}) \ne F(a_{\alpha 3}) \ne \ldots \ne F(a_{\alpha k})$, вытекающее из свойства 1.

2. Заданная в десятичной системе счисления переключательная активность $F(a_{\alpha c})_{(10)}$, $c \in \{1, 2, 3, \ldots, k\}$, преобразуется в m-разрядный код, представленный в двоичной системе счисления $F(a_{\alpha c})_{(10)} = F(a_{\alpha c})_{(2)} = \beta_{\alpha c}(0)\cdot 2^{m-1} + \beta_{\alpha c}(1)\cdot 2^{m-2} + \beta_{\alpha c}(2)\cdot 2^{m-3} + \ldots + \beta_{\alpha c}(m-1)\cdot 2^0$. Отметим, что $\beta_{\alpha c}(0)$ представляет собой старший бит полученного двоичного кода, а сам код $\beta_{\alpha c}(0)\ \beta_{\alpha c}(1)\ \beta_{\alpha c}(2)\ \ldots\ \beta_{\alpha c}(m-1)$ однозначно определяет значения αc-го столбца порождающей матрицы V (3). Таким образом вычисляются значения всех $k \le m$ столбцов матрицы V, которые определяют переключательные активности $F(a_{\alpha 1})$, $F(a_{\alpha 2})$, $F(a_{\alpha 3})$, …, $F(a_{\alpha k})$.

3. Случайным образом (равновероятно и независимо) генерируются остальные столбцы двоичной матрицы $m \times m$, в которой столбцы $a_{\alpha 1}, a_{\alpha 2}, a_{\alpha 3}, \ldots, a_{\alpha k}$ принимают заданные значения.

4. Определяется ранг полученной матрицы. В случае максимального ранга данная матрица является искомой и используется для построения генератора адресных последовательностей (см. рис. 2). При получении матрицы с рангом, отличным от максимального, повторно выполняется этап 3.

Как было показано ранее (см. (6)), вероятность нахождения двоичной матрицы максимального ранга достаточно высока, однако в случае специфики требований к виду матрицы и невозможности нахождения матрицы максимального ранга следует незначительно изменить одну из величин переключательной активности.

Пример 1. Предположим, что необходимо синтезировать устройство для $m = 4$, формирующее последовательность $A(n) = a_3a_2a_1a_0$, в которой определены средние переключательные активности $F_{av}(a_2) = 0{,}20$ и $F_{av}(a_0) = 0{,}75$ для разрядов a_2 и a_0, значения которых соответствуют диапазону [0,066÷1] (см. табл. 3).

Для синтеза адресной последовательности согласно примеру 1 выполним следующие действия:

1. Получим значения $F(a_2)$ и $F(a_0)$ как $F(a_2) = \text{int}[F_{av}(a_2)\cdot(2^m-1)] = 0{,}2\cdot(2^4-1) = 3$ и $F(a_0) = \text{int}[F_{av}(a_0)\cdot(2^m-1)] = 0{,}75\cdot(2^4-1) = 11$. Отметим, что величина $F(a_2) \neq F(a_0)$. Это соответствует свойству 1.

2. Представим $F(a_2)$ и $F(a_0)$ в виде $F(a_2) = 3_{(10)} = 0011_{(2)}$ и $F(a_0) = 11_{(10)} = 1011_{(2)}$, тогда значения второго и нулевого столбцов матрицы V примут значения $\beta_2(0)\beta_2(1)\beta_2(2)\beta_2(3) = 0011$ и $\beta_0(0)\beta_0(1)\beta_0(2)\beta_0(3) = 1011$.

3. Третий и первый столбцы матрицы V сформируем случайным образом, исключая нулевые и повторяющиеся значения.

4. В результате проверки ранга матрицы получим результирующую матрицу, два варианта для которой (B1 и B2) приведены в табл. 4.

Таблица 4

Адресные последовательности для $m = 4$

V для $m = 4$	B1	B2	B3	B4
$\beta_3(0)\ \beta_2(0)\ \beta_1(0)\ \beta_0(0)$	0 0 0 1	1 0 1 1	1 1 1 0	1 1 1 0
$\beta_3(1)\ \beta_2(1)\ \beta_1(1)\ \beta_0(1)$	1 0 0 0	1 0 0 0	1 0 0 1	1 1 0 0
$\beta_3(2)\ \beta_2(2)\ \beta_1(2)\ \beta_0(2)$	0 1 0 1	0 1 0 1	0 0 1 1	1 0 0 1
$\beta_3(3)\ \beta_2(3)\ \beta_1(3)\ \beta_0(3)$	0 1 1 1	1 1 1 1	0 0 0 1	0 0 0 1
$A(0)$	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
$A(1) = A(0) \oplus \text{v}_0$	0 0 0 1	1 0 1 1	1 1 1 0	1 1 1 0
$A(2) = A(1) \oplus \text{v}_1$	1 0 0 1	0 0 1 1	0 1 1 1	0 0 1 0
$A(3) = A(2) \oplus \text{v}_0$	1 0 0 0	1 0 0 0	1 0 0 1	1 1 0 0
$A(4) = A(3) \oplus \text{v}_2$	1 1 0 1	1 1 0 1	1 0 1 0	0 1 0 1
$A(5) = A(4) \oplus \text{v}_0$	1 1 0 0	0 1 1 0	0 1 0 0	1 0 1 1
$A(6) = A(5) \oplus \text{v}_1$	0 1 0 0	1 1 1 0	1 1 0 1	0 1 1 1
$A(7) = A(6) \oplus \text{v}_0$	0 1 0 1	0 1 0 1	0 0 1 1	1 0 0 1
$A(8) = A(7) \oplus \text{v}_3$	0 0 1 0	1 0 1 0	0 0 1 0	1 0 0 0
$A(9) = A(8) \oplus \text{v}_0$	0 0 1 1	0 0 0 1	1 1 0 0	0 1 1 0
$A(10) = A(9) \oplus \text{v}_1$	1 0 1 1	1 0 0 1	0 1 0 1	1 0 1 0
$A(11) = A(10) \oplus \text{v}_0$	1 0 1 0	0 0 1 0	1 0 1 1	0 1 0 0
$A(12) = A(11) \oplus \text{v}_2$	1 1 1 1	0 1 1 1	1 0 0 0	1 1 0 1
$A(13) = A(12) \oplus \text{v}_0$	1 1 1 0	1 1 0 0	0 1 1 0	0 0 1 1
$A(14) = A(13) \oplus \text{v}_1$	0 1 1 0	0 1 0 0	1 1 1 1	1 1 1 1
$A(15) = A(14) \oplus \text{v}_0$	0 1 1 1	1 1 1 1	0 0 0 1	0 0 0 1

Как видно из табл. 4, для B1 и B2 $F(a_2) = 3$ и $F(a_2) = 11$, а $F(a_3)$ и $F(a_1)$ принимают значения 4 и 1 для B1 и 13 и 9 для B2. Для обоих вариантов интегральная метрика $F_{av}(A)$, характеризующая последовательности, равняется 1,26 и 2,4 соответственно.

Методика синтеза генератора последовательностей $A(n)$ с заданной переключательной активностью $F_{av}(A)$. Данная методика, так же, как и методика синтеза генератора последовательностей $A(n)$ с заданной переключательной активностью ее $k \leq m$ разрядов, будет заключаться в нахождении соответствующей порождающей матрицы V (3). Для этого необходимо сформировать произвольную матрицу максимального ранга с заданными ограничениями. Определим эти ограничения, для чего переключательную активность $F(A) = \text{int}[F_{av}(a_0)\cdot(2^m-1)]$ запишем в виде выражения

$$F(A) = w(\text{v}_0)\cdot 2^{m-1} + w(\text{v}_1)\cdot 2^{m-2} + w(\text{v}_2)\cdot 2^{m-3} + \ldots + w(\text{v}_{m-1})\cdot 2^0. \qquad (12)$$

Значение $w(\text{v}_i)$ представляет собой вес Хэмминга $w(\text{v}_i)$ двоичного вектора $\text{v}_i = \beta_{m-1}(i)\ \beta_{m-2}(i)\ldots \beta_0(i)$, $i = \overline{0, m-1}$. Следует отметить, что подобное разложение $F(A)$ возможно только для его величин, удовлетворяющих неравенству $\min F(A) \leq F(A) \leq \max F(A)$.

Для случая квадратной матрицы $m \times m$, состоящей из m линейно независимых двоичных векторов, величина $w(\mathrm{v}_i)$ принимает значения от единицы до m, т. е. каждая строка такой матрицы должна содержать от одного единичного значения до m единичных значений, а их конкретное количество зависит от заданной величины $F(A)$. Разложение величины $F(A)$ в виде (12) можно интерпретировать как ее представление в m-ичной смешанной системе счисления, в которой веса разрядов представлены в виде степеней двойки от 2^0 до 2^{m-1}. Методика синтеза генератора последовательностей $A(n)$ с заданной переключательной активностью $F_{av}(A)$ включает следующие этапы:

1. На основании среднего значения переключательной активности $F_{av}(A)$ вычисляется значение переключательной активности $F(A) = \mathrm{int}[F_{av}(A)\cdot(2^m-1)]$.

2. Для получения значений $w(\mathrm{v}_i)$, обеспечивающих согласно (12) требуемую величину $F(A)$, определяется разность $F(A) - \min F(A) = F(A) - 2^m+1$.

3. Проверяется условие $F(A) - 2^m+1 = 0$, выполнение которого означает, что $F(A)$ принимает минимально возможное значение. Как указывалось в работе [4], оно достигается заданием матрицы V, в которой все строки $\mathrm{v}_i = \beta_{m-1}(i)\ \beta_{m-2}(i)\ \ldots\ \beta_0(i)$, $i = \overline{0, m-1}$, содержат по одной единице. Другими словами, вес Хэмминга $w(\mathrm{v}_i)$ двоичного вектора v_i равняется единице, что свидетельствует о существовании $m!$ подобных матриц, каждая из которых может быть матрицей V. Соответственно, случайным образом формируются m m-разрядных неповторяющихся векторов, каждый из которых содержит по одной единице. В результате будет получена искомая матрица V.

Для $F(A)$, отличных от минимального значения, необходимо определить значения весов $w(\mathrm{v}_i)$, удовлетворяющих неравенству $1 \le w(\mathrm{v}_i) \le m$.

4. При условии, что $F(A) - 2^m+1 \ne 0$, определяются величины $w(\mathrm{v}_i) - 1$ путем последовательного выполнения операций деления. Первоначально величина $F(A) - 2^m+1$ делится на 2^{m-1}. Полученное частное и будет являться значением $w(\mathrm{v}_0) - 1$, что следует из разложения (12). Затем остаток от предыдущей операции делится на 2^{m-2}. В результате имеем остаток, определяющий $w(\mathrm{v}_1)-1$, и таким образом получаем все значения $w(\mathrm{v}_i) - 1$. Основываясь на значениях $w(\mathrm{v}_i) - 1$, легко определить веса $w(\mathrm{v}_i)$ строк v_i порождающей матрицы V (3), которые и являются входными данными для синтеза произвольной, сформированной случайным образом матрицы с фиксированными весами Хэмминга. Конкретное значение $w(\mathrm{v}_i)$ для строки v_i определяет формирование случайным образом m-разрядного двоичного вектора, содержащего $w(\mathrm{v}_i)$ единиц и $m - w(\mathrm{v}_i)$ нулей.

5. Проверяется ранг построенной таким образом матрицы. Если он максимален, искомая матрица V (3) может быть использована для генерирования последовательности $A(n)$ с заданной переключательной активностью $F_{av}(A)$. Как было показано ранее (см. (6)), в общем случае вероятность того, что ранг матрицы максимален, достаточно велика и приблизительно равна 0,288.

При получении матрицы с рангом, отличным от максимального, повторно выполняется этап 4 в части формирования случайным образом матрицы с фиксированными весами Хэмминга. Каждая строка этой матрицы представляет собой случайный вектор с заданным весом $w(\mathrm{v}_i)$. Затем опять выполняется этап 5.

Пример 2. Необходимо синтезировать устройство для $m = 4$, формирующее последовательность $A(n) = a_3a_2a_1a_0$ с заданной переключательной активностью $F_{av}(A) = 2{,}45$.

Для синтеза адресной последовательности согласно примеру 2 выполним следующие действия:

1. На основании среднего значения переключательной активности $F_{av}(A) = 2{,}45$ вычислим значение переключательной активности $F(A) = \mathrm{int}[2{,}45\cdot 15] = 37$.

2. Определим разность $F(A) - \min F(A) = 37 - 15 = 22$.

3. Значение разности $F(A) - \min F(A) = 22 \ne 0$.

4. В результате первой операции деления $F(A) - \min F(A) = 22$ на $2^{m-1} = 8$ получим частное, равное 2. Соответственно, $w(\mathrm{v}_0)-1 = 2$, а $w(\mathrm{v}_0) = 3$. Остаток от предыдущей операции, равный шести, делится на $2^{m-2} = 4$. В результате частное, равное единице, определяет вес $w(\mathrm{v}_1) = 2$. Последующие шаги формируют значения $w(\mathrm{v}_2) = 2$ и $w(\mathrm{v}_3) = 1$. Следовательно, десятичное значение $F(A) = 37$ представляется в виде разложения $F(A) = 37 = 3\cdot 8 + 2\cdot 4 + 2\cdot 2 + 1\cdot 1$ (12). Значения цифр этого разложения $w(\mathrm{v}_3) = 3$, $w(\mathrm{v}_1) = 2$, $w(\mathrm{v}_2) = 2$ и $w(\mathrm{v}_0) = 1$ используются в качестве ограничений на формируемую порождающую матрицу V, в которой первая строка должна содержать три единицы, вторая и третья строки – по две единицы и четвертая строка – одну единицу.

Любая матрица, удовлетворяющая сформулированным выше условиям, позволит сгенерировать адресную последовательность $A(n)$ с заданной переключательной активностью $F_{av}(A)$. Варианты B3 и B4 последовательностей с переключательной активностью $F_{av}(A) = 2{,}45$ приведены в табл. 4.

Пример 3. Необходимо синтезировать устройство для $m = 4$, генерирующее последовательность $A(n) = a_3a_2a_1a_0$, для которой в каждом такте формируются два изменения значений в следующем коде последовательности. Подобную последовательность можно охарактеризовать как «двойной Грей». Формально такая последовательность описывается средней переключательной активностью $F_{av}(A) = 2$. Отметим, что последовательность Грея имеет значение $F_{av}(A) = 1$.

Как и в примере 2, последовательно применив рассмотренную методику синтеза, получим значения цифр $w(v_3) = 2$, $w(v_2) = 2$, $w(v_1) = 2$ и $w(v_0) = 2$ разложения (12). Однако попытка нахождения соответствующей матрицы максимального ранга для $m = 4$, у которой все строки содержат по две единицы, не дает положительного результата. Это связано с тем, что в данном случае требование о линейной независимости векторов v_3, v_2, v_1 и v_0 и значения их весов $w(v_3)$, $w(v_1)$, $w(v_2)$ и $w(v_0)$ несовместимы. Очевидно, что существует достаточно много подобных ситуаций [22, 23]. Например, они имеют место для случая последовательности анти-Грея, которую можно построить только для четных значений m [4]. Решение задачи, сформулированной в примере 3, возможно путем коррекции значения $F(A)$, которое в этом случае равняется 30.

В общем случае для обеспечения заданного значения $F_{av}(A)$ с минимальной погрешностью первоначально изменяют значение $F(A)$ на минимальную величину (+1 или −1) и переходят к поиску соответствующей порождающей матрицы V (3). В случае отрицательного исхода значение отклонения величины $F(A)$ от требуемого $\mathrm{int}[F_{av}(A) \cdot (2^m - 1)]$ увеличивается.

Для примера 3 уменьшение $F(A)$ на единицу позволяет получить матрицу

$$V = \begin{vmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{vmatrix}. \qquad (13)$$

Матрица (13) дает возможность сгенерировать адресную последовательность, для которой $F(A) = 29$, а $F_{av}(A) = 1{,}933\ldots$, что незначительно отличается от требуемого значения $F_{av}(A) = 2$. Для реальных значений $m > 20$ погрешность отклонения и полученного значения переключательной активности от заданной величины несущественна.

Применение адресных последовательностей. Очевидной областью применения рассмотренных методик синтеза адресных последовательностей являются встроенные средства самотестирования запоминающих устройств (Memory Built-In Self-Test, MBIST) современных вычислительных систем. При реализации MBIST аппаратные затраты на генератор адресных последовательностей составляют до 30 % общих затрат на встроенные средства самотестирования [24–26]. В то же время набор адресных последовательностей в приведенных в литературе архитектурах MBIST весьма ограничен, что обусловлено в первую очередь ограничениями на аппаратурные затраты. Набор таких последовательностей включает: пересчетные последовательности (Linear Counting Method); последовательности Грея (Gray Code Counting Method); последовательности с максимальной переключательной активностью (Address Complement Counting Method); последовательности с расстоянием Хэмминга, равным единице для всех пар адресов (2^i Counting Method), и др. [24].

Все перечисленные последовательности реализуются рассмотренным в настоящей работе генератором адресных последовательностей (см. рис. 2). Вид формируемой последовательности задается порождающей матрицей V. Количество адресных последовательностей, формируемых генератором для реальных значений m, достигает астрономических значений, равных более 25 % от общего числа 2^{m^2} возможных двоичных матриц (6). При этом в отличие от известных решений [24, 25], когда MBIST реализует одну последовательность из семейства последовательностей, генератор адресных последовательностей позволяет формировать либо все семейство последовательностей, либо их подмножество. Например, в случае последовательности Грея,

задавая одну из $m!$ порождающих матриц V (3), содержащих по одной единице в строке и столбце, возможно формирование $m!$ последовательностей Грея. В качестве еще одного примера можно привести широкие возможности для формирования адресных последовательностей типа 2^i Counting Method, для которых обеспечивается не только максимальная переключательная активность i-го разряда адреса, но и произвольные значения активности остальных разрядов адреса. Такие адресные последовательности эффективны для обнаружения неисправностей, связанных с временными параметрами запоминающих устройств (Speed-Related Faults) [24, 25].

Изменение переключательной активности адресов запоминающих устройств позволяет обнаруживать неисправности как самой матрицы запоминающих элементов, так и ее электронного обрамления за счет изменений потребляемой энергии (power surge), временных задержек (delay) и шумовых эффектов, связанных с переключением элементов дешифратора адресов (noise) [24–26].

Средние значения переключательной активности $F_{av}(A)$ и $F_{av}(a_j)$ можно интерпретировать как средние значения расстояния Хэмминга, которое широко применяется для построения управляемых вероятностных тестовых последовательностей [27, 28]. Изменение значений указанных характеристик позволяет строить управляемые вероятностные тесты с заданными величинами расстояния Хэмминга.

Основные характеристики генератора адресных последовательностей исследовались с помощью его реализации на FPGA Intel Cyclone *V* (5CSXFC6D6F31C8ES) (рис. 3). Схема FPGA состоит из 41 910 адаптивных логических модулей (ALMs) и 553 блоков памяти SRAM (M10k). Реализация генератора для $m = 8$ потребовала 17 модулей ALMs и один блок встроенной памяти M10k, что составляет менее 1 % площади кристалла FPGA.

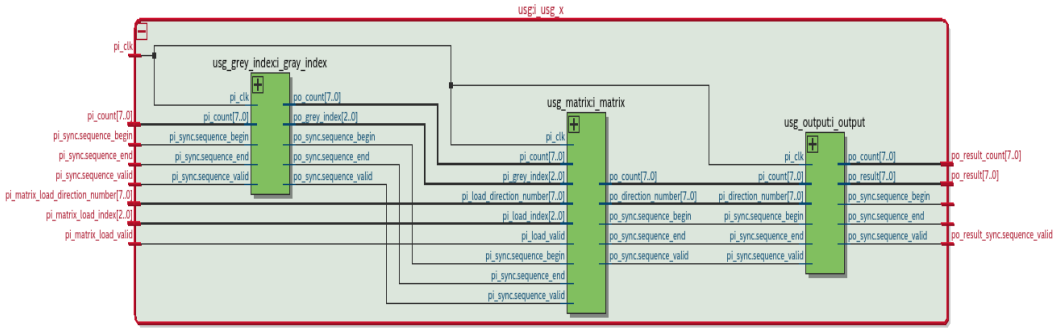


Рис. 3. Реализация генератора адресных последовательностей на FPGA

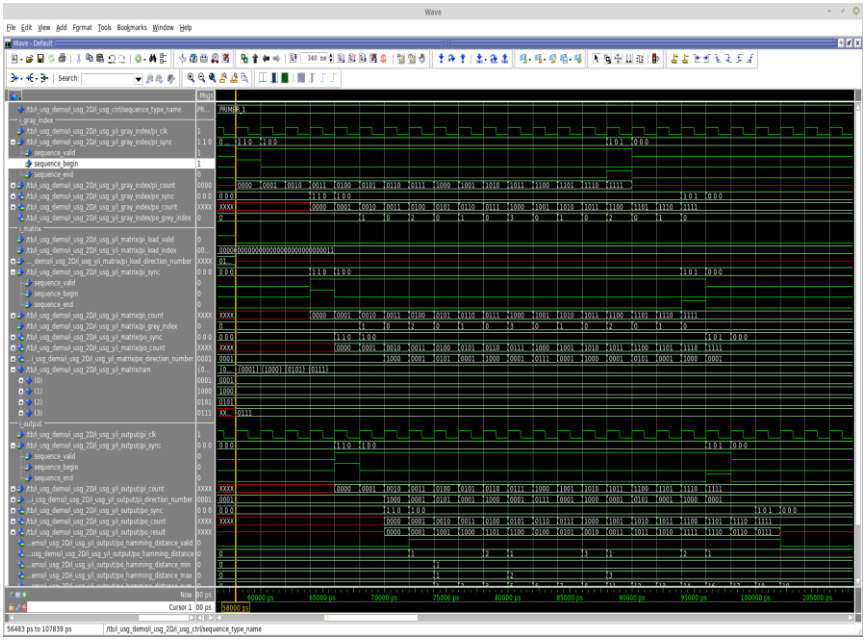


Рис. 4. Расшифровка сигналов и временная диаграмма работы генератора

Реализация генератора адресных последовательностей на рис. 3 идентична структуре, изображенной на рис. 2. Входные, выходные и промежуточные полюса реализованного устройства и его детализированной структуры, а также их описания находятся в полном соответствии. Моделирование работы генератора адресных последовательностей показано на рис. 4.

Оценка энергопотребления схемы формирования адресов (см. рис. 3) проводилась с использованием Quartus Prime Version 19.1.0 Build 670 09/22/2019 SJ Lite Edition. Результаты анализа свидетельствуют о минимальном потреблении мощности предлагаемым устройством: Total Thermal Power Dissipation – 463,45 Вт, Core Dynamic Thermal Power Dissipation –14,63 Вт, Core Static Thermal Power Dissipation – 415,27 Вт, I/O Thermal Power Dissipation – 33,56 Вт.

Временные параметры генератора соответствуют максимально возможным временным параметрам FPGA.

Заключение. Использование модифицированной математической модели формирования последовательностей Соболя позволило расширить возможности генератора адресных последовательностей в части значительного увеличения количества видов подобных последовательностей. В работе изложен метод построения генератора адресных последовательностей с заданными значениями переключательной активности как формируемых кодов адресов, так и активности их разрядов. Сущность метода состоит в синтезе требуемой порождающей матрицы максимального ранга, обеспечивающей заданные значения переключательной активности. Показаны ограничения предложенных методик, связанные с возможными противоречивыми требованиями к значениям весов строк матрицы и их линейной независимости. Описаны примеры применения подобных последовательностей построения встроенных средств самотестирования запоминающих устройств и синтеза управляемых вероятностных тестов. Представлена практическая реализация генератора адресных последовательностей, показывающая реализуемость такого устройства с минимальными аппаратными затратами и максимальным быстродействием.

Список использованных источников

1. Bushnell, M. L. Essentials of Electronic Testing for Digital, Memory & Mixed-Signal VLSI Circuits / M. L. Bushnell, V. D. Agrawal. – N. Y. : Kluwer Academic Publishers, 2000. – 690 p.

2. Wang, L.-T. VLSI Test Principles and Architectures: Design for Testability / L.-T. Wang, C.-W. Wu, X. Wen. – Amsterdam : Elsevier, 2006. – 808 p.

3. Ярмолик, С. В. Многократные неразрушающие маршевые тесты с изменяемыми адресными последовательностями / С. В. Ярмолик, В. Н. Ярмолик // Автоматика и телемеханика. – 2007. – № 4. – С. 126–137.

4. Ярмолик, В. Н. Адресные последовательности для многократного тестирования ОЗУ / В. Н. Ярмолик, С. В. Ярмолик // Информатика. – 2014. – № 2(42). – С. 124–136.

5. Sharma, A. K. Semiconductor Memories: Technology, Testing, and Reliability / A. K. Sharma. – London : John Wiley & Sons, 2002. – 480 p.

6. Угрюмов, Е. П. Цифровая схемотехника / Е. П. Угрюмов. – 3-е изд., перераб. и доп. – СПб. : БХВ-Петербург, 2010. – 816 с.

7. Pomeranz, I. An adjacent switching activity metric under functional broadside tests / I. Pomeranz // IEEE Transaction on Computers. – 2013. – Vol. 62, no. 4. – P. 404–410.

8. Pomeranz, I. Switching activity as a test compaction heuristic for transition faults / I. Pomeranz, S. M. Reddy // IEEE Transaction VLSI Systems. – 2010. – Vol. 18, no. 9. – P. 1357–1361.

9. Pedram, M. Power minimization in IC design: principles and applications / M. Pedram // ACM Transactions Design Automation Electronic Systems. – 1996. – Vol. 1. – P. 3–56.

10. Черемисинова, Л. Д. Оптимизация скобочных представлений булевых функций с учетом энергопотребления / Л. Д. Черемисинова, Н. А. Кириенко // Информатика. – 2011. – № 3(31). – С. 77–87.

11. Мурашко, И. А. Встроенное самотестирование. Методы минимизации энергопотребления / И. А. Мурашко, В. Н. Ярмолик. – Saarbrücken : LAP Lambert Academic Publishing, 2012. – 348 с.

12. A test vector ordering technique for switching activity reduction during test operation / P. Girard [et al.] // Proc. Ninth Great Lakes Symp. on VLSI, Ypsilanti, MI, USA, 1999. – Ypsilanti, 1999. – P. 24–27.

13. Кириенко, Н. А. Оптимизация многоуровневых представлений логических схем для сокращения площади кристалла СБИС и энергопотребления / Н. А. Кириенко, Д. И. Черемисинов, Л. Д. Черемисинова // Вес. Нац. акад. навук Беларусі. Сер. фіз.-мат. навук. – 2015. – № 2. – С. 103–111.

14. Wang, S. An automatic test pattern generator for minimizing switching activity during scan testing activity / S. Wang, S. K. Gupta // IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. – 2002. – Vol. 21, no. 8. – P. 954–968.

15. On low-capture-power test generation for scan testing / X. Wen [et al.] // Proc. VLSI Test Symp., Palm Springs, California, USA, 2005. – Palm Springs, 2005. – P. 265–270.

16. Yarmolik, V. N. Modified gray and counter sequences for memory test address generation / V. N. Yarmolik, S. V. Yarmolik // Proc. of the 13th Intern. Conf. MIXDES Design of Integrated Circuits and Systems, Gdynia, Poland, 2006. – Gdynia, 2006. – P. 572–576.

17. Ярмолик, В. Н. Контроль и диагностика вычислительных систем / В. Н. Ярмолик. – Минск : Бестпринт, 2019. – 387 с.

18. Соболь, И. М. Точки, равномерно заполняющие многомерный куб / И. М. Соболь. – М. : Знание, 1985. – 32 с.

19. Антонов, И. А. Экономичный способ вычисления $ЛП_\tau$-последовательностей / И. А. Антонов, В. М. Салеев // Журн. вычисл. матем. и матем. физ. – 1979. – Т. 19, № 1. – С. 243–245.

20. Ярмолик, С. В. Квазислучайное тестирование вычислительных систем / С. В. Ярмолик, В. Н. Ярмолик // Информатика. – 2013. – № 3(39). – С. 65–81.

21. Savage, C. A survey of combinatorial Gray code / C. Savage // SIAM Review. – 1997. – Vol. 39, no. 4. – P. 605–629.

22. Boyd, S. Introduction to Applied Linear Algebra: Vectors, Matrices, and Least Squares / S. Boyd. – Cambridge : University Printing House, 2018. – 463 p.

23. The rank of random binary matrices and distributed storage applications / P. Ferreira [et al.] // IEEE Communication Letters. – 2013. – Vol. 17, no. 1. – P. 151–154.

24. Goor, A. J. Optimizing memory BIST Address Generator implementations / A. J. Goor, H. Kukner, S. Hamdioui // Proc. of 2011 6th Intern. Conf. on Design & Technology of Integrated Systems in Nanoscale Era (DTIS), Athens, Greece, 2011. – Athens, 2011. – P. 572–576.

25. Full-speed field-programmable memory BIST architecture / X. Du [et al.] // Proc. of IEEE Intern. Test Conf., Austin, TX, USA, 2005. – Austin, 2005. – P. 1173–1182.

26. Aswin, A. M. Implementation and validation of memory built in self-test (MBIST) – survey / A. M. Aswin, S. S. Ganesh // Intern. J. of Mechanical Engineering and Technology (IJMET). – 2019. – Vol. 10, no. 3. – P. 153–160.

27. Mrozek, I. Iterative antirandom testing / I. Mrozek, V. N. Yarmolik // J. of Electronic Testing: Theory and Applications (JETTA). – 2012. – Vol. 9, no. 3. – P. 251–266.

28. Mrozek, I. Antirandom test vectors for BIST in Hardware / Software systems / I. Mrozek, V. N. Yarmolik // Fundamenta Informaticae. – 2012. – No. 119. – P. 1–23.

References

1. Bushnell M. L., Agrawal V. D. *Essentials of Electronic Testing for Digital, Memory & Mixed-Signal VLSI Circuits*. New York, Kluwer Academic Publishers, 2000, 690 p.

2. Wang L.-T., Wu C.-W., Wen X. *VLSI Test Principles and Architectures: Design for Testability*. Amsterdam, Elsevier, 2006, 808 p.

3. Yarmolik S. V., Yarmolik V. N. Mnogokratnue nerazrushayuschie marshevue testu s izmenyaemumi adresnumi posledovatel'nostymi [Multiple non-destructive marching tests with variable address sequences]. Avtomatika i telemehanika [*Automation and Remote*], 2007, no. 4, pp. 126–137 (in Russian).

4. Yarmolik V. N., Yarmolik S. V. Adresnue posledovatel'nosti dlya mnogokratnogo testirovaniya OZU [Address sequences for repeated testing of RAM]. Informatika [*Informatics*], 2014, no. 2(42), pp. 124–136 (in Russian).

5. Sharma A. K. *Semiconductor Memories: Technology, Testing, and Reliability*. London, John Wiley & Sons, 2002, 480 p.

6. Ugryumov E. P. Cifrovaya shemotehnika. *Digital Circuitry*. Saint Petersburg, BHV-Peterburg, 2010, 816 p. (in Russian).

7. Pomeranz I. An adjacent switching activity metric under functional broadside tests. *IEEE Transaction on Computers*, 2013, vol. 62, no. 4, pp. 404–410.

8. Pomeranz I., Reddy S. M. Switching activity as a test compaction heuristic for transition faults. *IEEE Transaction VLSI Systems*, 2010, vol. 18, no. 9, pp. 1357–1361.

9. Pedram M. Power minimization in IC design: principles and applications. *ACM Transactions Design Automation Electronic Systems*, 1996, vol. 1, pp. 3–56.

10. Cheremisinova L. D., Kirienko N. A. Optimizaciya skobochnuh predstavlenii bulevuh phunkcii s uchetom energopotrebleniya [Optimization of bracket representations of Boolean functions taking into account energy consumption]. Informatika [*Informatics*], 2011, no. 3(31), pp. 77–87 (in Russian).

11. Murashko I. A., Yarmolik V. N. Vstroennoe samotestirovanie. Metodu minimizacii energopotrebleniya. *Built-in Self Test. Methods to Minimize Power Consumption*. Saarbrücken, LAP Lambert Academic Publishing, 2012, 348 p. (in Russian).

12. Girard P., Guiller L., Landrault C., Pravossoudovitch S. A test vector ordering technique for switching activity reduction during test operation. *Proceedings Ninth Great Lakes Symposium on VLSI, Ypsilanti, MI, USA, 1999*. Ypsilanti, 1999, pp. 24–27.

13. Kirienko N. A., Cheremisinov D. I., Cheremisinova L. D. Optimizaciya mnogourovnevuh predstavlenii logicheskih shem glya sokrascheniya ploschadi kristala SBIS i energopotrebleniya [Optimization of multi-level representations of logic circuits to reduce VLSI chip area and power consumption]. Vestsi Natsyyanal'nai akademii navuk Belarusi. Seryya fizika-matematychnykh navuk [*Proceedings of the National Academy of Sciences of Belarus. Physics and Mathematics series*], 2015, no. 2, pp. 103–111 (in Russian).

14. Wang S., Gupta S. K. An automatic test pattern generator for minimizing switching activity during scan testing activity. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2002, vol. 21, no. 8, pp. 954–968.

15. Wen X., Yamashita Y., Kajihara S., Wang L.-T., Saluja K. K., Kinoshita K. On low-capture-power test generation for scan testing. *Proceedings VLSI Test Symposium, Palm Springs, California, USA, 2005*. Palm Springs, 2005, pp. 265–270.

16. Yarmolik V. N., Yarmolik S. V. Modified gray and counter sequences for memory test address generation. *Proceedings of the 13th International Conference MIXDES Design of Integrated Circuits and Systems, Gdynia, Poland, 2006*. Gdynia, 2006, pp. 572–576.

17. Yarmolik V. N. Kontrol' i diagnostika vuchislitel'nuh system. *Monitoring and Diagnostics of Computer Systems*. Minsk, Bestprint, 2019, 387 p. (in Russian).

18. Sobol' I. M. Tochki, ravnomerno zapolnyayuschie mnogomernui kub. *Points Uniformly Filling a Multidimensional Cube*. Moscow, Znanie, 1985, 32 p. (in Russian).

19. Antonov I. A., Saleev V. M. Ekonomichnui sposob vuchisleniya LP_{τ}-posledovatel'nostei [An economical way to calculate LPτ sequences]. Zhurnal vychislitel'noj matematiki i matematicheskoj fiziki [*Journal of Computational Mathematics and Mathematical Physics*], 1979, vol. 19, no. 1, pp. 243–245 (in Russian).

20. Yarmolik S. V., Yarmolik V. N. Kvazisluchainoe testirovanie vuchislitel'nuh system [Quasi-random testing of computing systems]. Informatika [*Informatics*], 2013, no. 3(39), pp. 65–81 (in Russian).

21. Savage C. A survey of combinatorial Gray code. *SIAM Review*, 1997, vol. 39, no. 4, pp. 605–629.

22. Boyd S. *Introduction to Applied Linear Algebra: Vectors, Matrices, and Least Squares*. Cambridge, University Printing House, 2018, 463 p.

23. Ferreira P., Jesus B., Vieira J., Pinho A. J. The rank of random binary matrices and distributed storage applications. *IEEE Communication Letters*, 2013, vol. 17, no. 1, pp. 151–154.

24. Goor A. J., Kukner H., Hamdioui S. Optimizing memory BIST Address Generator implementations. *Proceedings of 2011 6th International Conference on Design & Technology of Integrated Systems in Nanoscale Era (DTIS), Athens, Greece, 2011*. Athens, 2011, pp. 572–576.

25. Du X., Mukherjee N., Cheng W. T., Reddy S. M. Full-speed field-programmable memory BIST architecture. *Proceedings of IEEE International Test Conference, Austin, TX, USA, 2005*. Austin, 2005, pp. 1173–1182.

26. Aswin A. M., Ganesh S. S. Implementation and validation of memory built in self-test (MBIST) – survey. *International Journal of Mechanical Engineering and Technology (IJMET)*, 2019, vol. 10, no. 3, pp. 153–160.

27. Mrozek I., Yarmolik V. N. Iterative antirandom testing. *Journal of Electronic Testing: Theory and Applications (JETTA)*, 2012, vol. 9, no. 3, pp. 251–266.

28. Mrozek I., Yarmolik V. N. Antirandom test vectors for BIST in Hardware / Software systems. *Fundamenta Informaticae*, 2012, no. 119, pp. 1–23.

Информация об авторах

Ярмолик Вячеслав Николаевич, доктор технических наук, профессор, Белорусский государственный университет радиоэлектроники и информатики, Минск, Беларусь.
E-mail: yarmolik10ru@yahoo.com

Шевченко Николай Алексеевич, студент, член научного сообщества Weird Science Club, гимназия имени Лихтенберга, Дармштадт, Германия.
E-mail: nik.sh.de@gmail.com

Information about the authors

Vyacheslav N. Yarmolik, Dr. Sci. (Eng.), Professor, Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus.
E-mail: yarmolik10ru@yahoo.com

Nikolai A. Shevchenko, Student, Member of the Scientific Community Weird Science Club, Lichtenberg Gymnasium, Darmstadt, Germany.
E-mail: nik.sh.de@gmail.com

ISSN 1816-0301 (Print)
ISSN 2617-6963 (Online)

УДК 519.714
https://doi.org/10.37661/1816-0301-2020-17-1-63-77

Поступила в редакцию 05.11.2019
Received 05.11.2019

Принята к публикации 19.12.2019
Accepted 19.12.2019

Выделение подсистем связанных функций из многоуровневого представления системы булевых функций

П. Н. Бибило✉, А. М. Позняк

Объединенный институт проблем информатики
Национальной академии наук Беларуси, Минск, Беларусь
✉*E-mail: bibilo@newman.bas-net.by*

Аннотация. Одним из направлений логической оптимизации многоуровневых представлений систем булевых функций являются методы, основанные на выделении подсистем функций, которые имеют одинаковые части в областях определения функций выделенных подсистем. Такие подсистемы называются связанными. Связанность функций приводит к появлению большого числа одинаковых структурных частей (конъюнкций, алгебраических выражений, подфункций и др.) в оптимизированных формах представления функций, по которым строятся в дальнейшем комбинационные логические схемы. Чем сильнее связаны функции выделенной подсистемы, тем скорее можно ожидать, что в представлениях функций данной подсистемы будет больше одинаковых подвыражений и синтезированные логические схемы будут иметь меньшую сложность.
Описываются программно реализованные алгоритмы выделения подсистем связанных функций из BDD-представления системы булевых функций на основе введенных численных оценок связанности BDD-представлений функций. Связанность заключается в наличии одинаковых частей в областях единичных значений функций системы либо одинаковых уравнений в BDD-представлениях. Такие представления являются компактными формами задания функций и получаются в результате разложения Шеннона функций исходной системы (и получающихся в результате разложения подфункций) по всем своим переменным. Проведенные эксперименты показывают эффективность применения предложенных алгоритмов и программ при синтезе логических схем из библиотечных логических элементов.

Ключевые слова: булева функция, разложение Шеннона, BDD-представление, дизъюнктивная нормальная форма, синтез логических схем

Для цитирования. Бибило, П. Н. Выделение подсистем связанных функций из многоуровневого представления системы булевых функций / П. Н. Бибило, А. М. Позняк // Информатика. – 2020. − Т. 17, № 1. – С. 63–77. https://doi.org/10.37661/1816-0301-2020-17-1-63-77

The search for subsystems of related functions from multilevel representation of systems of Boolean functions

Petr N. Bibilo✉, Andrei M. Pazniak

The United Institute of Informatics Problems of the National Academy
of Sciences of Belarus, Minsk, Belarus
✉*E-mail: bibilo@newman.bas-net.by*

Abstract. One of the directions of logical optimization of multilevel representations of systems of Boolean functions is the methods based on the search of subsystems of functions that have the same parts in the domains of functions of selected subsystems. Such subsystems are called related. The good relationship of functions leads to the appearance of a large number of identical structural parts (conjunctions, algebraic expressions, subfunctions, etc.) in optimized forms of representation of functions which are used in the construction of combinational logic circuits. The more the functions of the selected subsystem are related, the sooner it is expected that in the representations of the functions of this subsystem will be more identical subexpressions and synthesized logic circuits will have less complexity.

We describe software-implemented algorithms for extracting subsystems of related functions from a BDD representation of a system of Boolean functions based on introduced numerical estimates of the relationship of BDD representations of functions. The relationship of Boolean functions is the presence of Boolean vectors, where the functions take the value as one, or of the same equations in BDD representations. BDD representations of Boolean functions are compact forms defining functions and are constructed as the result of Shannon decomposition of the functions of the original system (resulting from the decomposition of subfunctions) by all variables, which the functions of the original system depend on. The experiments show the effectiveness of proposed algorithms and programs in the synthesis of logic circuits from logic elements library.

Keywords: Boolean function, Shannon decomposition, BDD representation, disjunctive normal form, logic synthesis

For citation. Bibilo P. N., Pazniak A. M. The search for subsystems of related functions from multilevel representation of systems of Boolean functions. *Informatics*, 2020, vol. 17, no. 1, pp. 63−77 (in Russian). https://doi.org/10.37661/1816-0301-2020-17-1-63-77

Введение. Синтез комбинационных схем из библиотечных элементов выполняется по оптимизированным двухуровневым либо многоуровневым представлениям систем булевых функций. Двухуровневыми (И-ИЛИ) представлениями называют в литературе [1–3] представления функций в виде дизъюнктивных нормальных форм (ДНФ), многоуровневыми – различные формы функциональных разложений [1, 4]. Логическая оптимизация двухуровневых представлений, часто называемая также совместной минимизацией систем булевых функций в классе ДНФ, основывается на поиске одинаковых элементарных конъюнкций, входящих в ДНФ различных функций системы, т. е. выделении одинаковых частей в алгебраических представлениях функций.

Логическая минимизация функциональных разложений по подмножествам переменных при решении задач декомпозиции систем функций [4] основывается на поиске одинаковых подфункций, входящих в разложения исходных функций системы, либо подфункций, полученных в процессе разложения. Среди функциональных разложений по одной переменной широкое применение нашли разложения Шеннона, графические представления которых называются BDD (от англ. Binary Decision Diagram, диаграмма двоичного выбора) [5–9]. В русскоязычной литературе BDD называют также диаграммами двоичных решений, бинарными диаграммами решений, двоичными решающими диаграммами и т. д. Представления булевых функций в виде BDD соответствуют многоуровневым представлениям на базе разложения Шеннона по всем переменным, от которых зависят функции системы [9], и поиска одинаковых подфункций (коэффициентов разложений), получаемых в процессе разложения. В работе [10] предложено при построении BDD-представлений систем функций находить равные и взаимно инверсные подфункции, что позволяет получать BDDI-представления (BDDI – Binary Decision Diagram withInverse cofactors), которые являются более компактными по сравнению с BDD-представлениями, основывавными на поиске только одинаковых (равных) подфункций.

Еще одним направлением логической оптимизации многоуровневых представлений систем функций являются методы, основанные на выделении подсистем функций, которые имеют одинаковые части в областях определения функций системы. В работе [11] такие подсистемы называются связанными. «Хорошая» связанность функций существенно влияет на появление одинаковых структурных частей (конъюнкций, алгебраических выражений, подфункций и т. д.) в оптимизированных двухуровневых либо многоуровневых формах представления функций, по которым и строятся комбинационные схемы. Чем сильнее связанность функций, тем скорее можно ожидать, что в их представлениях будет больше одинаковых подвыражений и синтезированные схемы будут менее сложными. По сути, выделение подсистем связанных функций является одним из приемов предварительной логической оптимизации многоуровневых представлений систем функций.

В настоящей статье формулируются понятия связанности булевых функций по их характеристическим множествам (областям единичных значений функций) либо по уравнениям в BDD-представлениях и предлагаются алгоритмы выделения связанных подсистем функций из BDD-представления системы функций. Проведенные эксперименты по выделению связанных подсистем функций показали, что данную процедуру целесообразно выполнять перед

BDDI-оптимизацией, являющейся эффективным методом логической минимизации при синтезе логических схем из библиотечных элементов. Выделение связанных функций позволяет объединить в одну подсистему те функции, которые целесообразно минимизировать на основе BDD либо BDDI-представления данной подсистемы.

Основные определения и формы задания систем булевых функций. Пусть задана система $\boldsymbol{f}(\boldsymbol{x}) = (f^1(\boldsymbol{x}), \ldots, f^m(\boldsymbol{x}))$ булевых функций, через $\boldsymbol{x}$ обозначен вектор $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ аргументов $x_1, x_2, \ldots, x_n$. Обозначим через V^x булево пространство, построенное над переменными булева вектора $\boldsymbol{x} = (x_1, \ldots, x_n)$. Элементами пространства V^x являются n-компонентные наборы (векторы) $\boldsymbol{x}^*$ нулей и единиц. Характеристическим множеством $M^1_{f^i}$ компонентной функции $f^i(\boldsymbol{x})$, $i = 1, \ldots, m$, системы $\boldsymbol{f}(\boldsymbol{x})$ называется множество наборов булева пространства, на которых функция $f^i(\boldsymbol{x})$ принимает единичное значение. Через $M^0_{f^i}$ обозначим множество наборов нулевых значений функции $f^i(\boldsymbol{x})$.

Далее под связанностью булевых функций будет пониматься совпадение подобластей в характеристических множествах $M^1_{f^i}$ компонентных функций. Обозначим через $|A|$ мощность множества A. Система функций $\boldsymbol{f}(\boldsymbol{x})$ называется S^1_e-связанной, если $e \le e^n_{\max}$, где

$$e^n_{\max} = \left| \bigcap_{i=1}^{m} M^1_{f^i} \right|. \qquad (1)$$

Иными словами, система функций $\boldsymbol{f}(\boldsymbol{x})$ называется S^1_e-связанной, если имеется e наборов n-мерного булева пространства, на которых все компонентные функции $f^i(\boldsymbol{x})$ системы одновременно принимают единичное значение. Очевидно, что для заданной системы булевых функций, зависящих от n переменных, параметр $e^n_{\max}$ задает максимальное значение e**.** Если система функций является S^1_e-связанной, то она будет S^1_q-связанной для всех q, удовлетворяющих условию $0 \le q \le e$. Число $e^n_{\max}$ назовем весом связанности системы функций. Для одной булевой функции, зависящей от n переменных, вес связанности – это число, равное мощности множества $M^1_{f^i}$.

Мерой (долей) связанности $\rho^n_e(f^1, \ldots, f^m)$ системы функций $\boldsymbol{f}(\boldsymbol{x})$ назовем отношение

$$\rho^n_e(f^1, \ldots, f^m) = \frac{e^n_{\max}}{2^n}. \qquad (2)$$

Очевидно, что мера связанности $\rho^n_e(f^1, \ldots, f^m)$ ограничена: $0 \le \rho^n_e(f^1, \ldots, f^m) \le 1$.

Если все компонентные функции $f^i(\boldsymbol{x}) = 1$, $i = 1, \ldots, m$, то $\rho^n_e(f^1, \ldots, f^m) = 1$. Если же система функций состоит, например, из пары f^1, $\overline{f^1}$ взаимно инверсных функций, то $\rho^n_e(f^1, \overline{f^1}) = 0$. Очевидно, что это не единственный пример системы функций с нулевой мерой связанности, такие системы будем называть несвязанными.

Системы булевых функций могут быть заданы в различной форме. В качестве форм задания систем функций далее будут рассматриваться матричные формы – таблицы истинности (табл. 1) и системы ДНФ (табл. 2), а также представления систем функций алгебраическими формулами, задающими разложения Шеннона (таким формулам соответствуют графовые BDD-представления). Для системы функций (табл. 1) мера связанности $\rho^4_e(f^1, f^2, f^3, f^4) = 0$, так как нет ни одного набора значений переменных вектора $\boldsymbol{x} = (x_1, x_2, x_3, x_4)$, на котором

значения всех четырех компонентных функций одновременно равны единице. Позже будет показано, что данная система содержит подсистемы связанных функций.

Таблица 1
Система полностью определенных булевых функций

$x_1\ x_2\ x_3\ x_4$	$f^1\ f^2\ f^3\ f^4$
0 0 0 0	0 0 1 1
0 0 0 1	1 1 0 0
0 0 1 0	1 0 0 0
0 0 1 1	1 1 0 0
0 1 0 0	0 0 1 1
0 1 0 1	1 1 0 0
0 1 1 0	0 1 1 1
0 1 1 1	1 1 1 0
1 0 0 0	0 0 1 1
1 0 0 1	1 0 0 0
1 0 1 0	1 1 0 0
1 0 1 1	1 1 0 0
1 1 0 0	0 0 1 1
1 1 0 1	1 0 1 1
1 1 1 0	0 0 0 1
1 1 1 1	1 0 1 0

Таблица 2
Система ДНФ булевых функций

T^x	B^f
$x_1\ x_2\ x_3\ x_4$	$f^1\ f^2\ f^3\ f^4$
– 0 1 –	1 0 0 0
0 1 1 –	0 1 1 0
– – – 1	1 0 0 0
1 0 1 –	0 1 0 0
1 1 0 –	0 0 1 1
– 1 – 0	0 0 0 1
– 1 1 1	0 0 1 0
0 – – 1	0 1 0 0
– – 0 0	0 0 1 1

В матричной форме система ДНФ (табл. 2) задается парой матриц: строки троичной матрицы T^x представляют элементарные конъюнкции (троичные векторы – интервалы булева пространства [3]), а единичные значения элементов в булевой матрице B^f отмечают вхождения соответствующих конъюнкций в ДНФ функций:

$$D^1 = \overline{x}_2 x_3 \vee x_4,\ D^2 = \overline{x}_1 x_2 x_3 \vee x_1 \overline{x}_2 x_3 \vee \overline{x}_1 x_4,$$

$$D^3 = \overline{x}_1 x_2 x_3 \vee x_1 x_2 \overline{x}_3 \vee x_2 x_3 x_4 \vee \overline{x}_3 \overline{x}_4,\ D^4 = \overline{x}_1 x_2 x_3 \vee x_2 \overline{x}_4 \vee \overline{x}_3 \overline{x}_4.$$

Заметим, что данная система ДНФ представляет ту же систему булевых функций, которая приведена в табл. 1. Если в элементарной конъюнкции отсутствуют q литералов, то в представляющем ее троичном векторе имеется q неопределенных элементов «–». Весом троичного вектора, содержащего q неопределенных элементов, назовем число 2^q. Другими словами, вес троичного вектора – это число двоичных векторов, получающихся всевозможными заменами неопределенных элементов троичного вектора на определенные элементы: нули либо единицы.

Системы ДНФ обычно минимизируются [2, 3], при этом стремятся уменьшить число элементарных конъюнкций и (или) число литералов в конъюнкциях. В получаемых минимизированных системах ДНФ элементарные конъюнкции (троичные векторы) находятся в различных отношениях. Далее будет использоваться отношение ортогональности. Если все троичные векторы матрицы T^x попарно ортогональны, то система ДНФ называется ортогонализованной [3, 9]. Троичные векторы $a = (x_1^a, ..., x_n^a)$, $b = (x_1^b, ..., x_n^b)$ ортогональны, если найдется хотя бы одна компонента $i \in \{1, \ldots, n\}$, означающая, что x_i^a, x_i^b определены и не равны. Например, троичные векторы a = (0, –, 1, 0), b = (–, 1, 0, 0) ортогональны, так как для i = 3 выполняются условия ортогональности $x_3^a = 1$ и $x_3^b = 0$. Если троичные векторы ортогональны, то конъюнкция (логическое произведение) соответствующих им элементарных конъюнкций равна нулю: $a \,\&\, b = ab = (\overline{x}_1 x_3 \overline{x}_4)(x_2 \overline{x}_3 \overline{x}_4) = 0$.

BDD являются представлениями булевых функций в виде ориентированных ациклических графов. Как показано в работе [9], таким представлениям соответствуют задания каждой из компонентных функций $f^i(\boldsymbol{x})$ в виде пары ортогонализованных ДНФ. Одна из таких ДНФ задает область $M^1_{f^i}$ единичных значений компонентной функции, другая ДНФ – область $M^0_{f^i}$ нулевых значений функции. Компактность BDD-представления системы функций в виде графа

обеспечивается тем, что задание графа более компактно, чем перечисление всех путей из корневых вершин к листовым вершинам 0, 1. Для упрощения графа листовые вершины обычно дублируются, а ориентация дуг на рисунках графов BDD не показывается, так как всегда принимается, что дуги ориентированы сверху вниз. Каждому пути из корневой вершины BDD, помеченной функцией f^i, к листовой вершине 1 соответствует элементарная конъюнкция, включающая дуги (литералы) x_i, $\bar{x}_i$ на этом пути. При этом дуге, помеченной символом 0, соответствует отрицательный литерал $\bar{x}_i$; дуге, помеченной символом 1, – положительный литерал x_i, а всем путям между указанными вершинами – дизъюнкция получаемых элементарных конъюнкций, образующая ортогонализованную ДНФ $D^1_{f^i}$. Пути из корневой вершины f^i к листовой вершине 0 задают ортогонализованную ДНФ $D^0_{f^i}$.

На рис. 1 показана BDD, представляющая систему булевых функций, которая задана в табл. 1 и 2. В табл. 3 даны ортогонализованные ДНФ, полученные по графовому BDD-представлению на рис. 1 и задающие характеристические множества компонентных функций.

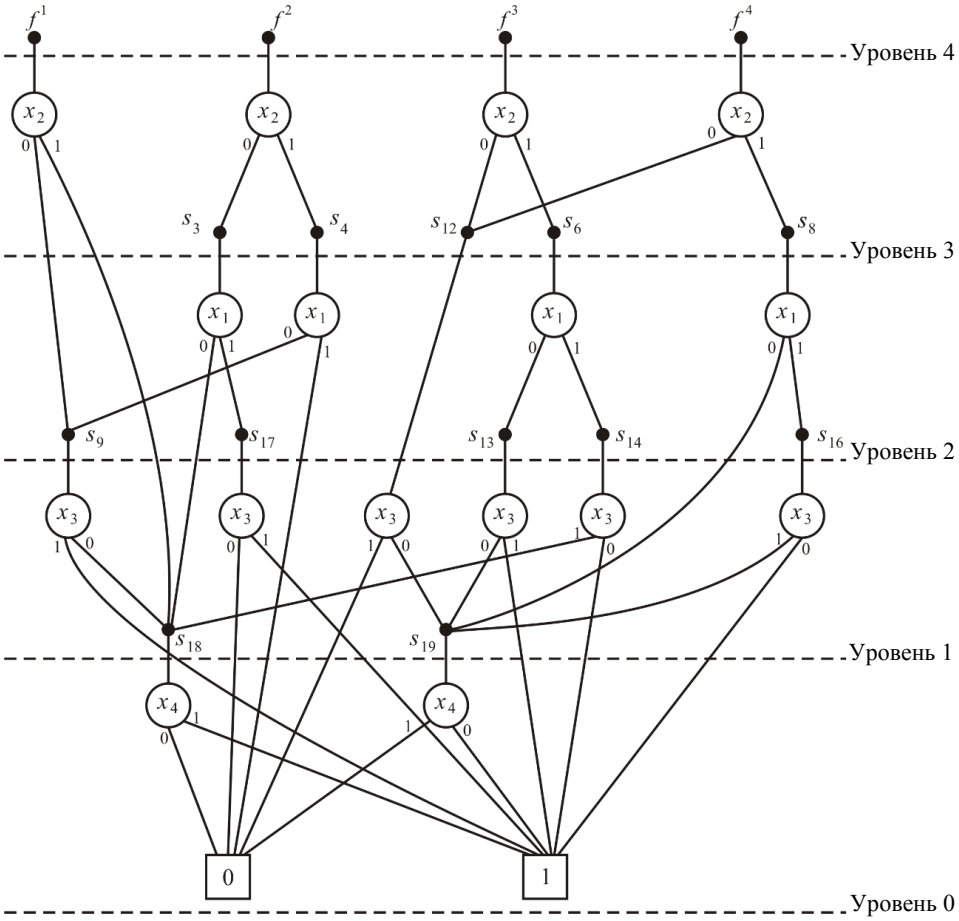


Рис. 1. BDD, реализующая систему булевых функций (см. табл. 1)

Каждой функциональной вершине BDD соответствует формула разложения Шеннона. Например, функциональной вершине f^1 соответствует формула $f^1 = \bar{x}_2 s_9 \vee x_2 x_4$, функциональной вершине s_{13} – формула $s_{13} = \bar{x}_3 \bar{x}_4 \vee x_3$ и т. д. В литературе функциональные вершины BDD не изображаются, а пометки 0, 1 заменяются различными изображениями дуг. Например, если дуга помечена символом 0, то она рисуется прерывистой линией [7, 8].

Таблица 3

Ортогонализованные ДНФ, полученные по BDD-представлению

ДНФ	x_1 x_2 x_3 x_4
$D^1_{f^1}$	– 1 – 1 – 0 1 – – 0 0 1
$D^1_{f^2}$	1 0 1 – 0 1 1 – 0 0 – 1 0 1 0 1
$D^1_{f^3}$	0 1 1 – – 0 0 0 1 1 0 – 0 1 0 0 1 1 1 1
$D^1_{f^4}$	1 1 0 – 0 1 – 0 1 1 1 0 – 0 0 0

Таблица 4

Матричное задание СДНФ функций f^1, f^2

СДНФ	x_1 x_2 x_3 x_4
$D^1_{f^1}$	**0 1 0 1** **0 1 1 1** 1 1 0 1 1 1 1 1 0 0 1 0 **0 0 1 1** **1 0 1 0** **1 0 1 1** **0 0 0 1** 1 0 0 1
$D^1_{f^2}$	**1 0 1 0** **1 0 1 1** 0 1 1 0 **0 1 1 1** **0 0 0 1** **0 0 1 1** **0 1 0 1**

Всему графу BDD (рис. 1) соответствуют 16 формул:

$$f^1 = \bar{x}_2 s_9 \vee x_2 x_4,\ f^2 = \bar{x}_2 s_3 \vee x_2 s_4,\ f^3 = \bar{x}_2 s_{12} \vee x_2 s_6,\ f^4 = \bar{x}_2 s_{12} \vee x_2 s_8,$$
$$s_3 = \bar{x}_1 x_4 \vee x_1 x_3,\ s_4 = \bar{x}_1 s_9,\ s_6 = \bar{x}_1 s_{13} \vee x_1 s_{14},\ s_8 = \bar{x}_1 \bar{x}_4 \vee x_1 s_{16},$$
$$s_9 = \bar{x}_3 x_4 \vee x_3,\ s_{12} = \bar{x}_3 \bar{x}_4,\ s_{13} = \bar{x}_3 \bar{x}_4 \vee x_3,\ s_{14} = \bar{x}_3 \vee x_3 x_4, \qquad (3)$$
$$s_{16} = \bar{x}_3 \vee x_3 \bar{x}_4,\ s_{17} = x_3,\ s_{18} = x_4,\ s_{19} = \bar{x}_4.$$

Вычисление меры связанности ρ^n_e подсистемы по BDD-представлению исходной системы булевых функций. Чтобы вычислить меру связанности $\rho^n_e(f^1, ..., f^k)$ подсистемы функций, требуется по BDD-представлению получить ДНФ этих функций, затем по полученным ДНФ определить число наборов, на которых все функции подсистемы одновременно принимают единичное значение.

Приведем пример вычисления меры связанности $\rho^4_e(f^1, f^2)$ функций f^1, f^2, ДНФ которых заданы в табл. 3. Напомним, что такие ДНФ были получены по BDD-представлению (рис. 1) системы функций, заданной в табл. 1. Матричное задание совершенных ДНФ (СДНФ) функций f^1, f^2 представлено в табл. 4, где одинаковые двоичные наборы, соответствующие полным элементарным конъюнкциям СДНФ, отмечены жирным шрифтом. Двоичные наборы полных элементарных конъюнкций легко получить заменой «–» в троичном векторе, представляющем элементарную конъюнкцию, всевозможными комбинациями нулей и единиц. Число одинаковых наборов (полных элементарных конъюнкций) равно шести, общее число наборов булева пространства размерности $n = 4$ равно 16. Поэтому $\rho^4_e(f^1, f^2) = 6/16 = 0{,}375$ (37,5 %).

Переход к СДНФ и их сравнение по числу одинаковых полных элементарных конъюнкций являются не единственным способом оценки меры связности. Можно выполнить перемножение ДНФ $D^1_{f^1}$ & $D^1_{f^2}$, полученных по BDD-представлению, вычислить соответствующую ДНФ, а затем перейти к СДНФ:

$$D^1_{f^1} \,\&\, D^1_{f^2} = (x_2 x_4 \vee \bar{x}_2 \bar{x}_3 \vee \bar{x}_2 \bar{x}_3 x_4) \,\&\, (x_1 \bar{x}_2 x_3 \vee \bar{x}_1 x_2 x_3 \vee \bar{x}_1 \bar{x}_2 x_4 \vee \bar{x}_1 x_2 x_3 \bar{x}_4) =$$
$$= \bar{x}_1 x_2 x_3 x_4 \vee \bar{x}_1 x_2 \bar{x}_3 x_4 \vee x_1 \bar{x}_2 x_3 \vee \bar{x}_1 \bar{x}_2 x_3 x_4 \vee \bar{x}_1 \bar{x}_2 x_4 =$$
$$= \bar{x}_1 x_2 x_3 x_4 \vee \bar{x}_1 x_2 \bar{x}_3 x_4 \vee x_1 \bar{x}_2 x_3 \bar{x}_4 \vee x_1 \bar{x}_2 x_3 x_4 \vee \bar{x}_1 \bar{x}_2 x_3 x_4 \vee \bar{x}_1 \bar{x}_2 \bar{x}_3 x_4.$$

Полученная СДНФ содержит шесть полных элементарных конъюнкций, соответствующих наборам, которые отмечены в табл. 4 жирным шрифтом. Это и есть наборы, на которых f^1 и f^2 одновременно принимают единичные значения (см. табл. 1).

Связанность формульных BDD-представлений системы функций. Обозначим через $R_{\text{BDD}}(f^1, ..., f^m)$ множество функциональных вершин (формул) BDD, реализующей систему функций $f^1(\boldsymbol{x}),\ldots, f^m(\boldsymbol{x})$, а через $R_{\text{BDD}}(f^i)$ – множество функциональных вершин (формул) подграфа BDD, реализующего компонентную функцию f^i. В рассматриваемом примере множество формул (3) задает $R_{\text{BDD}}(f^1, f^2, f^3, f^4)$.

Связанностью $S^{\text{node}}_{\text{BDD}}(f^1, ..., f^m)$ по вершинам BDD назовем

$$S^{\text{node}}_{\text{BDD}}(f^1, ..., f^m) = \left|\bigcap_{i=1}^{m} R_{\text{BDD}}(f^i)\right|. \tag{4}$$

Иначе говоря, связанностью по вершинам BDD называется число общих функциональных вершин (формул), входящих в BDD-представление системы функций. В рассматриваемом примере $S^{\text{node}}_{\text{BDD}}(f^1, ..., f^m) = 0$, так как нет ни одной общей функциональной вершины при реализации каждой из четырех функций системы. Заметим, что найдутся подсистемы данной системы, для которых связанность по вершинам BDD будет не нулевой. Например, такой подсистемой является $\{ f^1, f^2 \}$: $R_{\text{BDD}}(f^1) = \{ s_9, s_{18} \}$, $R_{\text{BDD}}(f^2) = \{ s_3, s_4, s_9, s_{17}, s_{18} \}$, где две общие функциональные вершины – s_9 и s_{18}, поэтому $S^{\text{node}}_{\text{BDD}}(f^1, f^2) = 2$.

Мерой (долей) связанности $\rho^{\text{node}}_{\text{BDD}}(f^1, ..., f^m)$ системы функций $\boldsymbol{f}(\boldsymbol{x}) = (f^1(\boldsymbol{x}),\ldots, f^m(\boldsymbol{x}))$ назовем отношение

$$\rho^{\text{node}}_{\text{BDD}}(f^1, ..., f^m) = \frac{S^{\text{node}}_{\text{BDD}}(f^1, ..., f^m)}{\max\left|R_{\text{BDD}}(f^i)\right|}. \tag{5}$$

В рассматриваемом примере для подсистемы из двух функций f^1, f^2 значение $\max\left|R_{\text{BDD}}(f^2)\right| = 5$, поэтому выполняется соотношение

$$\rho^{\text{node}}_{\text{BDD}}(f^1, f^2) = \frac{S^{\text{node}}_{\text{BDD}}(f^1, f^2)}{\left|R_{\text{BDD}}(f^2)\right|} = 2/5 = 0{,}4.$$

Доля связанности $\rho^{\text{node}}_{\text{BDD}}(f^1, ..., f^m)$ ограничена:

$$0 \le \rho^{\text{node}}_{\text{BDD}}(f^1, ..., f^m) \le 1. \tag{6}$$

Введем понятие уровня BDD. Листовые константные вершины 0, 1 расположены на уровне 0 (см. рис. 1), функциональные вершины-переменные – на уровне 1 и т. д. Если все переменные системы функций являются существенными, то число всех уровней BDD равно $n + 1$. По сути, номер уровня определяет число переменных, от которых зависит подфункция, расположенная на данном уровне.

Связанностью $S^{\text{weight}}_{\text{BDD}}(f^1, ..., f^m)$ по вершинам BDD с учетом их весов назовем сумму весов общих вершин. Вес общей вершины уровня i равен 2^i. Однако множество общих вершин в данном случае формируется более сложным образом: из множества общих вершин исключаются «подчиненные» общие вершины. Под «подчиненными» общими вершинами понимаются общие вершины, которые являются дочерними вершинами других общих вершин. Иными сло-

вами, суммируются веса только вершин верхних уровней из множества всех общих вершин. Например, для подсистемы из двух функций f^1, f^2 (см. рис. 1) вес вершины s_9 на уровне 2 равен четырем, а вес вершины s_{18} на уровне 1 – двум. Поэтому $S_{\text{BDD}}^{\text{weight}}(f^1, f^2) = 4 + 2 = 6$.

Мерой (долей) связанности $\rho_{\text{BDD}}^{\text{weight}}(f^1, ..., f^m)$ системы функций $\boldsymbol{f}(\boldsymbol{x}) = (f^1(\boldsymbol{x}), \ldots, f^m(\boldsymbol{x}))$ назовем отношение

$$\rho_{\text{BDD}}^{\text{weight}}(f^1, ..., f^m) = \frac{S_{\text{BDD}}^{\text{weight}}(f^1, ..., f^m)}{2^n}. \quad (7)$$

Подсчитаем меру связанности $\rho_{\text{BDD}}^{\text{weight}}(f^1, f^2)$ для подсистемы $\{f^1, f^2\}$:

$$\rho_{\text{BDD}}^{\text{weight}}(f^1, f^2) = \frac{S_{\text{BDD}}^{\text{weight}}(f^1, f^2)}{2^4} = 6/16 = 0{,}375.$$

Постановка задач и алгоритмы выделения связанных подсистем

Задача 1. Задано BDD-представление системы $\boldsymbol{f}(\boldsymbol{x}) = (f^1(\boldsymbol{x}), \ldots, f^m(\boldsymbol{x}))$ булевых функций, зависящих от n переменных, и параметр p $(0 < p < 2^n)$. Требуется выделить из системы $\boldsymbol{f}(\boldsymbol{x})$ максимальное число функций, которые могут быть разбиты на минимальное число S_p^1-связанных подсистем, таких, что каждая из них содержит не менее чем две функции.

Задача 2. Задано BDD-представление системы $\boldsymbol{f}(\boldsymbol{x}) = (f^1(\boldsymbol{x}), \ldots, f^m(\boldsymbol{x}))$ булевых функций, зависящих от n переменных, и параметр ρ $(0 < \rho < 1)$. Требуется выделить из системы $\boldsymbol{f}(\boldsymbol{x})$ максимальное число функций, которые могут быть разбиты на минимальное число подсистем с мерой связанности $\rho_{\text{BDD}}^{\text{node}} \geq \rho$, причем каждая из подсистем включает не менее чем две функции.

Задача 3. Задано BDD-представление системы $\boldsymbol{f}(\boldsymbol{x}) = (f^1(\boldsymbol{x}), \ldots, f^m(\boldsymbol{x}))$ булевых функций, зависящих от n переменных, и параметр ρ $(0 < \rho < 1)$. Требуется выделить из системы $\boldsymbol{f}(\boldsymbol{x})$ максимальное число функций, которые могут быть разбиты на минимальное число подсистем с мерой связанности $\rho_{\text{BDD}}^{\text{weight}} \geq \rho$, причем каждая из подсистем включает не менее чем две функции.

Предлагаемый эвристический алгоритм 1 (решение задачи 1) состоит в последовательном формировании (на каждой итерации i) очередной подсистемы P^i S_p^1-связанных функций по текущей (остаточной) системе функций. На первой итерации (i = 1) текущую систему функций образуют функции исходной системы.

На каждой итерации требуется выполнить шаги 1–3.

Шаг 1. Рассмотреть $m - 1$ неупорядоченную пару функций $\{f^1, f^j\}$, j = 2, ..., m, текущей системы и найти такую пару L функций, которые являются S_q-связанными с максимальным значением параметра q, причем $q \geq p$. Если таких пар функций несколько, то выбирается первая из них (эвристика E1). Если указанной пары L функций нет, то из системы функций нельзя выделить ни одной S_p^1-связанной подсистемы. Конец алгоритма.

Шаг 2. Составить из функций найденной на первом шаге пары L функций формируемую подсистему P^i из двух связанных функций, исключив выбранную пару L функций из текущей системы, и добавлять в формируемую подсистему поочередно те функции f^r, которые находятся с помощью следующей эвристики.

Эвристика E2. Из множества функций текущей системы выбирается та функция f^r, которая обеспечивает наибольшее возможное значение параметра q для подсистемы $P^i \cup \{f^r\}$. Если таких функций несколько, то выбирается и добавляется в формируемую подсистему P^i первая из них.

Шаг 3. Если нет ни одной функции f^r, такой, что подсистема $P^i \cup \{f^r\}$ является S_p^1-связанной, – закончить формирование подсистемы P^i и объявить не входящие в нее функции текущей подсистемой. Переход на шаг 1 (формирование следующей подсистемы на итерации $i + 1$).

Шаг 4. Закончить формирование подсистем, когда все функции текущей системы будут включены в формируемые подсистемы либо когда в текущей подсистеме нельзя будет найти ни одной пары функций, которые образуют S_p^1-связанную подсистему. Конец алгоритма.

Алгоритмы решения задач 2 и 3 аналогичны, только формируемые подсистемы проверяются на выполнение ограничения по связанности для значений параметров $\rho_{\text{BDD}}^{\text{node}}$ (задача 2) и $\rho_{\text{BDD}}^{\text{weight}}$ (задача 3).

Эвристический алгоритм 2 (решение задач 1–3) является более быстродействующим по сравнению с алгоритмом 1 и позволяет находить пары связанных функций, при этом мера связанности найденных пар удовлетворяет ограничению ρ. Алгоритм 2 отличается от алгоритма 1 тем, что в алгоритме 2 не выполняется шаг 2.

Пример выделения связанных подсистем. Проиллюстрируем эвристический алгоритм 2 для решения задач 1–3 на примере выделения пар связанных функций для BDD-представления (см. рис. 1), заданного формулами (3) для меры связанности ρ = 20 %. В табл. 5 указаны меры связанности $\rho_e^4(f^i, f^j)$ пар функций – одна из функций f^i пары соответствует строке, вторая f^j – столбцу. Для функции f^1 наибольшая мера связанности будет для пары $\rho_e^4(f^1, f^2) = 6/16 = 0{,}375$, что соответствует 37,5 %. Оставшаяся пара $\{f^3, f^4\}$ имеет меру связанности $\rho_e^4(f^3, f^4)$ = 0,375 (37,5 %), что также больше 20 %. Решением задачи 1 являются пары $\{f^1, f^2\}$ и $\{f^3, f^4\}$. В табл. 5–7 жирным шрифтом выделены значения мер связанности, по которым формируются связанные пары функций.

Таблица 5

Мера связанности $\rho_e^4(f^i, f^j)$ пар функций

	f^2	f^3	f^4
f^1	**37,5**	18,75	6,25
f^2	–	12,5	6,25
f^3	–	–	**37,5**

Аналогичные решения имеют задачи 2 и 3. Соответствующие меры связанности пар функций приведены в табл. 6 и 7. Заметим, что для данного примера значения меры связанности $\rho_{\text{BDD}}^{\text{node}}(f^i, f^j)$ более близки к значениям эталонной меры связанности $\rho_e^4(f^i, f^j)$ по сравнению со значениями меры связанности $\rho_{\text{BDD}}^{\text{weight}}(f^i, f^j)$. Однако при экспериментальном исследовании алгоритмов решения задач 1–3 использование $\rho_{\text{BDD}}^{\text{weight}}(f^i, f^j)$ иногда позволяло получать лучшие решения при синтезе схем.

Таблица 6

Мера связанности $\rho_{\text{BDD}}^{\text{node}}(f^i, f^j)$ пар функций

	f^2	f^3	f^4
f^1	**40**	16,6	0
f^2	–	16,6	0
f^3	–	–	**33,3**

Таблица 7

Мера связанности $\rho_{\text{BDD}}^{\text{weight}}(f^i, f^j)$ пар функций

	f^2	f^3	f^4
f^1	**37,5**	12,5	0
f^2	–	12,5	0
f^3	–	–	**62,5**

Приведем подсчет меры связанности $\rho_{BDD}^{weight}(f^3, f^4)$ для пары $\{f^3, f^4\}$. BDD-представление подсистемы $\{f^3, f^4\}$ (см. рис. 1) содержит общие функциональные вершины s_{12} и s_{19}. Вершина s_{12} расположена на третьем уровне BDD и имеет вес $2^3 = 8$, вершина s_{19} – на первом уровне и имеет вес $2^1 = 2$. Следовательно, связанность $S_{BDD}^{weight}(f^3, f^4) = 8 + 2 = 10$, мера связанности $\rho_{BDD}^{weight}(f^3, f^4) = \frac{S_{BDD}^{weight}(f^3, f^4)}{2^4} = 10/16 = 0,625$ (62,5 %) (см. табл. 7).

Программная реализация. Предложенные алгоритмы решения задач 1–3 были программно реализованы в среде QtCreator на языке программирования C++ с использованием библиотеки классов Qt [12] и включены в систему FLC [13] логической оптимизации функционально-структурных описаний дискретных устройств.

Программы выделения подсистем (либо пар) связанных функций используются для технологически независимой оптимизации функциональных описаний схем комбинационной логики. Оптимизация таких описаний в системе FLC осуществляется на основе различных методов совместной и раздельной минимизации систем булевых функций в классе ДНФ, методов декомпозиции и методов многоуровневой минимизации BDD- и BDDI-представлений систем булевых функций. Разработанные по алгоритмам выделения подсистем функций программы используются как предварительный этап для минимизации BDD- и BDDI-представлений систем булевых функций. Выполнение этого этапа позволяет уменьшить сложность минимизированных BDD- и BDDI-описаний по такому критерию, как суммарное число литералов. Данный критерий оценки сложности алгебраических представлений систем функций давно используется при синтезе логических схем [1]. Разработанные программы выделения подсистем связанных функций могут быть использованы также в системе CMOSLD [14], предназначенной для проектирования заказных КМОП СБИС.

Экспериментальные исследования. Для проверки эффективности влияния алгоритмов выделения связанных подсистем функций на сложность (площадь) логических схем были проведены вычислительные эксперименты. Синтез схем из библиотечных КМОП-элементов по VHDL-описаниям во всех случаях выполнялся в системе LeonardoSpectrum [15] при одних и тех же режимах (опциях) синтеза. Под площадью схемы на этапе логического проектирования обычно понимается суммарная площадь кристалла, требуемая для размещения элементов схемы. Хотя данный критерий оценки сложности является приблизительным (в расчет не принимается площадь под межсоединения элементов схемы), он часто используется на этапе логического проектирования схем в отличие от этапа топологического проектирования, когда под площадью понимается общая площадь под элементы и межсоединения (связи) элементов. Далее в экспериментах площадь S_{ASIC} схемы из библиотечных КМОП-элементов подсчитывалась как сумма площадей элементов, составляющих схему. Именно такую оценку сложности синтезированной схемы получает LeonardoSpectrum. Библиотека логических элементов представлена в работе [9, с. 191], пример логической схемы из элементов данной библиотеки и подсчет ее площади приведены в статье [16].

Примеры матричных SF-описаний систем функций были взяты из набора промышленных тестовых примеров [17], и для каждого них были построены BDD-представления с помощью программы Tie_BDD [9], входящей в систему FLC логической оптимизации [13]. При BDD-оптимизации программа Tie_BDD испытывала 5000 перестановок переменных исходной системы функций, перестановки оценивались по числу функциональных вершин и BDD-представление выбиралось по той перестановке, которая давала минимальное число функциональных вершин. После выделения связанных подсистем они оптимизировались в классе BDDI с помощью программы BDD-Builder [10] либо Tie_BDD. Программа BDD_Builder при выборе очередной переменной разложения руководствовалась правилом: выбиралась та переменная, по которой использовалось минимальное число различных взаимно инверсных подфункций разложения Шеннона. Схема организации экспериментов показана на рис. 2.

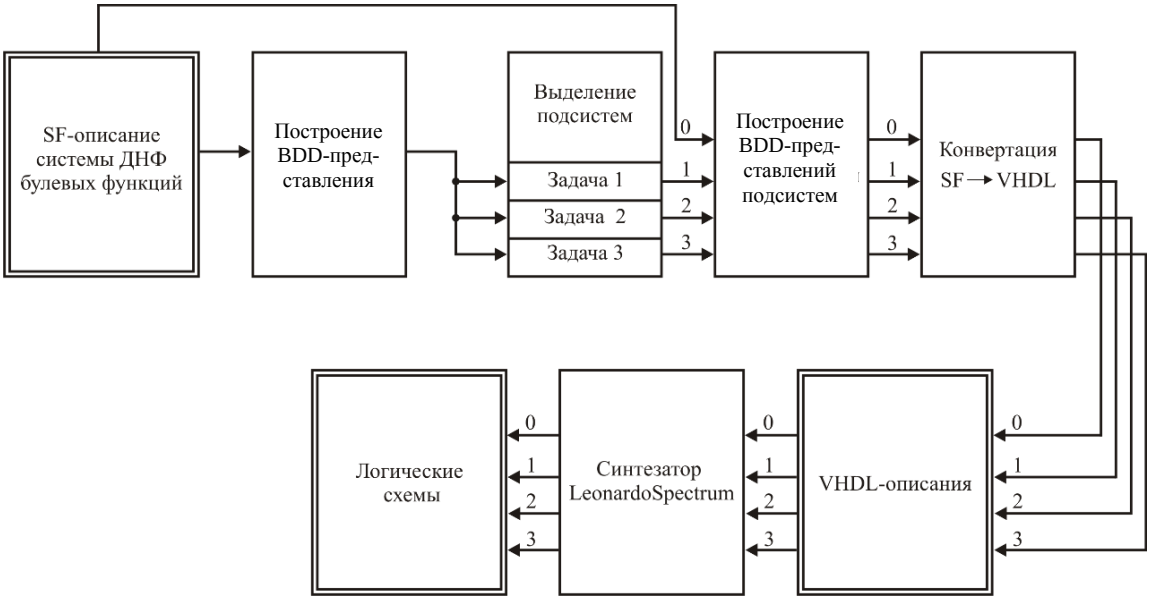


Рис. 2. Организация экспериментов

Результаты экспериментов представлены в табл. 8–12, где n – число переменных; m – число функций системы; k – число общих элементарных конъюнкций исходной системы ДНФ булевых функций, по которой строилось BDD-представление; S_{ASIC} – площадь логической схемы; t (с) – время выполнения программы на персональном компьютере с процессором AMD Ryzen 5 2400G. Жирным шрифтом в табл. 8–12 выделены лучшие решения – схемы меньшей площади. Все значения различных мер связанности ρ_e^n, $\rho_{\text{BDD}}^{\text{node}}$, $\rho_{\text{BDD}}^{\text{weight}}$ (табл. 8, 10–12) заданы в процентах.

Эксперимент 1. Исследовался алгоритм 1 для решения задач 1–3. Результаты эксперимента 1 для промышленных примеров схем приведены в табл. 8–10.

Результаты эксперимента 1 для «блочных» систем ДНФ представлены в табл. 9 и 10. Общий вид «блочных» систем ДНФ показан на рис. 3, число общих переменных для пары блоков – не более четырех.

Таблица 8

Результаты эксперимента 1 для промышленных примеров

Пример	n	m	Мера связанности, %	BDDI исходной системы S_{ASIC}	Выделение подсистем связанных функций, оптимизация BDDI					
					Задача 1		Задача 2		Задача 3	
					S_{ASIC}	t, с	S_{ASIC}	t, с	S_{ASIC}	t, с
ADD6	12	7	25	**12 806**	**12 806**	0,180	**12 806**	0,007	**12 806**	0,012
ADDM4	9	8	10	80 782	**71 173**	0,161	83 226	0,192	73 522	0,206
B12	15	9	20	18 966	**16 009**	0,017	16 472	0,007	17 744	0,013
B2	16	17	20	**199 106**	261 730	8,904	215 020	15,154	252 138	14,219
B9	16	5	5	**27 621**	28 620	0,048	28 369	0,013	27 889	0,023
IN0	15	11	15	94 620	91 306	0,237	90 190	0,335	**89 486**	0,587
INTB	15	7	20	**273 532**	311 470	2,585	308 379	6,679	308 379	5,053
M181	15	9	15	18 849	**16 467**	0,014	19 469	0,005	19 156	0,026
M2	8	16	15	**45 114**	47 357	0,046	**45 114**	0,091	47 413	0,157
M3	8	16	15	**52 580**	53 657	0,068	53 445	0,189	58 942	0,201
MP2D	14	14	15	**17 471**	18 135	0,038	17 700	0,043	18 252	0,077
P82	5	14	5	19 988	**18 620**	0,009	20 082	0,018	20 981	0,134
ROOT	8	5	5	26 109	27 816	0,025	**25 194**	0,024	26 494	0,034
T3	12	8	5	16 534	17 276	0,008	**14 558**	0,010	17 772	0,070
TIAL	14	8	15	360 264	**325 219**	6,113	390 846	4,619	335 079	5,607
Z5XP1	7	10	25	**18 442**	**18 442**	0,012	20 412	0,011	18 827	0,032

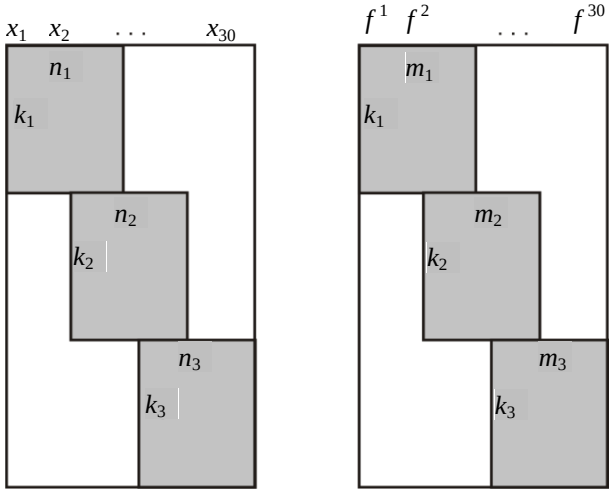


Рис. 3. Общий вид матричного задания «блочных» систем ДНФ

Таблица 9

Результаты эксперимента 1 для «блочных» систем ДНФ – сложности S_{ASIC} схем при реализации исходной системы ДНФ-функций

Пример	n	m	k	Оптимизация BDD	Оптимизация BDDI
				S_{ASIC}	S_{ASIC}
BL_1	30	30	400	3 616 883	**3 406 194**
BL_2	30	30	605	4 165 967	**4 064 779**
BL_3	30	30	636	**4 457 806**	4 482 687

Алгоритмы выделения подсистем связанных функций из BDD-представлений системы функций позволяют сформировать подсистемы, которые соответствуют блокам матричного представления исходной системы ДНФ функций. Для блочных систем функций выделение связанных подсистем является целесообразным при последующем синтезе.

Таблица 10

Результаты эксперимента 1 для «блочных» систем ДНФ

Пример	Мера связанности, %	Выделение подсистем связанных функций							
		Задача 2				Задача 3			
		Число подсистем	t, с	Оптимизация BDD	Оптимизация BDDI	Число подсистем	t, с	Оптимизация BDD	Оптимизация BDDI
				S_{ASIC}	S_{ASIC}			S_{ASIC}	S_{ASIC}
BL_1	5	3	529	3 207 367	3 247 783	11	408	**3 192 418**	3 436 594
	10	4	456	3 385 749	3 210 196	4	476	3 556 564	3 339 970
	20	1	539	3 469 583	3 279 193	3	538	3 566 357	3 494 743
	40	0	708	3 616 883	3 406 194	0	714	3 616 883	3 406 194
BL_2	5	2	648	3 635 275	3 681 500	13	496	3 869 646	3 963 865
	10	4	547	**3 532 146**	3 657 450	12	420	3 931 127	4 113 370
	20	5	437	3 849 904	3 788 653	0	949	4 165 967	4 064 779
	40	0	929	4 165 967	4 064 779	0	951	4 165 967	4 064 779
BL_3	5	2	1004	4 119 915	**3 969 690**	10	850	4 222 057	4 551 807
	10	3	1003	4 210 657	4 050 701	12	673	4 478 184	4 665 884
	20	5	692	4 099 135	4 238 205	4	1081	4 387 476	4 346 011
	40	0	1271	4 457 806	4 482 687	0	1307	4 457 806	4 482 687

Эксперимент 2. Исследовался алгоритм 2 – выделение пар связанных функций, исходными данными были матричные представления систем ДНФ булевых функций. Результаты приведены в табл. 11 и 12.

Таблица 11

Результаты эксперимента 2, площади схем

Пример	*n*	*m*	Мера связанности, %	BDDI исходной системы	Выделение пар связанных функций, оптимизация BDDI		
					Задача 1	Задача 2	Задача 3
				S_{ASIC}	S_{ASIC}	S_{ASIC}	S_{ASIC}
ADD6	12	7	50	**12 806**	12 806	12 806	12 806
ADDM4	9	8	20	80 782	76 368	**75 810**	81 083
B12	15	9	10	18 966	16 506	**15 485**	19 017
B2	16	17	20	**199 106**	208 128	208 128	261 005
B9	16	5	10	27 621	27 621	27 889	**27 242**
IN0	15	11	25	94 620	92 081	93 281	**89 486**
INTB	15	7	50	**273 532**	273 532	273 532	273 532
M181	15	9	25	18 849	16 026	**15 468**	18 955
M2	8	16	15	45 114	46 520	**44 088**	49 232
M3	8	16	15	**52 580**	53 936	54 634	54 154
MP2D	14	14	10	**17 471**	18 738	17 700	18 576
P82	5	14	25	19 988	**19 039**	20 947	22 766
ROOT	8	5	25	26 109	**25 194**	25 618	**25 194**
T3	12	8	15	16 534	16 534	**14 558**	16 941
TIAL	14	8	15	360 264	**279 960**	362 164	332 847
Z5XP1	7	10	25	18 442	19 279	18 793	**18 369**

Анализ результатов проведенных экспериментов позволяет сделать вывод о том, что алгоритмы 1 и 2 решения задач 1–3 являются конкурирующими. Эксперимент 2 показал, что для испытанных значений меры связанности выделяется мало пар связанных функций (если в табл. 12 элемент равен нулю, то это значит, что нет ни одной пары с заданным значением меры связанности). Для примеров небольшой размерности (до 16 входов и выходов) программы справляются за 0,5 с, но в случае BDD с большим числом уравнений, например B2 (697 уравнений), INTB (792 уравнения), TIAL (807 уравнений), время выделения подсистем связанных функций может доходить до 15 с. Для больших псевдослучайных примеров (BL_1, BL_2, BL_3) с числом входов и выходов, равным 30, время работы программ составляет 10–15 мин. Такие примеры содержат более 7000 уравнений (например, BL_1 состоит из 7477 уравнений). На практике требуется перебор значений параметра меры связанности, потому что при меньшем значении данного параметра могут быть найдены пары связанных функций и это может дать положительный эффект при синтезе.

Таблица 12

Результаты эксперимента 2, число выделенных пар связанных функций

Пример	Мера связанности, %	Задача 1		Задача 2		Задача 3	
		Число пар	*t*, с	Число пар	*t*, с	Число пар	*t*, с
ADD6	50	0	0,191	0	0,007	0	0,006
ADDM4	20	1	0,072	3	0,035	1	0,074
B12	10	1	0,005	2	0,001	2	0,002
B2	20	1	3,140	1	2,264	3	4,128
B9	10	0	0,025	1	0,005	1	0,010
IN0	25	1	0,317	2	0,199	3	0,198
INTB	50	0	7,626	0	4,792	0	4,770
M181	25	1	0,006	2	0,002	2	0,003
M2	15	1	0,027	2	0,011	4	0,009
M3	15	1	0,040	3	0,011	2	0,011
MP2D	10	1	0,013	3	0,005	2	0,008
P82	25	1	0,006	2	0,002	5	0,002
ROOT	25	1	0,012	2	0,004	1	0,006
T3	15	0	0,016	2	0,004	3	0,003
TIAL	15	1	2,821	1	4,126	1	3,998
Z5XP1	25	1	0,011	1	0,005	2	0,004

Заключение. Эксперименты показали, что для исследованного набора тестовых примеров систем булевых функций выделение связанных подсистем может оказаться эффективной процедурой при логической оптимизации многоуровневых BDD- либо BDDI-представлений, так как при последующем синтезе схемы получаются схемы меньшей площади. При этом не вошедшие в подсистемы функции целесообразно объединять в одну подсистему, а не формировать подсистемы, состоящие из одной функции. Для блочных систем ДНФ предложенный алгоритм позволяет выделять блоки из BDD-представлений исходной системы функций. Для промышленных примеров систем ДНФ BDDI-оптимизация имеет преимущество по сравнению с BDD-оптимизацией выделенных подсистем. Предложенные оценки меры связанности формульных BDD-представлений оказались конкурирующими, при этом решение более трудоемкой задачи 1 позволяет получать лучшие решения по сравнению с решениями задач 2 и 3. Алгоритм выделения пар связанных функций является быстродействующим и также позволяет в ряде примеров уменьшать сложность синтезируемых логических схем. Эксперименты показали, что при практическом использовании соответствующих программ возникает важная задача выбора значения параметра «мера связанности».

Список использованных источников

1. Брейтон, Р. К. Синтез многоуровневых комбинационных логических схем / Р. К. Брейтон, Г. Д. Хэчтел, А. Л. Санджованни-Винчентелли // ТИИЭР. – 1990. – Т. 78, № 2. – С. 38–83.

2. Logic Minimization Algorithm for VLSI Synthesis / K. R. Brayton [et al.]. – Boston : Kluwer Academic Publishers, 1984. – 193 p.

3. Закревский, А. Д. Логические основы проектирования дискретных устройств / А. Д. Закревский, Ю. В. Поттосин, Л. Д. Черемисинова. – М. : Физматлит, 2007. – 592 с.

4. Бибило, П. Н. Декомпозиция булевых функций на основе решения логических уравнений / П. Н. Бибило. – Минск : Беларус. навука, 2009. – 211 с.

5. Кузнецов, О. П. О программной реализации логических функций и автоматов / О. П. Кузнецов // Автоматика и телемеханика. – 1977. – № 7. – С. 63–74.

6. Akers, S. B. Binary decision diagrams / S. B. Akers // IEEE Trans. on Computers. – 1978. – Vol. C-27, no. 6. – P. 509–516.

7. Bryant, R. E. Ordered binary decision diagrams / R. E. Bryant, C. Meinel // Logic Synthesis and Verification / ed.: S. Hassoun, T. Sasao, R. K. Brayton. – Kluwer Academic Publishers, 2002. – P. 285–307.

8. Yang, S. BDS: a BDD-based logic optimization system / S. Yang, M. Ciesielski // IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. – 2002. – Vol. 21, no. 7. – P. 866–876.

9. Бибило, П. Н. Применение диаграмм двоичного выбора при синтезе логических схем / П. Н. Бибило. – Минск : Беларус. навука, 2014. – 231 с.

10. Бибило, П. Н. Использование полиномов Жегалкина при минимизации многоуровневых представлений систем булевых функций на основе разложения Шеннона / П. Н. Бибило, Ю. Ю. Ланкевич // Программная инженерия. – 2017. – № 3. – С. 369–384.

11. Бибило, П. Н. Разбиение системы булевых функций на подсистемы «связанных» функций / П. Н. Бибило // Известия РАН. Теория и системы управления. – 2019. – № 2. – С. 14–29.

12. Шлее, М. Qt 5.3. Профессиональное программирование на C++ / М. Шлее. – СПб. : БХВ-Петербург, 2015. – 928 с.

13. Бибило, П. Н. Логическое проектирование дискретных устройств с использованием продукционно-фреймовой модели представления знаний / П. Н. Бибило, В. И. Романов. – Минск : Беларус. навука, 2011. – 279 с.

14. Система логического проектирования функциональных блоков заказных КМОП СБИС с пониженным энергопотреблением / П. Н. Бибило [и др.] // Микроэлектроника. – 2017. – Т. 46, № 1. – С. 72–88.

15. Бибило, П. Н. Системы проектирования интегральных схем на основе языка VHDL. StateCAD, ModelSim, LeonardoSpectrum / П. Н. Бибило. – М. : СОЛОН-Пресс, 2005. – 384 с.

16. Авдеев, Н. А. Эффективность логической оптимизации при синтезе комбинационных схем из библиотечных элементов / Н. А. Авдеев, П. Н. Бибило // Микроэлектроника. – 2015. – Т. 44, № 5. – С. 383–399.

17. Jeong, C. Computer-aided design of digital systems / C. Jeong // Department of Computer Science [Electronic resource]. – Mode of access: http://www1.cs.columbia.edu/~cs6861/sis/espresso-examples/ex. – Date of access: 20.03.2018.

References

1. Brayton R. K., Hachtel G. D., Sangiovanni-Vincentelli A. L. Sintez mnogourovnevyh kombinacionnyh logicheskih skhem [Synthesis of multi-level combinational logic circuits]. Trudy Institute inzhenerov po jelektronike i radiotehnike [*Proceedings of the Institute of Electronics and Radio Engineering*], 1990, vol. 78, no. 2, pp. 38–83 (in Russian).

2. Brayton K. R., Hachtel G. D., McMullen C., Sangiovanni-Vincentelli A. L. *Logic Minimization Algorithm for VLSI Synthesis*. Boston, Kluwer Academic Publishers, 1984, 193 p.

3. Zakrevskij A. D., Pottosin Ju. V., Cheremisinova L. D. Logicheskie osnovy proektirovanija diskretnyh ustrojstv. *Logical Bases of Design of Discrete Devices*. Moscow, Fizmatlit, 2007, 592 p. (in Russian).

4. Bibilo P. N. Dekompoziciya bulevyh funkcij na osnove resheniya logicheskih uravnenij. *Decomposition of Boolean Functions Based on the Solution of Logical Equations*. Minsk, Belaruskaja navuka, 2009, 211 p. (in Russian).

5. Kuznecov O. P. O programmnoj realizacii logicheskih funkcij i avtomatov [On the software implementation of logical functions and automata]. Avtomatika i telemekhanika [*Automation and Telemechanics*], 1977, no. 7, pp. 63–74 (in Russian).

6. Akers S. B. Binary decision diagrams. *IEEE Transactions on Computers*, 1978, vol. C-27, no. 6, pp. 509–516.

7. Bryant R. E., Meinel C. Ordered binary decision diagrams. *Logic Synthesis and Verification*. In S. Hassoun, T. Sasao, R. K. Brayton. Kluwer Academic Publishers, 2002, pp. 285–307.

8. Yang S., Ciesielski M. BDS: a BDD-based logic optimization system. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2002, vol. 21, no. 7, pp. 866–876.

9. Bibilo P. N. Primenenie diagram dvoichnogo vybora pri sinteze logicheskih shem. *Application of Binary Selection Diagrams in the Synthesis of Logic Circuits*. Minsk, Belaruskaja navuka, 2014, 231 p. (in Russian).

10. Bibilo P. N., Lankevich Yu. Yu. Ispol'zovanie polinomov Zhegalkina pri minimizacii mnogourovnevyh predstavlenij system bulevyh funkcij na osnove razlozheniya Shennona [The use of Zhegalkin polynomials in minimizing multilevel representations of systems of Boolean functions based on the Shannon expansion]. Programmnaya inzheneriya [*Software Engineering*], 2017, no. 3, pp. 369–384 (in Russian).

11. Bibilo P. N. Razbienie sistemy bulevyh funkcij na podsistemy "svyazannyh" funkcij [Partitioning a system of Boolean functions into subsystems of "related" functions]. Izvestija Rossijskoj akademii nauk. Teoriya i sistem upravleniya [*Proceedings of the Russian Academy of Sciences. Theory and control systems*], 2019, no. 2, pp. 14–29 (in Russian).

12. SHlee M. Qt 5.3. Professional'noe programmirovanie na S++. *Qt 5.3. Professional C ++ Programming*. Saint Petersburg, BHV-Peterburg, 2015, 928 p. (in Russian).

13. Bibilo P. N., Romanov V. I. Logicheskoe proektirovanie diskretnyh ustrojstv s ispol'zovaniem produkcionno-frejmovoj modeli predstavlenija znanij. *Logical Design of Discrete Devices Using a Production-Frame Knowledge Representation Model*. Minsk, Belaruskaja navuka, 2011, 279 p. (in Russian).

14. Bibilo P. N., Avdeev N. A., Kardash S. N., Kirienko N. A., Lankevich Yu. Yu., …, Cheremisinova L. D. Sistema logicheskogo proektirovaniya funkcional'nyh blokov zakaznyh KMOP SBIS s ponizhennym energopotrebleniem [System for the logical design of functional blocks of custom CMOS VLSI with low power consumption]. Mikroelektronika [*Microelectronics*], 2017, vol. 46, no. 1, pp. 72–88 (in Russian).

15. Bibilo P. N. Cistemy proektirovaniya integral'nyh skhem na osnove yazyka VHDL. StateCAD, ModelSim, LeonardoSpectrum. *Integrated Circuit Design Systems Based on the VHDL Language. StateCAD, ModelSim, LeonardoSpectrum*. Moscow, SOLON-Press, 2005, 384 p. (in Russian).

16. Avdeev N. A., Bibilo P. N. Effektivnost' logicheskoj optimizacii pri sinteze kombinacionnyh skhem iz bibliotechnyh elementov [The effectiveness of logical optimization in the synthesis of combinational circuits from library elements]. Mikroelektronika [*Microelectronics*], 2015, vol. 44, no. 5, pp. 383–399 (in Russian).

17. Jeong C. Computer-aided design of digital systems. *Department of Computer Science*. Available at: http://www1.cs.columbia.edu/~cs6861/sis/espresso-examples/ex (accessed 20.03.2018).

Информация об авторах

Бибило Петр Николаевич, доктор технических наук, профессор, Объединенный институт проблем информатики Национальной академии наук Беларуси, Минск, Беларусь.
E-mail: bibilo@newman.bas-net.by

Позняк Андрей Михайлович, магистрант, Объединенный институт проблем информатики Национальной академии наук Беларуси, Минск, Беларусь.
E-mail: krucios@mail.ru

Information about the authors

Petr N. Bibilo, Dr. Sci. (Eng.), Professor, The United Institute of Informatics Problems of the National Academy of Sciences of Belarus, Minsk, Belarus.
E-mail: bibilo@newman.bas-net.by

Andrei M. Pazniak, Undergraduate, The United Institute of Informatics Problems of the National Academy of Sciences of Belarus, Minsk, Belarus.
E-mail: krucios@mail.ru

ISSN 1816-0301 (Print)
ISSN 2617-6963 (Online)

ОБРАБОТКА СИГНАЛОВ, ИЗОБРАЖЕНИЙ И РЕЧИ

SIGNAL, IMAGE AND SPEECH PROCESSING

УДК 616-71 + 612.78
https://doi.org/10.37661/1816-0301-2020-17-1-78-86

Поступила в редакцию 16.10.2019
Received 16.10.2019

Принята к публикации 12.12.2019
Accepted 12.12.2019

Анализ акустических параметров голоса для выявления заболеваний гортани

М. И. Вашкевич[1]✉, А. А. Бурак[1], Н. С. Конойко[2], В. С. Долдова[2]

[1]*Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь*
✉*E-mail: vashkevich@bsuir.by*

[2]*Республиканский научно-практический центр оториноларингологии, Минск, Беларусь*

Аннотация. Приведены результаты анализа двух способов описания голосового сигнала для решения задачи выявления заболеваний гортани. Сравнивались параметры голоса, определяемые клинической системой lingWaves, и параметры, получаемые в результате мел-частотного кепстрального анализа голоса. Для определения пригодности данных параметров при решении задачи выявления заболеваний гортани на их основе строился классификатор с использованием вероятностной модели – логистической регрессии. Для обучения классификатора была записана база голосов 60 человек, 30 из которых составляли контрольную группу, а другие 30 имели различные заболевания гортани (узелки голосовых складок, паралич гортани или функциональную дисфонию). Показано, что точность классификатора на основе мел-частотных кепстральных параметров (83,8 %) выше, чем точность классификатора на основе параметров, полученных в системе lingWaves (60,4 %).

Ключевые слова: анализ голоса, акустические параметры голоса, кепстральный анализ, детектирование патологии в голосе, логистическая регрессия

Для цитирования. Анализ акустических параметров голоса для выявления заболеваний гортани / М. И. Вашкевич [и др.] // Информатика. – 2020. − Т. 17, № 1. – С. 78–86. https://doi.org/10.37661/1816-0301-2020-17-1-78-86

Analysis of acoustic voice parameters for larynx pathology detection

Maxim I. Vashkevich[1]✉, Anton A. Burak[1], Natallia S. Kanoika[2], Valeria S. Daldova[2]

[1]*Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus*
✉*E-mail: vashkevich@bsuir.by*

[2]*Republican Scientific and Practical Center of Otorhinolaryngology, Minsk, Belarus*

Abstract. The comparative study of two types of voice signal representation for larynx pathology detection is presented. Parameters obtained in clinical system lingWaves compared to parameters obtained by mel-frequency cepstral analysis. The classifier based on the probabilistic model (logistic regression) was designed to determine the suitability of given parameters for the larynx pathology detection problem. To train the classifier, the base of voice samples of 60 persons was recorded, 30 of which constitute the control group, and the other 30 had various diseases of the larynx (nodules of the vocal folds, laryngeal paralysis, or functional dysphonia). The results show that the classifier based on mel-frequency cepstral parameters (83,8 %) higher than the classifier based on parameters obtained in lingWaves (60,4 %).

Keywords: voice analysis, acoustic voice parameters, cepstral analysis, voice pathology detection, logistic regression

For citation. Vashkevich M. I., Burak A. A., Kanoika N. S., Daldova V. S. Analysis of acoustic voice parameters for larynx pathology detection. *Informatics*, 2020, vol. 17, no. 1, pp. 78−86 (in Russian). https://doi.org/10.37661/1816-0301-2020-17-1-78-86

Введение. Человеческий голос, и как акустический феномен, и как анатомо-физиологическое действие, а также по своему социальному значению, – явление в своем роде уникальное. Голос служит не только средством передачи информации и общения между людьми, но и своеобразным орудием производства у представителей ряда профессий: преподавателей, экскурсоводов, диспетчеров и др. Пациенты с нарушениями голоса испытывают физические и психологические затруднения в общении, формирующие чувство неполноценности или более глубокие психические осложнения [1].

Изменения в звучании голоса могут предшествовать структурным изменениям в ЛОР-органах. Поэтому естественно полагать, что существенная информация о состоянии голосового аппарата пациента отражается в характере звучания его голоса. Извлечь эту информацию можно лишь путем соответствующего акустического анализа голоса [2]. Преимуществом такого анализа является то, что он позволяет получить объективное представление о качестве голоса [3].

В настоящее время в Республиканском научно-практическом центре оториноларингологии для акустического анализа голоса используется аппаратно-программный комплекс lingWaves ver. 2.5 (Германия). Самым трудным и важным этапом анализа является интерпретация данных акустического исследования, поскольку часто его результаты неоднозначны.

Цель работы – анализ акустических параметров, выделяемых программой lingWaves с точки зрения их пользы для задачи выявления заболеваний гортани. Для достижения поставленной цели ставится задача построения бинарного классификатора для определения голосов с патологией. Для сравнения предлагается использовать два набора признаков, описывающих голосовой сигнал: рассчитанных в системе lingWaves и полученных в результате мел-кепстрального представления голосового сигнала [4]. Эти наборы признаков предлагается применять для обучения детектора патологии в голосе на основе логистической регрессионной модели. Сравнительный анализ полученных детекторов позволит определить прогностическую ценность применяемых в них параметров.

Анализ голоса в системе lingWaves. При использовании системы lingWaves голос записывается с помощью микрофона, оснащенного встроенным измерителем уровня шума. Оптимальным режимом для записи голоса считается уровень шума не более 40 дБ. Микрофон следует располагать на расстоянии 30 см от рта исследуемого. В качестве тестового сигнала записывают протяжный звук /*a*/ с частотой дискретизации F_s 44,1 кГц. Пример отчета, получаемого в результате анализа голоса в системе lingWaves, показан на рис. 1.

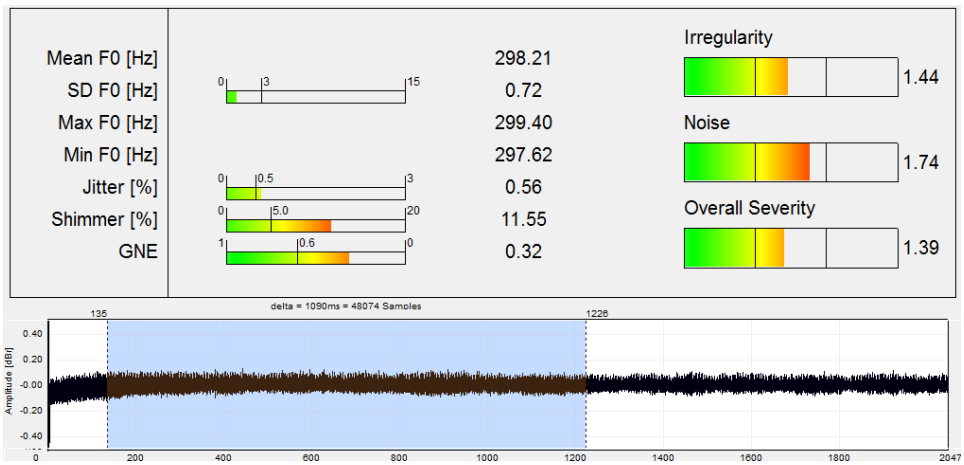


Рис. 1. Пример отчета lingWaves

Основными показателями, позволяющими оценить состояние голосовой функции, служат частота основного тона f_o; степень частотной нестабильности вибрации голосовых складок, или джиттер (от англ. jitter – дрожание), и аналогичная мера амплитудной нестабильности – шиммер (от англ. shimmer – мерцание); соотношение шума и гармонических компонентов (harmonic/noise ratio, HNR); гортанно-шумовой коэффициент (glottal noise excitation ratio, GNE). Дополнительными обобщающими параметрами голоса являются нерегулярность (irregularity), шум (noise) и общая тяжесть дисфонии (overall severity). Приведенные параметры рассчитывались для исследуемой базы голосов и использовались для обучения детектора на основе логистической регрессии.

Мел-кепстральное представление голосового сигнала. В качестве альтернативного способа описания голосового сигнала в работе использовалось его мел-частотное кепстральное представление [4]. Расчет мел-частотных кепстральных коэффициентов (МЧКК) относится к методам кратковременного анализа голосового сигнала, которые предполагают разбиение сигнала на интервалы (кадры) анализа [5]. Как правило, в интервале от 10 до 30 мс голосовой сигнал можно считать стационарным. Рассматриваемый в настоящей статье анализ выполнялся на интервалах длительностью 20 мс, которые имели перекрытие 10 мс. Вычисление МЧКК производилось в частотной шкале мелов, которая учитывает специфику восприятия высоты звука человеческим ухом [6].

В результате кратковременного анализа формируется большой набор МЧКК, которые описывают локальную структуру сигнала. Для перехода к более глобальному представлению и уменьшению объема данных получающиеся МЧКК усредняются для формирования надсегментного вектора признаков.

В работе использовался следующий алгоритм мел-частотного кепстрального анализа:

Шаг 1. Коррекция спектра сигнала, заключающаяся в выравнивании энергий высокочастотной и низкочастотной составляющих при помощи фильтра, который имеет подъем амплитудно-частотной характеристики приблизительно 6 дБ на октаву:

$$s(n) = x(n) - 0{,}82 \cdot x(n-1).$$

Шаг 2. Разбиение сигнала на кадры длительностью N отсчетов (и с перекрытием в $N/2$ отсчетов) и взвешивание их с помощью окна Хэмминга:

$$w(n) = 0{,}54 + 0{,}46 \cdot \cos\left(2\pi n / N\right).$$

Далее для всех кадров $s_t(n)$, где t – номер кадра, выполняются шаги 3–6.

Шаг 3. Расчет кратковременного спектра при помощи быстрого преобразования Фурье (БПФ) для каждого анализируемого кадра:

$$S_t(k) = \sum_{n=0}^{N-1} w(n) \cdot s_t(n) \cdot e^{\frac{-j2\pi kn}{N}}, \quad k = 0, 1, ..., N-1.$$

Шаг 4. Расчет набора из M фильтров ($m = 1, 2, ..., M$) треугольной формы:

$$H_m(k) = \begin{cases} 0, & k < f(m-1); \\ \dfrac{k - f(m-1)}{f(m) - f(m-1)}, & f(m-1) \le k \le f(m); \\ \dfrac{f(m+1) - k}{f(m+1) - f(m)}, & f(m) \le k \le f(m+1); \\ 0, & k > f(m+1), \end{cases}$$

которые используются для усреднения спектра вблизи центральных частот $f(m)$, расположенных равномерно в шкале мелов (рис. 2). В данном расчете параметр $M = 19$ обозначает число критических полос в анализируемом частотном диапазоне.

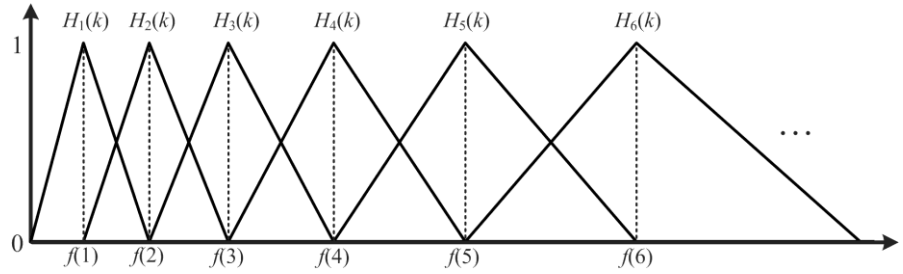


Рис. 2. Треугольные фильтры для вычисления мел-спектра

Если f_l и f_h – нижняя и верхняя границы частотного диапазона (Гц), который покрывает набор фильтров, то граничные частоты $f(m)$, равномерно расположенные в шкале мелов, рассчитываются по формуле [6]

$$f(m) = \frac{N}{F_s} B^{-1}\left(B(f_l) + m\frac{B(f_h) - B(f_l)}{M+1} \right),$$

где функция B осуществляет переход от шкалы герцев к шкале мелов:

$$B(f) = 1127 \cdot \ln(1 + f / 700).$$

Значения f_l и f_h выбирались равными 50 и 5300 Гц соответственно. Указанный диапазон частот соответствует первым 19 критическим полосам слуха. Кроме того, в него попадает основная энергия анализируемого в данной работе гласного звука /*a*/.

Шаг 5. Применение набора фильтров, полученного на шаге 4, для расчета логарифма от энергии на выходе каждого фильтра:

$$Y_t(m) = \ln\left(\sum_{k=0}^{N-1} |S_t(k)|^2 \cdot H_m(k) \right), \quad 0 \le m < M.$$

Шаг 6. Вычисление МЧКК при помощи дискретного косинусного преобразования:

$$c_t(k) = \sum_{m=0}^{M-1} Y_t(m) \cdot \cos\left(\pi k (m + 1/2) / M \right),$$

где $k = 0,\ 1,\ ...,\ M-1$.

В формировании вектора признаков участвовали P начальных коэффициентов ($k = 1, 2,\ ..., P$), использовалось значение $P = 12$.

Шаг 7. Вычисление конечных разностей МЧКК, которые применяются наряду с МЧКК в качестве информационных признаков:

$$\Delta c_t(k) = c_t(k) - c_{t-1}(k),$$

где $c_t(k)$ – это *k*-й коэффициент, вычисленный для кадра с номером t.

Шаг 8. Выполнение расчета надсегментных признаков на основе МЧКК для получения характеристического вектора. Для этого последовательности $c_t(k)$ и $\Delta c_t(k)$ разбиваются на сегменты длительностью 0,8 с, по которым вычисляются их средние значения $c^{\mu}(k)$, $\Delta c^{\mu}(k)$ и среднеквадратические отклонения (СКО) $c^{\sigma}(k)$ и $\Delta c^{\sigma}(k)$.

В результате для каждого сегмента был получен следующий вектор признаков:

$$\mathbf{x} = \left[c^{\mu}(1), ..., c^{\mu}(P);\ \ \Delta c^{\mu}(1), ..., \Delta c^{\mu}(P);\ c^{\sigma}(1), ..., c^{\sigma}(P);\ \ \Delta c^{\sigma}(1), ..., \Delta c^{\sigma}(P) \right]. \quad (1)$$

Описанный процесс анализа голосового сигнала проиллюстрирован на рис. 3.

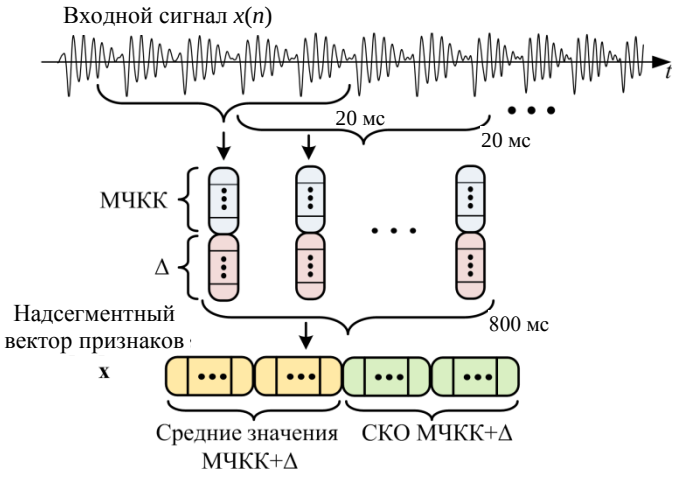


Рис. 3. Получение вектора надсегментных признаков на основе МЧКК

Детектор патологии в голосе на основе логистической регрессии. Определение наличия патологии в голосе является задачей бинарной классификации. В данной работе классификатор строился на основе распространенной вероятностной дискриминантной модели – логистической регрессии [7].

Логистическая регрессия моделирует апостериорную вероятность принадлежности характеристического вектора $\mathbf{x}$ к классу $y=1$:

$$P(y=1|\,\mathbf{x})=f(z),\quad z=\boldsymbol{\theta}^T\mathbf{x},\quad f(z)=\frac{1}{1+e^{-z}},\tag{2}$$

где $\mathbf{x}$ – вектор-столбец признаков (1), к которому добавлена компонента с единичным значением для перехода к однородным координатам; $\boldsymbol{\theta}$ – вектор-столбец параметров регрессии. Для определения $\boldsymbol{\theta}$ использовался метод, основанный на максимизации функции условного правдоподобия:

$$\hat{\boldsymbol{\theta}}=\underset{\boldsymbol{\theta}}{\operatorname{argmax}}\,CL(\boldsymbol{\theta}),\quad CL(\boldsymbol{\theta})=\prod_{i=1}^{m}P(y_i\mid\mathbf{x}^{(i)})=\prod_{i=1}^{m}\hat{p}\left(\mathbf{x}^{(i)}\right)^{y_i}\left(1-\hat{p}\left(\mathbf{x}^{(i)}\right)\right)^{(1-y_i)},$$

где m – количество примеров в обучающей выборке.

Для упрощения формул лучше использовать логарифм функции правдоподобия:

$$LCL(\boldsymbol{\theta})=\ln CL(\boldsymbol{\theta})=\sum_{i=1}^{m}y^{(i)}\ln f(\boldsymbol{\theta}^T\mathbf{x}^{(i)})+(1-y^{(i)})\ln(1-f(\boldsymbol{\theta}^T\mathbf{x}^{(i)})).\tag{3}$$

Поиск оптимального значения параметра $\boldsymbol{\theta}$, минимизирующего (3), выполнялся посредством метода градиентного спуска [7]:

$$\boldsymbol{\theta}'=\boldsymbol{\theta}+\alpha\nabla\ln CL(\boldsymbol{\theta})=\boldsymbol{\theta}+\alpha\sum_{i=1}^{m}(y^{(i)}-f(\boldsymbol{\theta}^T\mathbf{x}^{(i)}))\mathbf{x}^{(i)},\ \alpha>0.$$

После обучения, в результате которого находится оптимальное значение параметра $\boldsymbol{\theta}$, процесс бинарной классификации выполняется следующим образом. Для поступающего вектора признаков $\mathbf{x}$ вычисляется вероятность по формулам (2). Если полученное значение вероятности больше $0{,}5$, то $\mathbf{x}$ относился к классу «патология» ($y=1$), в противном случае – к классу «норма» ($y=0$).

Отбор признаков и оценка производительности классификатора. Отбор признаков для классификатора является важной задачей, от решения которой во многом зависит качество его работы. В исследовании для отбора признаков использовался метод LASSO (от англ. least absolute shrinkage and selection operator) [8]. Этот метод основан на решении задачи линейной регрессии со штрафной функцией, накладываемой на абсолютные значения коэффициентов

линейной модели. Задача решается для различных (возрастающих) значений параметра регуляризации λ, в результате чего веса при некоторых признаках (предикторах) линейной модели приближаются к нулю или становятся равными нулю. Фиксируя порядок, в котором модель отбрасывает признаки, можно ранжировать их по значимости, так как первыми исключаются наименее значимые признаки.

Для оценки производительности классификатора использовался метод перекрестной проверки по *K* блокам (англ. *K*-fold cross-validation) [7], которая заключается в следующем. Исходный набор данных перемешивается случайным образом и разбивается на *K* блоков. Далее выполняется обучение классификатора, причем один из блоков выступает как тестовый набор, а оставшиеся $K-1$ в совокупности составляют обучающий набор. Эта процедура повторяется *K* раз таким образом, чтобы каждый блок один раз выступил в роли тестового набора. Метки, присвоенные классификаторами, для тестовых наборов сохраняются, и по ним выполняется оценка производительности классификатора. В качестве основных характеристик классификатора вычислялись точность (accuracy), чувствительность (sensitivity) и специфичность (specificity):

$$\text{acc} = \frac{TP + TN}{TP + TN + FP + FN}, \quad \text{sens} = \frac{TP}{TP + FN}, \quad \text{spec} = \frac{TN}{TN + FP},$$

где TP, TN, FP, FN – количество истинно положительных и истинно отрицательных, ложно положительных и ложно отрицательных результатов классификации соответственно. Процедура перекрестной проверки повторялась 40 раз, после чего вычислялись выборочное среднее и выборочное СКО для оценок точности, чувствительности и специфичности.

Результаты экспериментов. В исследовании использовалась база голосов, записанная в фониатрическом отделении Республиканского научно-практического центра оториноларингологии. Всего были выполнены записи образцов голосов 60 человек, 30 из которых были здоровыми, а 30 имели различные заболевания гортани (18 – узелки голосовых складок, 6 – парез или паралич гортани, 8 – функциональную дисфонию). Все записанные звуковые файлы были обезличены, им присвоены буквенно-цифровые коды. Также записи звука не содержали никаких персональных данных (имя, возраст и пр.).

Для получения предварительного представления о статистических свойствах признаков, описывающих голосовой сигнал, выполнялся их корреляционный анализ. Для всех пар $(x_{i,j}, y_i)$ вычислялся коэффициент корреляции R, где $x_{i,j}$ – *j*-й признак *i*-го примера из соответствующего набора, а y_i – метка класса для *i*-го примера (голоса с патологией имели метку «1», а здоровые – «–1»). Результаты корреляционного анализа для первого набора признаков приведены в табл. 1.

Полученные результаты показывают, что лишь три признака (нерегулярность, шум и GNE) имеют статистически значимый ($p < 0,05$) коэффициент корреляции (в табл. 1 они выделены жирным шрифтом). Для признаков, связанных с частотой основного тона, низкая корреляция ожидаема, поскольку они сильно зависят от пола и возраста. Однако низкая корреляция параметров «джиттер» и «шиммер» – неожиданное явление, так как считается, что при патологии голоса эти показатели имеют повышенные значения. Признак общей тяжести дисфонии не использовался, поскольку было установлено, что он является линейной комбинацией параметров «нерегулярность» и «шум»:

$$\text{общая тяжесть дисфонии} = 0,8 \cdot \text{нерегулярность} + 0,135 \cdot \text{шум}.$$

В табл. 2 представлены результаты корреляционного анализа для второго набора признаков: перечислены девять признаков, имеющих наибольшие коэффициенты корреляции. Приведенные результаты показывают, что признаки, полученные на основе анализа МЧКК, имеют гораздо большую корреляционную связь с наличием патологии в голосе, чем параметры, получаемые в lingWaves. Следует заметить, что выполненный корреляционный анализ направлен на выявление лишь линейной зависимости между параметрами голосового сигнала и меткой класса голоса. В данной работе не предпринимались попытки поиска более сложных нелинейных зависимостей.

Таблица 1

Результат анализа признаков lingWaves

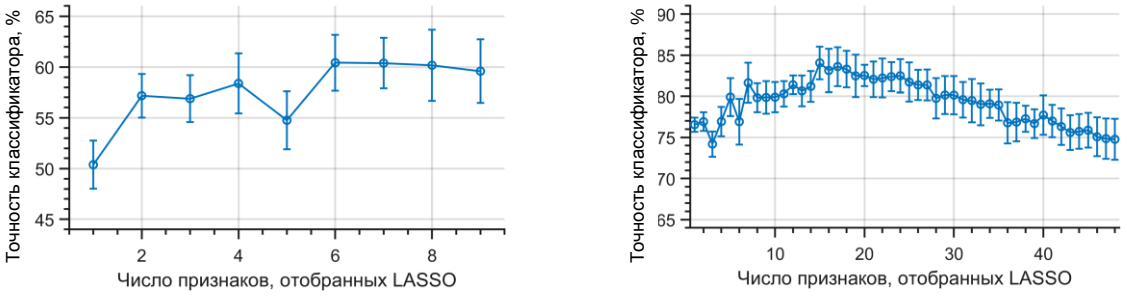
Признак	Коэффициент корреляции R (уровень значимости p)	Границы 95 % доверительного интервала
Нерегулярность	**0,27 (p = 0,03)**	[0,022; 0,49]
Шум	**0,27 (p = 0,04)**	[0,015; 0,49]
GNE	**–0,27 (p = 0,04)**	[–0,49; –0,014]
Джиттер	0,19 (p = 0,14)	[–0,07; 0,42]
min f_o	0,18 (p = 0,18)	[–0,08; 0,41]
СКО f_o	0,17 (p = 0,20)	[–0,09; 0,41]
Среднее f_o	0,14 (p = 0,28)	[–0,12; 0,38]
max f_o	0,12 (p = 0,37)	[–0,14; 0,36]
Шиммер	0,06 (p = 0,65)	[–0,20; 0,31]

Таблица 2

Результат анализа признаков на основе МЧКК

Признак	Коэффициент корреляции R (уровень значимости p)	Границы 95 % доверительного интервала
$\Delta c^{\sigma}(10)$	**0,46 ($p = 1{,}8 \cdot 10^{-16}$)**	[0,37; 0,55]
$c^{\mu}(7)$	**–0,44 ($p = 4{,}6 \cdot 10^{-15}$)**	[–0,53; –0,34]
$c^{\mu}(8)$	**–0,42 ($p = 3{,}0 \cdot 10^{-13}$)**	[–0,51; –0,31]
$\Delta c^{\sigma}(8)$	**0,41 ($p = 3{,}4 \cdot 10^{-13}$)**	[0,31; 0,51]
$\Delta c^{\sigma}(9)$	**0,40 ($p = 1{,}6 \cdot 10^{-12}$)**	[0,30; 0,50]
$\Delta c^{\sigma}(6)$	**0,40 ($p = 2{,}4 \cdot 10^{-12}$)**	[0,30; 0,49]
$\Delta c^{\sigma}(12)$	**0,40 ($p = 3{,}6 \cdot 10^{-12}$)**	[0,29; 0,49]
$\Delta c^{\sigma}(7)$	**0,39 ($p = 9{,}3 \cdot 10^{-12}$)**	[0,29; 0,49]
$\Delta c^{\sigma}(11)$	**0,38 ($p = 3{,}4 \cdot 10^{-11}$)**	[0,28; 0,48]

На рис. 4 показаны результаты классификации в зависимости от набора и числа информационных признаков. Из приведенных графиков видно, что точность классификатора с признаками на основе МЧКК в целом выше, чем точность классификатора на основе признаков lingWaves. В табл. 3 приведены параметры классификаторов с максимальной точностью, полученных на основе набора признаков lingWaves (оптимальное число признаков – 6) и набора надсегментных МЧКК (оптимальное число признаков – 15). Интересно, что добавление признака «шиммер» (шестого по счету на рис. 4, *а*) значительно улучшает точность правильной классификации, хотя корреляционный анализ (см. табл. 1) не выявил его значимости. Это говорит о том, что данный параметр содержит важную дополнительную информацию в контексте других признаков.



а) *б)*

Рис. 4. Производительность классификатора в зависимости от числа используемых признаков: *а)* набор признаков lingWaves; *б)* набор признаков на основе МЧКК

Таблица 3

Результаты классификации, %

Набор признаков	Подмножество признаков (в порядке убывания значимости)	Точность	Чувствительность	Специфичность
lingWaves	Нерегулярность, шум, GNE, max_f_0, СКО_ f_0, шиммер	60,4 ± 2,7	55,3 ± 4,7	65,6 ± 4,0
Надсегментарные МЧКК	$\Delta c^{\sigma}(10)$, $c^{\mu}(7)$, $c^{\mu}(8)$, $c^{\mu}(11)$, $c^{\mu}(5)$, $c^{\mu}(1)$, $c^{\sigma}(8)$, $c^{\mu}(2)$, $c^{\sigma}(4)$, $c^{\sigma}(11)$, $c^{\mu}(3)$, $c^{\sigma}(1)$, $c^{\sigma}(2)$, $c^{\sigma}(3)$, $c^{\sigma}(6)$	83,8 ± 1,2	74,5 ± 1,8	88,7 ± 1,7

Заключение. Проведенное исследование показало, что параметры голоса, определяемые в системе lingWaves, в целом дают недостаточно информации, чтобы выявить наличие патологических изменений в голосе. Напротив, использование надсегментных признаков на основе МЧКК позволяет значительно повысить вероятность правильного детектирования патологии

голоса. Преимущество параметров, выделяемых системой lingWaves, заключается в том, что они имеют ясную интерпретацию и понятны для врача-фониатра. Следовательно, существует насущная задача конструирования таких признаков патологии голоса, которые бы, с одной стороны, повышали вероятность выявления патологии, а с другой – имели вполне ясную интерпретацию для врача-специалиста.

Выполнен анализ акустических параметров голоса применительно к задаче выявления заболеваний гортани. Проанализированы наборы признаков, получаемых в системе lingWaves, которая используется во многих медицинских центрах СНГ и Европы, а также признаков, получаемых в результате кепстрального анализа голосового сигнала. Для сравнения данных наборов признаков на их основе выполнено обучение классификаторов на базе логистической регрессии. Точность классификатора на основе признаков lingWaves составила 60,4 %, а на основе признаков, полученных в результате кепстрального анализа, – 83,8 %. Несмотря на то что кепстральные признаки обладают большей информативностью, следует отметить и их недостаток – отсутствие ясной интерпретации, понятной для врача-фониатра.

Список использованных источников

1. Шиленкова, В. В. Дисфонии и голос / В. В. Шиленкова. – Ярославль : Аверс Плюс, 2018. – 256 с.

2. Ермолаев, В. Г. Руководство по фониатрии / В. Г. Ермолаев, Н. Ф. Лебедева, В. П. Морозов. – Л. : Медицина, Ленинград. отд., 1970. – 271 с.

3. Коротченко, В. В. Акустический анализ голоса у детей в норме и при заболеваниях гортани : автореф. дис. … канд. мед. наук / В. В. Коротченко ; Мин-во здравоохр. и соц. развития РФ, Ярославская гос. мед. академия. – М., 2012. – 24 с.

4. Automatic detection of laryngeal pathologies in records of sustained vowels by means of mel-frequency cepstral coefficient parameters and differentiation of patients by sex / R. Fraile [et al.] // Folia Phoniatrica Logopaedica. – 2009. – Vol. 61. – P. 146–152.

5. Рылов, А. С. Анализ речи в распознающих системах / А. С. Рылов. – Минск : Бестринт, 2003. – 264 с.

6. Huang, X. Spoken Language Processing: a Guide to Theory, Algorithm and System Development / X. Huang, A. Acero, H.-W. Hon. – New Jersey : Prentice Hall, 2001. – 1009 p.

7. Флах, П. Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных : пер. с англ. / П. Флах. – М. : ДМК Пресс, 2015. – 400 с.

8. Tibshirani, R. Regression shrinkage and selection via the Lasso / R. Tibshirani // J. of the Royal Statistical Society. – 1996. – Vol. 58, no. 1. – P. 267–288.

References

1. Shilenkova V. V. Disfonii i golos. *Dysphonies and Voice*. Yaroslavl, Avers Pljus, 2018, 256 p. (in Russian).

2. Ermolayev V. G., Lebedeva N. F., Morozov V. P. Rukovodstvo po foniatrii. *Phoniatrics Guide*. Leningrad, Medicina, Leningradskoe otdelenie, 1970, 271 p. (in Russian).

3. Korotchenko V. V. Akusticheskij analiz golosa u detej v norme i pri zabolevaniyax gortani. Avtoref. dis. … kand. med. nauk. *Acoustic Analysis of Voice in Children Is Normal and with Diseases of the Larynx*. *Cand. med. sci. diss. abstr*. Ministerstvo zdravoohranenija i social'nogo razvitija Rossijskoj Federacii, Jaroslavskaja gosudarstvennaja medicinskaja akademija. Moscow, 2012, 24 p. (in Russian).

4. Fraile R., Sáenz-Lechón N., Godino-Llorente J., Osma-Ruiz V., Fredouille C. Automatic detection of laryngeal pathologies in records of sustained vowels by means of mel-frequency cepstral coefficient parameters and differentiation of patients by sex. *Folia Phoniatrica Logopaedica*, 2009, vol. 61, pp. 146–152.

5. Rilov A. S. Analiz rechi v raspoznajushhih sistemah. *Speech Analysis in Recognition Systems*. Minsk, Bestprint, 2003, 264 p. (in Russian).

6. Huang X., Acero A., Hon H.-W. *Spoken Language Processing: a Guide to Theory, Algorithm and System Development*. New Jersey, Prentice Hall, 2001, 1009 p.

7. Flach P. *Machine Learning. The Art and Science of Algorithms that Make Sense of Data*. Cambridge University Press, 2012, 409 p.

8. Tibshirani R. Regression shrinkage and selection via the Lasso. *Journal of the Royal Statistical Society*, 1996, vol. 58, no. 1, pp. 267–288.

Информация об авторах

Вашкевич Максим Иосифович, кандидат технических наук, доцент кафедры электронных вычислительных средств, Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь.
E-mail: vashkevich@bsuir.by

Бурак Антон Андреевич, студент, Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь.

Конойко Наталья Сергеевна, заведующий фониатрическим отделением, Республиканский научно-практический центр оториноларингологии, Минск, Беларусь.

Долдова Валерия Сергеевна, врач-фониатр фониатрического отделения, Республиканский научно-практический центр оториноларингологии, Минск, Беларусь.

Information about the authors

Maxim I. Vashkevich, Cand. Sci. (Eng.), Associate Professor of Computer Engineering Department, Belarusian State University of Informatics and Radioelectronics Minsk, Belarus.
E-mail: vashkevich@bsuir.by

Anton A. Burak, Student, Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus.

Natallia S. Kanoika, Head of the Phoniatric Department, Republican Scientific and Practical Center of Otorhinolaryngology, Minsk, Belarus.

Valeria S. Daldova, Phoniatrist of the Phoniatric Department, Republican Scientific and Practical Center of Otorhinolaryngology, Minsk, Belarus.

ISSN 1816-0301 (Print)
ISSN 2617-6963 (Online)

УДК 004.93
https://doi.org/10.37661/1816-0301-2020-17-1-87-101

Поступила в редакцию 08.01.2020
Received 08.01.2020

Принята к публикации 10.02.2020
Accepted 10.02.2020

Сравнительный анализ оценок качества бинарной классификации

В. В. Старовойтов✉, Ю. И. Голуб

Объединенный институт проблем информатики
Национальной академии наук Беларуси, Минск, Беларусь
✉E-mail: valerys@newman.bas-net.by

Аннотация. Приведены данные аналитического и экспериментального анализов 17 функций, используемых для оценки результатов бинарной классификации произвольных данных. Результаты классификации представлены матрицами ошибок размером 2×2. Исследованы поведение и свойства основных функций, вычисляемых по элементам этих матриц. Анализируются варианты классификации со сбалансированными и несбалансированными классами данных. Показано, что между отдельными функциями существуют линейные зависимости. Многие функции инвариантны к транспонированию матриц ошибок, что позволяет вычислять оценки, не уточняя порядок записи данных в эти матрицы.

Доказано, что все классические функции (Sensitivity, Specificity, Precision, Accuracy, F1, F2, GM, индекс Жаккара) чувствительны к дисбалансу классифицируемых данных и искажают оценки при ошибках классификации объектов меньшего класса. Чувствительность к дисбалансу имеется у коэффициента корреляции Мэтьюса и каппы Коэна. Экспериментально показано, что такие функции, как энтропия ошибки (confusion entropy), степень разделимости (discriminatory power) и диагностическое отношение шансов (diagnostic odds ratio), не стоит использовать для анализа результатов бинарной классификации несбалансированных классов. Две последние функции инвариантны к дисбалансу классифицируемых данных, но плохо оценивают результаты с примерно равным суммарным процентом ошибок классификации.

Доказано, что площадь под ROC-кривой (AUC) и индекс Юдена, вычисляемые по матрице ошибок бинарной классификации, линейно зависимы и являются наиболее подходящими оценочными функциями для сравнения результатов бинарной классификации как сбалансированных, так и несбалансированных данных.

Ключевые слова: бинарная классификация, матрица ошибок, функции точности классификации, площадь под ROC-кривой, индекс Юдена

Для цитирования. Старовойтов, В. В. Сравнительный анализ оценок качества бинарной классификации / В. В. Старовойтов, Ю. И. Голуб // Информатика. – 2020. − Т. 17, № 1. – С. 87–101. https://doi.org/10.37661/1816-0301-2020-17-1-87-101

Comparative study of quality estimation of binary classification

Valery V. Starovoitov✉, Yuliya I. Golub

The United Institute of Informatics Problems of the National Academy
of Sciences of Belarus, Minsk, Belarus
✉E-mail: valerys@newman.bas-net.by

Abstract. The paper describes results of analytical and experimental analysis of seventeen functions used for evaluation of binary classification results of arbitrary data. The results are presented by 2×2 error matrices. The behavior and properties of the main functions calculated by the elements of such matrices are studied. Classification options with balanced and imbalanced datasets are analyzed. It is shown that there are linear dependencies between some functions, many functions are invariant to the transposition of the error matrix,

which allows us to calculate the estimation without specifying the order in which their elements were written to the matrices.
It has been proven that all classical measures such as Sensitivity, Specificity, Precision, Accuracy, F1, F2, GM, the Jacquard index are sensitive to the imbalance of classified data and distort estimation of smaller class objects classification errors. Sensitivity to imbalance is found in the Matthews correlation coefficient and Kohen's kappa. It has been experimentally shown that functions such as the confusion entropy, the discriminatory power, and the diagnostic odds ratio should not be used for analysis of binary classification of imbalanced datasets. The last two functions are invariant to the imbalance of classified data, but poorly evaluate results with approximately equal common percentage of classification errors in two classes.
We proved that the area under the ROC curve (AUC) and the Yuden index calculated from the binary classification confusion matrix are linearly dependent and are the best estimation functions of both balanced and imbalanced datasets.

Keywords: binary classification, confusion matrix, functions of Accuracy classification, area under ROC curve, Youden's index

For citation. Starovoitov V. V., Golub Y. I. Comparative study of quality estimation of binary classification. *Informatics*, 2020, vol. 17, no. 1, pp. 87−101 (in Russian). https://doi.org/10.37661/ 1816-0301-2020-17-1-87-101

Введение. Следует отметить, что распознавание и классификация часто трактуются как синонимы. Например, в работе [1] задача распознавания образов формулируется как классификация заданного множества объектов. На взгляд авторов, это схожие, но отличающиеся понятия. Под классификацией понимается отнесение заданного объекта к одному или нескольким классам, определенным заранее. В данном случае термин «распознавание» можно использовать как синоним классификации. Процесс распознавания имеет самостоятельное значение, если речь идет о выявлении объекта с последующим отнесением его к классу из заданного множества. Например, при распознавании текста или дорожных знаков на изображениях, если большую часть кадра занимает один знак и требуется определить, что это за знак, – это задача классификации изображений как объектов; если же требуется найти знак на изображении и опознать его, – это задача распознавания изображений.

Задачи классификации делятся на бинарные (имеются объекты только двух классов) и многоклассовые. Классификация может быть выполнена с непересекающимися классами и с пересекающимися, когда один объект может принадлежать нескольким классам. Термин «классификация» также можно использовать при диагностике заболевания и определении стадии этого заболевания. Если количество объектов разных классов представлено значениями одного порядка, классы называются сбалансированными [2]. Если же объемы классов различаются на порядок и более, то они называются несбалансированными. Например, в банковской сфере среди огромного числа легальных транзакций по кредитным картам встречается небольшое число (на несколько порядков меньше) мошеннических. Задачи медицинской диагностики также часто содержат несбалансированные классы анализируемых данных, так как здоровых людей больше, чем больных, а больных с начальными стадиями заболевания, как правило, больше, чем с последними.

На сайте kaggle.com в конкурсе по определению мошенничества с поддельными банковскими транзакциями данные представляли собой 284 807 корректных транзакций и 492 ложные (0,172 % от всех операций). Дисбаланс классов составляет 578:1. Тривиальный (необученный) классификатор относит все операции к классу корректных, при этом он имеет высокое значение функции Accuracy (99,827 %) и низкое значение функций Precision и Recall (0,0 %), однако ни одна ложная транзакция не будет выявлена.

Часто результаты работы классификаторов оцениваются по матрицам ошибок (confusion matrix). В табл. 1 представлены объекты верно определенных классов (true) и ошибочно определенных классов (false) для одной из таких матриц.

Таблица 1

Матрица ошибок бинарной классификации

Предсказанный класс	Истинная классификация	
	Класс 1	Класс 2
Класс 1	True Positive (tp)	False Positive (fp)
Класс 2	False Negative (fn)	True Negative (tn)
Число объектов в классе	tp + fn = общее число объектов класса 1	fp + tn = общее число объектов класса 2

Функции оценки результатов бинарной классификации данных. В статье [3] приведены формулы вычисления 76 функций, а в [4] описаны 44 функции оценки результатов бинарной классификации. В обоих работах сравнительный анализ функций и рекомендации по их применению отсутствуют. В статье [5] даны формулы пяти наиболее распространенных функций оценки результатов бинарной классификации, представленных матрицей ошибок, и исследованы некоторые свойства этих функций. Опишем исследуемые в настоящей работе функции оценки результатов бинарной классификации, представленных матрицей ошибок (табл. 2).

Наиболее простой для вычислений и популярной оценкой классификаторов является функция Accuracy. Она имеет парадоксальное свойство (Accuracy Paradox): в случае несбалансированных данных классификаторы с меньшим значением Accuracy могут давать лучший прогноз при решении прикладных задач, чем классификаторы, имеющие более высокие значения этого параметра [6]. Отметим, что функция Accuracy определяет долю правильных ответов. Кратко ее название можно перевести как правильность, и не рекомендуется называть ее точностью. Точностью в переводе с английского называют функцию Precision.

Отметим, что логистическая функция ошибки LogLoss также активно используется для оценки результатов бинарной классификации, но ее невозможно вычислить по матрице ошибок. Она рассчитывается через вероятности принадлежности к заданным классам, поэтому в данной статье не рассматривается.

В литературе встречаются функции, которые являются линейно преобразованными вариантами функций, приведенных в табл. 2. Например, функция Recall (или полнота) идентична функции Sensitivity, Error = 1–Accuracy, коэффициент Gini = 2·AUC–1 [5]. Далее эти функции в настоящей работе не рассматриваются.

Функции 1–7 (табл. 2) отнесем к первой группе. Они используют два-три из четырех элементов матрицы ошибок и в одиночку не дают объективной оценки результатов классификации данных.

Вторая группа – это функции 8–11. Они популярны, просты и используют все четыре элемента матрицы ошибок. Функция F1 – это гармоническое среднее между Recall и Precision, функция GM – геометрическое среднее этих же величин, F2 – вариант функции F1, в котором значение Precision имеет больший вес. Функции F1 и F2 так же, как Accuracy, Recall и Precision, точнее оценивают результаты классификации доминирующего множества при несбалансированных данных [7]. Отметим, что индекс Жаккара и функция F1 связаны следующими нелинейными зависимостями:

$$\text{индекс Жаккара} = F1 / (2 - F1), \quad F1 = 2 \cdot \text{индекс Жаккара} / (1 + \text{индекс Жаккара}).$$

Функция 11 вычисляет площадь под ROC-кривой (ROC – receiver operating characteristic), которую обозначают AUC (area under curve). Ее значения варьируются от 0,5 до 1. Подробнее о свойствах AUC можно прочитать в статье [8]. ROC-кривая строится численно (вычислительной формулы нет) как функция fp от величины tp, значения этих двух параметров могут изменяться от 0 до 1. Кривую можно построить только в случае бинарной классификации данных, фиксируя значения одного из параметров (fp или tp) и вычисляя значение второго параметра.

Таблица 2

Функции оценки результатов бинарной классификации

Наименование	Математическое выражение
1. False positive rate (FPR), ложноположительный коэффициент	$\frac{fp}{fp + tn}$
2. False negative rate (FNR), ложноотрицательный коэффициент	$\frac{fn}{fn + tp}$
3. Sensitivity или Recall, чувствительность	$\frac{tp}{tp + fn}$
4. Specificity, специфичность	$\frac{tn}{tn + fp}$
5. Precision, точность	$\frac{tp}{tp + fp}$
6. Accuracy, правильность	$\frac{tp + tn}{n}$
7. Jaccard index, индекс Жаккара	$\frac{tp}{tp + fn + fp}$
8. F1, гармоническое среднее	$\frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$ при $\beta = 1$
9. F2, взвешенное гармоническое среднее	$\frac{(1 + \beta^2) \cdot \text{Precision} \cdot \text{Recall}}{\beta^2 \cdot \text{Precision} + \text{Recall}}$ β любое
10. Geometric mean (GM), геометрическое среднее	$\sqrt{\text{Precision} \cdot \text{Recall}}$
11. Area under ROC curve (AUC) [5], площадь под ROC-кривой	$\frac{\text{Sensitivity} + \text{Specificity}}{2}$
12. Cohen's kappa [9], каппа Коэна	$\frac{(tp + fp)(tp + fn) + (fn + tn)(fp + tn)}{n^2}$
13. MCC [10], коэффициент корреляции Мэтьюса	Формула (1)
14. Confusion entropy (CEN) [11], энтропия ошибки	Формула (2)
15. Discriminatory power (DP) [12], степень разделимости	$k\left(\log\frac{\text{Sensitivity}}{1 - \text{Sensitivity}} + \log\frac{\text{Specificity}}{1 - \text{Specificity}}\right)$
16. Youden's index [13], индекс Юдена	Sensitivity + Specificity – 1
17. Diagnostic odds ratio (DOR) [14], диагностическое отношение шансов	$\frac{tp}{fn} \Big/ \frac{fp}{tn} = \frac{\text{Sensitivity}}{1 - \text{Sensitivity}} \Big/ \frac{1 - \text{Specificity}}{\text{Specificity}}$

Примечание: $n = tp + fp + fn + tn$, константа k описана в тексте.

Можно построить альтернативную кривую в плоскости Recall/Precision и вычислить площадь под ней. В статье [15] доказана теорема, в которой утверждается, что при бинарной классификации множества объектов существует взаимно-однозначное соответствие между точками ROC-кривой в плоскости fp/tp и кривой, построенной в плоскости Recall/Precision, если эти точки определяют одинаковые матрицы ошибок и Recall $\neq 0$. Однако данный результат нельзя использовать, если итог классификации задан в виде одной матрицы ошибок. Для такой матрицы ROC-кривая состоит из двух отрезков, задаваемых тремя точками с координатами (0,0),

(fpr, tpr), (1,1). Площадь под ROC-кривой можно вычислить как сумму площадей двух треугольников (функция 11 табл. 2). Кривую в плоскости Recall & Precision по одной матрице ошибок построить нельзя, так как известна только одна средняя точка с координатами (Recall, Precision). Поэтому вторая кривая далее не рассматривается. В работе [15] рекомендуется использовать площадь под ROC-кривой для оценки результатов при классификации сбалансированных данных.

Третью группу образуют реже используемые функции, собранные в процессе анализа научной литературы: каппа Коэна (Cohen's kappa) [9], коэффициент корреляции Мэтьюса (Matthews Correlation Coefficient, MCC) [10, 16], энтропия ошибки (Confusion Entropy, CEN) [11], степень разделимости классов (Discriminatory power, DP) [12], индекс Юдена (Youden's index) [13], диагностическое отношение шансов (diagnostic odds ratio, DOR) [14]. Отметим, что в некоторых публикациях индекс Юдена называют Bookmaker Informedness, его можно вычислить через функцию AUC следующим образом:

$$\text{индекс Юдена} = 2\cdot\text{AUC} - 1.$$

Оригинальное определение функции DP дает константу $k = 0{,}5513$, но при этом значение функции может достигать нескольких десятков. Для унификации графического представления функции DP вместе с другими функциями вместо константы k использовался десятичный логарифм от выражения, записанного в скобках в функции 15 табл. 2.

Коэффициент MCC – это дискретный случай коэффициента корреляции Пирсона. Для задач бинарной классификации он вычисляется по формуле

$$\text{MCC} = \frac{(\text{tp}\cdot\text{tn} - \text{fp}\cdot\text{fn})}{\sqrt{(\text{tp} + \text{fp})\cdot(\text{tp} + \text{fn})\cdot(\text{tn} + \text{fp})\cdot(\text{tn} + \text{fn})}}. \quad (1)$$

В статье [16] показано, что для двух классов, случайно сгенерированных и несбалансированных, функции MCC и AUC достаточно устойчивы. Недостатком функции AUC является отсутствие точной формулы ее вычисления в случае многоклассовой классификации. Однако при бинарной классификации и наличии одной матрицы ошибок имеется простая формула вычисления AUC_ROC, представленная в табл. 2.

В работе [17] исследуется зависимость между MCC и CEN в случае многоклассовой классификации, а также приведены формулы вычисления CEN для случая бинарной классификации:

$$\text{CEN} = \frac{(\text{fn} + \text{fp})\cdot\log_2\left((\text{tp} + \text{tn} + \text{fp} + \text{fn})^2 - (\text{tp} - \text{tn})^2\right)}{2(\text{tp} + \text{tn} + \text{fp} + \text{fn})} - \frac{\text{fn}\cdot\log_2\text{fn} + \text{fp}\cdot\log_2\text{fp}}{(\text{tp} + \text{tn} + \text{fp} + \text{fn})}. \quad (2)$$

Если $\text{tp} = \text{tn} = T$ и $\text{fp} = \text{fn} = F$, то верно равенство

$$\text{CEN} = \frac{F}{T+F}\log_2\frac{2(T+F)}{F}.$$

Максимальное значение CEN равно 1,0615 при $T / (T + F) = 0{,}737$ (рис. 1). Это справедливо, например, для матрицы ошибок со значениями [300, 700; 700, 300]. Для такой матрицы MCC = –0,400, что означает низкое качество классификации. При соотношении параметров $T / (T + F) > 0{,}5$ значение CEN > 1. Однако при tp = tn = 0, т. е. в случае полностью неверной классификации, CEN = 1. Эти примеры свидетельствуют о недостаточно корректной оценке функцией CEN матрицы ошибок при плохой классификации данных.

В медицинской статистике известна функция, называемая диагностическим отношением шансов (diagnostic odds ratio, DOR) [14]. Значения данной функции не ограничены сверху при fp или fn, стремящихся к нулю. Поэтому DOR имеет максимальное значение при fp или fn, стремящихся к нулю. Это означает отсутствие ошибок при классификации объектов одного из двух классов, что может привести к плохому разделению пересекающихся классов. Например,

если при определении, болен ли человек, его всегда относить к классу здоровых, то функция DOR в результате такой классификации будет иметь максимальное значение. По этой причине функция DOR не рекомендуется для применения в медицинской диагностике [18]. В настоящей статье данная функция модифицирована следующим образом:

$$\mathrm{DOR}^* = \frac{\log_{10}(\log_{10}(\mathrm{DOR}))}{1{,}4}.$$

Если DOR* > 1, то DOR* = 0,999.

Здесь и далее новые значения параметров будем обозначать значком *.

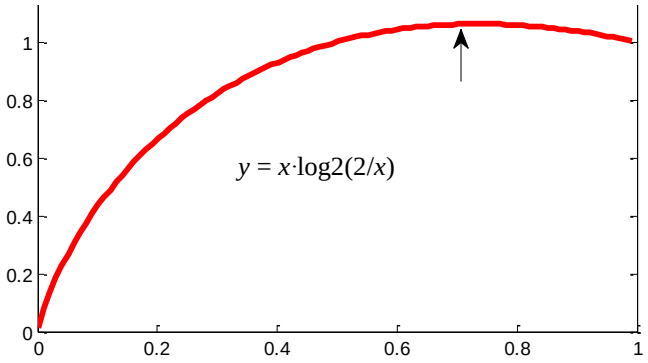


Рис. 1. График значений CEN при изменении $x = T / (T + F)$

Значения функции DOR* при суммарной ошибке классификации не более 49 % всегда находятся в диапазоне [0, 0,999], а при большем проценте ошибок никакие оценки не имеют смысла.

Экспериментальные исследования функций. Оценка результатов классификации, вычисленная по матрице ошибок, должна давать максимально объективную, сбалансированную оценку ошибок при анализе объектов как сбалансированных, так и несбалансированных классов. При решении задачи бинарной классификации такая оценка позволит выбрать объективно лучший метод, учитывающий дисбаланс классов.

Исследования выполнялись в три этапа. На *первом этапе* генерировались матрицы ошибок со сравнимыми размерами двух классов и фиксированным суммарным количеством ошибок, составляющим N % в классах 1 и 2. Например, $N_p = 5$ % ошибочно классифицированных данных класса 1 (positive) и $N_n = (N - N_p) = 95$ % ошибочно классифицированных данных класса 2 (negative). Пусть дисбаланс в размерах классов равен K, тогда размеры классов (tp + fn) = $= K \cdot$ (tn + fp). Затем вычислялись и анализировались значения функций, приведенных в табл. 2, путем изменения N_p от 0 до N.

Оценим изменения функции 1 из табл. 2 при дисбалансе K и процентном соотношении ошибок $N_n : N_p$:

$$\mathrm{FPR}^* = \mathrm{fp}^* / (\mathrm{fp}^* + \mathrm{tn}^*), \quad \mathrm{fp}^* = \mathrm{N_n}\, K \cdot (\mathrm{tn} + \mathrm{fp}) / 100,$$

$$\mathrm{FPR}^* = N_n \cdot K \cdot (\mathrm{tn} + \mathrm{fp}) / (100 \cdot K \cdot (\mathrm{tn} + \mathrm{fp}) = N_n / 100.$$

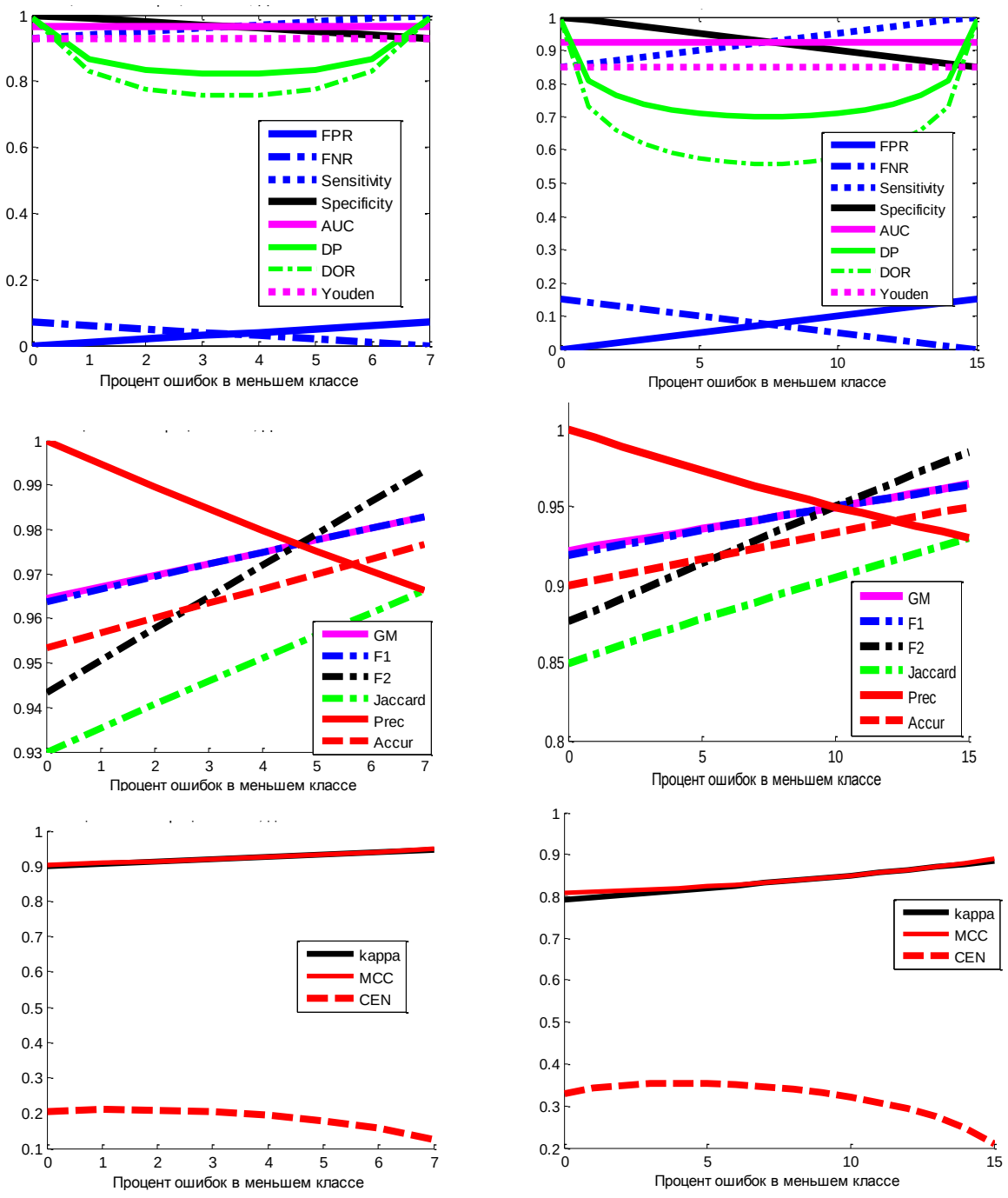
Таким образом, значение функции FPR линейно зависит от процента ошибок в классе 1 и не меняется при дисбалансе классов. Аналогично уточним значения пяти других функций из табл. 2:

$$\mathrm{FNR} = (N - N_p) / 100,$$
$$\mathrm{Sensitivity} = \mathrm{Recall} = (100 - (N - N_p)) / 100 = 1 - (N - N_p)) / 100,$$
$$\mathrm{Specificity} = (100 - N_p) / 100,$$
$$\text{индекс Юдена} = \mathrm{Sensitivity} + \mathrm{Specificity} - 1 = 1 - N,$$
$$\mathrm{AUC} = (\mathrm{Sensitivity} + \mathrm{Specificity}) / 2 = 1 - N / 200.$$

Функции индекс Юдена и AUC зависят только от суммарного процента ошибок в обоих классах и не меняются при разном распределении ошибок между классами даже в случае дисбаланса. Функции DP и DOR* являются комбинациями функций Sensitivity и Specificity, поэтому их значения не меняются при дисбалансе классов.

Рассмотрим оценки бинарной классификации с помощью функций из табл. 2 при разных степенях дисбаланса классов.

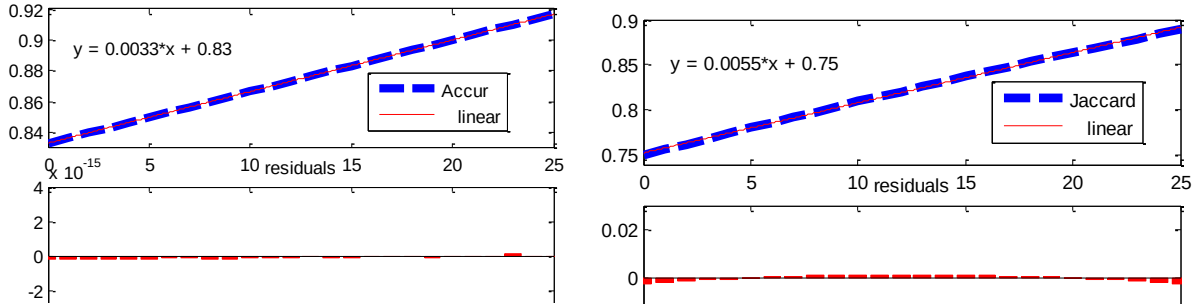
Анализ оценок в случае сбалансированных классов. В настоящей работе данные называются сбалансированными по классам, если отношение K размера большего класса к размеру меньшего находится в пределах от 1 до 5.



а) *б)*

Рис. 2. Графики оценок классификации при 7 % (*а*) и 15 % (*б*) суммарных ошибок в классах с отношением размеров классов $K = 2$

На рис. 2 видно, что шесть функций (FPR, FNR, Sensitivity, Specificity, AUC и индекс Юдена) линейны относительно суммарного процента ошибок. Другие шесть функций (Accuracy, Precision, индекс Жаккара, F1, F2 и GM) визуально почти линейны, но имеют небольшие отклонения от прямых линий (рис. 3).



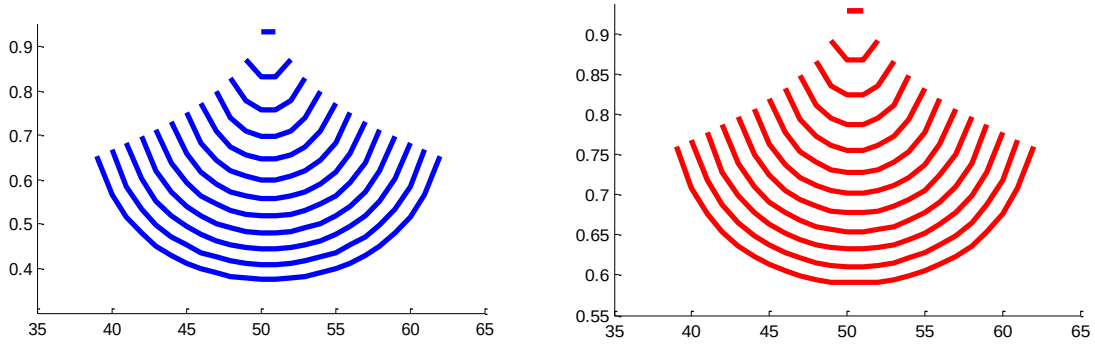
а) *б)*

Рис. 3. Графики функций Accuracy (*а*), индекс Жаккара (*б*) и их аппроксимация прямыми. Внизу представлены графики невязки линейной апроксимации

Значения функций каппа Коэна и MCC нелинейны и очень близки при суммарной величине ошибок до 10 %. При большем проценте ошибок кривая MCC больше изгибается на концах, т. е. сильнее отличается от кривой каппа Коэна при малых процентах ошибок в одном или другом классе. Значения обеих функций растут при увеличении процента ошибок классификации объектов меньшего класса.

Функция CEN при увеличении числа ошибок объектов меньшего класса сначала незначительно растет, а затем убывает (см. рис. 2). Это свойство затрудняет ее использование для сравнения результатов работы разных классификаторов между собой.

На рис. 4 изображены графики функций DOR* и DP. Они подобны, симметричны относительно равного процента ошибок в классах и имеют более высокие значения при меньшем проценте ошибок в одном из классов.



а) *б)*

Рис. 4. Оценки функций DOR* (*а*) и DP (*б*) при суммарной величине ошибок от 2 до 25 % при дисбалансе классов $K = 2$

Анализ оценок в случае несбалансированных классов. На *втором этапе* исследований генерировались матрицы ошибок с дисбалансом K от 10 до 1000 и суммарной ошибкой классификации, равной N % в обоих классах, и оценивались результаты с помощью функций из табл. 2. Графики этих функций показаны на рис. 5 при дисбалансе между классами, составляющем один и два порядка. Функции FPR, FNR, Sensitivity, Specificity, AUC, DP и индекс Юдена имеют такой же вид, как и на рис. 2. Функции DOR* и DP имеют такой же вид и такие же значения, как и на рис. 4. Шесть функций (FPR, FNR, Sensitivity, Specificity, AUC и индекс Юдена) являются линейными относительно суммарного процента ошибок независимо от дисбаланса классов. Другие шесть функций (Accuracy, Precision, индекс Жаккара, F1, F2 и GM) визуально почти линейны при любом дисбалансе, но имеют небольшие отклонения от прямых линий.

При дисбалансе классов K в один-два порядка и большом проценте ошибок многие функции имеют примерно равные значения для широкого диапазона значений процента ошибок в одном классе. Таковыми являются функции GM и F1, Accuracy и индекс Жаккара (рис. 5). Они возрастают почти до максимального значения, равного единице, при уменьшении ошибок в большем классе и увеличении ошибок в меньшем классе. Отмеченное свойство затрудняет использование этих функций для сравнения результатов работы разных классификаторов между собой при выборе лучшего из них для анализа несбалансированных данных.

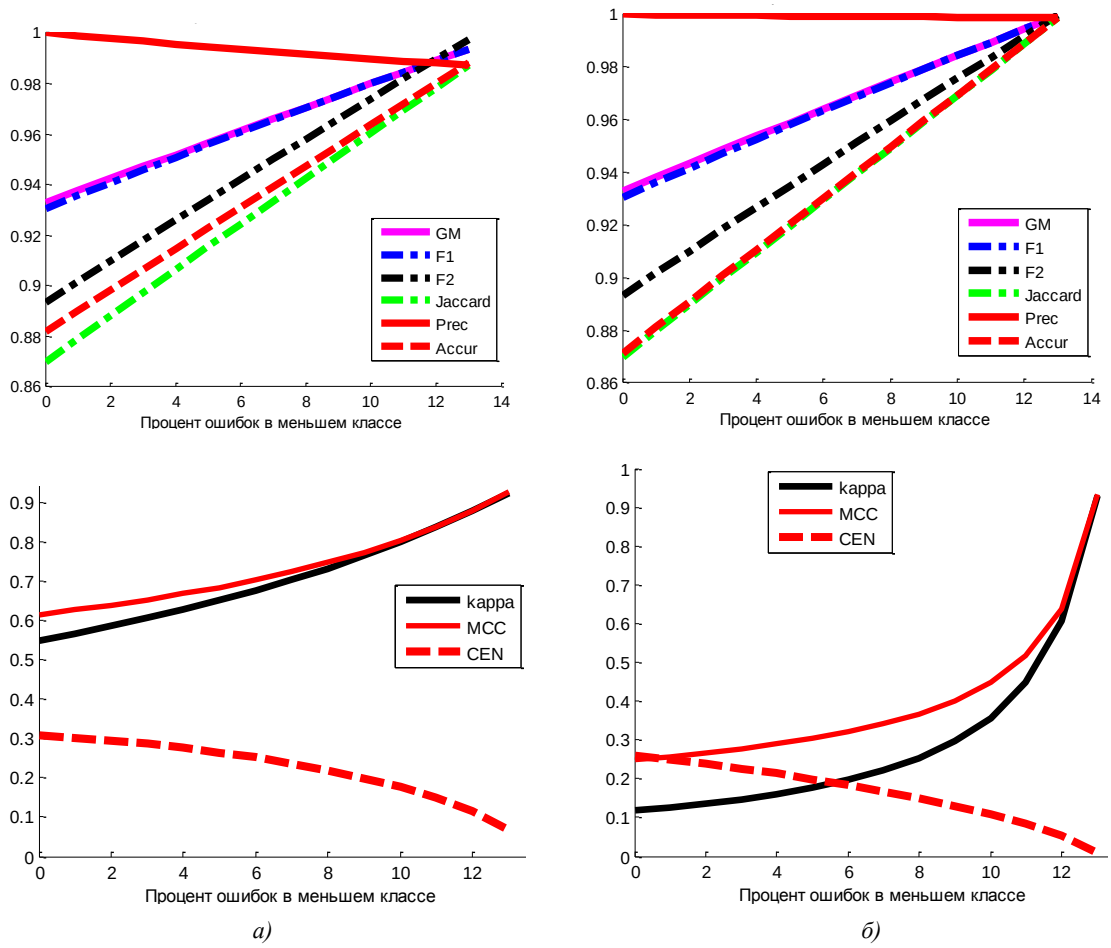


Рис. 5. Суммарная величина ошибок классификации N = 13 %, дисбаланс между классами K = 10 (*а*) и K = 100 (*б*)

При дисбалансе $K \geq 100$ значения функции Precision изменяются от 1 до 0,9977 с увеличением величины ошибок в меньшем классе от 0 до 23 %. Поэтому она не годится для оценки результатов существенно несбалансированных данных.

Функции Accuracy и индекс Жаккара практически совпадают и почти линейно зависят от процента ошибок в меньшем классе:

$$\text{Accuracy} \approx \text{индекс Жаккара} \approx (100 - N + N_1) / 100,$$

где N_1 – процент ошибок в меньшем классе (рис. 5, *б* вверху). На рис. 6 изображены уравнения линейной аппроксимации этих функций и показаны их отклонения от прямой линии. Уравнения линейной аппроксимации функций Accuracy и индекс Жаккара почти совпадают.

Выявлены следующие отношения между значениями функций: (1 – CEN) > MCC > каппа Коэна (см. рис. 5). Все три функции нелинейны, и их меньшие значения соответствуют наименьшему проценту ошибок в меньшем классе. Указанные зависимости проявляются при любом проценте суммарных ошибок и любом дисбалансе классов. При этом CEN имеет наименьший диапазон значений, а каппа Коэна – наибольший при одинаковых ошибках классификации и параметре дисбаланса K.

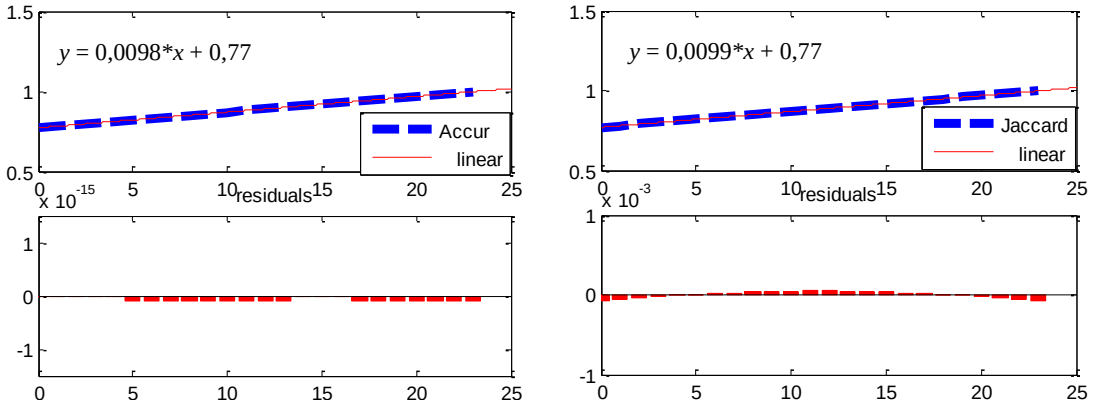


Рис. 6. Суммарная величина ошибок классификации N = 23 % при дисбалансе K = 100

Поведение рассмотренных функций инвариантно к размерам классов и меняется только при их дисбалансе.

Анализ степени разделимости функций DP и DOR. Значения функций DP и DOR для сбалансированных и несбалансированных классов полностью совпадают при одинаковом проценте ошибок N (см. рис. 4 и 7). Значения этих функций минимальны при равном проценте ошибок в обоих классах и максимальны при большем проценте в одном из них. Функции DP и DOR являются хорошими кандидатами в индикаторы ошибок бинарной классификации, инвариантными к дисбалансу классов. Они симметричны относительно равного числа ошибок в классах (рис. 7). Чем больше суммарный процент ошибочной классификации, тем ниже значения DP и DOR.

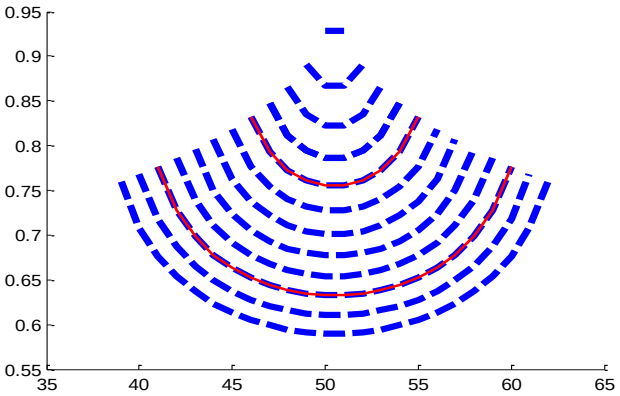


Рис. 7. Оценки DP при суммарной величине ошибок классификации N = 3–25 % при дисбалансе K = 1000 (пунктирная линия) и K = 10 (сплошная красная линия для двух случаев)

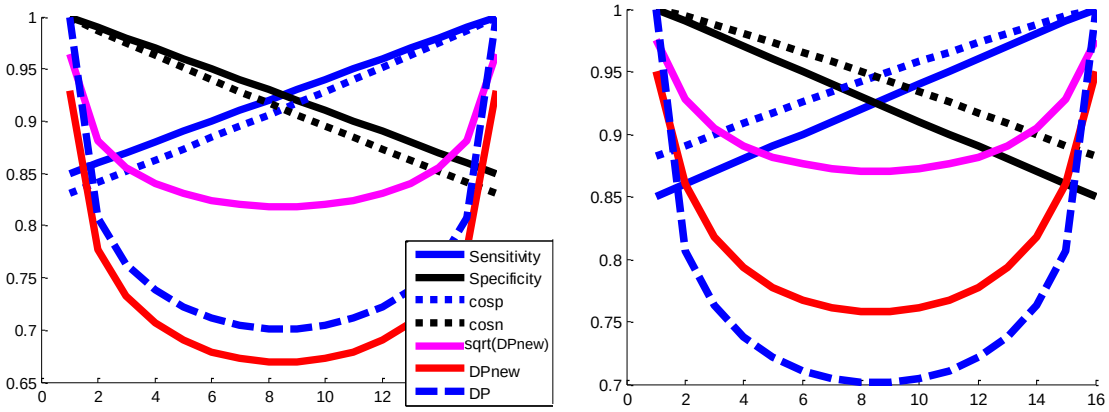
Функции DP и DOR можно скорректировать так, чтобы они принимали значения в более узком диапазоне, что точнее соответствовало бы качеству классификации объектов. На рис. 8 показаны графики модифицированной функции DPnew, в которой Sensitivity и Specificity вычисляются с помощью показателя степени $s > 1$:

$$\text{Sensitivity} = tp / (tp^s+fn^s)^{1/s}, \quad \text{Specificity} = tn / (tn^s+fp^s)^{1/s}. \tag{3}$$

Дополнительно из новых значений DP извлечен квадратный корень, чтобы приблизить минимальные значения модифицированной функции DP к минимальным значениям функций Sensitivity и Specificity. Графики cosp и cosn на рис. 8 – это обобщенные варианты функций Sensitivity и Specificity из формулы (2), которые совпадают с косинусами отношений верно и неверно (true – false) классифицированных объектов классов 1 и 2 при s = 2. Все функции, изображенные на рис. 8, инвариантны к дисбалансу классов. Однако функции Sensitivity, Specificity и их линейные обобщения cosp и cosn оценивают только ошибки в одном из двух

классов. Функции DP, DOR и их вариации оценивают суммарный процент ошибок классификации в обоих классах.

Единственной проблемой функций DP, DOR и их вариантов являются значения функций при fn и (или) fp, равные нулю. В таких случаях при вычислении возникает проблема деления на ноль, а функции принимают значения, бóльшие единицы, при попытке замены нулей константами. Формально в таких ситуациях можно приравнять значения функций DP к константе, близкой к единице.



а) *б)*

Рис. 8. Графики функций DP, DPnew и корень квадратный из DPnew при 15 % суммарных ошибок: *а)* DPnew при s = 0,95; *б)* DPnew при s = 1,1

Анализ абсолютных ошибок классификации несбалансированных данных. На *третьем этапе* исследований строились матрицы ошибок при дисбалансе классов K = 2, 10 и 100, при этом задавалось одинаковое количество ошибок в большем и меньшем классах и вычислялись оценки согласно табл. 2. Результаты экспериментов позволили сделать выводы относительно 17 исследуемых оценочных функций (табл. 3–5). В таблицах курсивом отмечены функции, которые инвариантны к транспонированию матрицы ошибок, подчеркиванием показаны максимальные значения функций, полужирным курсивом – минимальные.

Суммарная величина ошибок, представленных в табл. 3, находится в диапазоне от 1,5 до 15,0 % (в табл. 3 они выделены жирным шрифтом). Очевидно, что большему числу ошибок должны соответствовать меньшие значения оценочных функций, а для функций 1 и 2 – бóльшие значения оценочных функций. Однако функции 1–3 имеют одинаковые минимальные значения для разных пропорций ошибок в табл. 3. Они же и функции 4–6 имеют одинаковые максимальные значения для разных пропорций и количества ошибок классификации, что свидетельствует о ненадежности функций 1–6 в качестве оценок классификации данных. Эти же выводы подтверждают данные табл. 4 и 5.

Обобщим выводы по результатам экспериментов, приведенным в табл. 3–5. Функция Sensitivity при дисбалансе K = 100 имеет почти максимальные значения 0,999 (табл. 5) при ошибке 39 % в меньшем классе. В первую очередь эта функция реагирует на ошибку в большем классе (табл. 3), поэтому она не годится для оценки несбалансированных классов.

Функция Precision при дисбалансе K = 100 имеет почти одинаковые значения (табл. 5) при ошибке 39 и 1 % в меньшем классе, при этом суммарный процент ошибок составляет 39,1 и 1,39 % соответственно. Аналогична ситуация при дисбалансе K = 10 (табл. 4). Поэтому функция Precision не годится для оценки несбалансированных классов.

Функция Specificity при равном проценте ошибок реагирует только на ошибки меньшего класса. Следовательно, она тоже не годится для объективной оценки бинарной классификации данных.

Функция Accuracy в табл. 5 имеет очень высокое значение (0,9960) при 39 % ошибок в меньшем классе и дисбалансе K = 100. В табл. 4 для матрицы ошибок [961, 39; 1, 99] Accuracy имеет значение 0,9636 – почти столько же, как и в табл. 3 для матрицы [190 10; 1 99], где значение Accuracy равно 0,9633. В первом случае дисбаланс K = 10, ошибка в большем классе равна 3,9 %, а в меньшем – 1 %. Во втором случае дисбаланс K = 2, ошибка в большем классе

равна 5 %, в меньшем – 1 %. В табл. 3 для матрицы [199, 1; 10, 90] при $K = 2$ ошибка в большем классе равна 0,5 %, а в меньшем 10 % при таком же значении Accuracy (0,9633). Эта функция учитывает только суммарное количество правильно классифицированных объектов относительно общего числа объектов. Она ни в коем случае не годится для оценки несбалансированных классов.

Таблица 3

Значения оценочных функций при дисбалансе классов $K = 2$

Матрица ошибок	[199, 1; 1, 99]	[198, 2; 1, 99]	[199, 1; 2, 98]	[190, 10; 1, 99]	[190, 10; 10, 90]	[199, 1; 10, 90]	[195, 5; 5, 95]
Суммарная величина ошибок, %	**1,5**	2,0	2,5	6,0	**15,0**	10,5	7,5
1. FPR	***0,0100***	***0,0100***	0,0200	***0,0100***	0,1000	0,1000	0,0500
2. FNR	***0,0050***	0,0100	***0,0050***	0,0500	0,0500	***0,0050***	0,0250
3. Sensitivity	0,9950	0,9900	0,9950	***0,9500***	***0,9500***	0,9950	0,9750
4. Specificity	0,9900	0,9900	0,9800	0,9900	***0,9000***	0,9000	0,9500
5. Precision	0,9950	0,9950	0,9900	0,9948	***0,9500***	0,9522	0,9750
6. *Accuracy*	0,9933	0,9900	0,9900	0,9633	***0,9333***	0,9633	0,9667
7. *Индекс Жаккара*	0,9900	0,9851	0,9851	0,9453	***0,9048***	0,9476	0,9512
8. *F1*	0,9950	0,9925	0,9925	0,9719	***0,9500***	0,9731	0,9750
9. F2	0,9950	0,9910	0,9940	0,9586	***0,9500***	0,9861	0,9750
10. *GM*	0,9950	0,9925	0,9925	0,9721	***0,9500***	0,9733	0,9750
11. AUC	0,9925	0,9900	0,9875	0,9700	***0,9250***	0,9475	0,9625
12. Каппа Коэна	0,9850	0,9776	0,9774	0,9193	***0,8500***	0,9156	0,9250
13. CEN	0,9457	0,9252	0,9252	0,8116	***0,6785***	0,8128	0,8059
14. *MCC*	0,9850	0,9776	0,9775	0,9213	***0,8500***	0,9178	0,9250
15. *DP*	0,9951	0,9633	0,9631	0,8773	***0,7111***	0,8745	0,8201
16. Индекс Юдена	0,9850	0,9800	0,9750	0,9400	***0,8500***	0,8950	0,9250
17. *DOR*	0,9990	0,9886	0,9883	0,8472	***0,5738***	0,8426	0,7530

Таблица 4

Значения оценочных функций при дисбалансе классов K =10

Матрица ошибок	[999, 1; 1, 99]	[998 2 1, 99]	[999, 1; 1, 98]	[990, 10; 1, 99]	[990, 10; 10, 90]	[999, 1; 10, 90]	[995, 5; 5, 95]
Суммарная величина ошибок, %	**1,1**	1,2	2,1	2,0	**11,0**	10,1	5,5
1. FPR	***0,0100***	***0,0100***	0,0200	***0,0100***	0,1000	0,1000	0,0500
2. FNR	***0,0010***	0,0020	***0,0010***	0,0100	0,0100	***0,0010***	0,0050
3. Sensitivity	0,9990	0,9980	0,9990	***0,9900***	***0,9900***	0,9990	0,9950
4. Specificity	0,9900	0,9900	0,9800	0,9900	***0,9000***	***0,9000***	0,9500
5. Precision	0,9990	0,9990	0,9980	0,9990	***0,9900***	0,9901	0,9950
6. Accuracy	0,9982	0,9973	0,9973	0,9900	***0,9818***	0,9900	0,9909
7. Индекс Жаккара	0,9980	0,9970	0,9970	0,9890	***0,9802***	0,9891	0,9900
8. F1	0,9990	0,9985	0,9985	0,9945	***0,9900***	0,9945	0,9950
9. F2	0,9990	0,9982	0,9988	0,9918	***0,9900***	0,9972	0,9950
10. GM	0,9990	0,9985	0,9985	0,9945	***0,9900***	0,9945	0,9950
11. AUC	0,9945	0,9940	0,9895	0,9900	***0,9450***	0,9495	0,9725
12. Каппа Коэна	0,9890	0,9836	0,9834	0,9419	***0,8900***	0,9369	0,9450
13. CEN	0,9831	0,9764	0,9765	0,9369	***0,8912***	0,9375	0,9365
14. MCC	0,9890	0,9836	0,9834	0,9429	***0,8900***	0,9382	0,9450
15. DP	0,9990	0,9990	0,9990	0,9633	***0,8320***	0,9592	0,9158
16. Индекс Юдена	0,9890	0,9880	0,9790	0,9800	***0,8900***	0,8990	0,9450
17. DOR	0,9990	0,9990	0,9990	0,9886	***0,7727***	0,9819	0,9105

Таблица 5

Значения оценочных функций при дисбалансе классов $K = 10$ и $K = 100$

Матрица ошибок	[M1, 0; 0, M2] M1&M2>0	[961, 39; 1, 99], K =10	[999, 1; 39, 61], K =10	[9999, 1; 39, 61], K =100	[9990, 10; 39, 61], K =100	[9961, 39; 1, 99], K =100
Ошибка в большем классе, %	0	3,9	0,1	0,01	0,1	0,39
Ошибка в меньшем классе, %	0	1	***39***	***39***	***39***	1
Суммарная величина ошибок, %	0	4,9	***39,1***	39,01	***39,1***	1,39
1. FPR	0	***0,0100***	0,3900	0,3900	0,3900	***0,0100***
2. FNR	0	0,0390	0,0010	***0,0001***	0,0010	0,0039
3. Sensitivity	1	***0,9610***	0,9990	0,9999	0,9990	***0,9961***
4. Specificity	1	0,9900	***0,6100***	***0,6100***	***0,6100***	0,9900
5. Precision	1	0,9990	***0,9624***	0,9961	***0,9961***	0,9999
6. Accuracy	1	***0,9636***	***0,9636***	0,9960	0,9951	0,9960
7. Индекс Жаккара	1	***0,9600***	0,9615	0,9960	0,9951	0,9960
8. F1	1	***0,9796***	0,9804	0,9980	0,9976	0,9980
9. F2	1	***0,9684***	0,9915	0,9991	0,9984	0,9969
10. GM	1	***0,9798***	0,9805	0,9980	0,9976	***0,9980***
11. AUC	1	0,9755	***0,8045***	0,8050	***0,8045***	0,9930
12. Каппа Коэна	1	0,8121	0,7346	0,7512	***0,7111***	0,8300
13. CEN	1	***0,8450***	0,8541	0,9776	0,9710	0,9765
14. MCC	1	0,8254	0,7591	0,7731	***0,7217***	0,8410
15. DP	>1	0,8921	***0,8665***	0,9849	***0,8665***	1,0060
16. Индекс Юдена	1	0,9510	***0,6090***	0,6099	***0,6090***	0,9861
17. DOR	>1	0,8715	***0,8294***	1,0241	***0,8294***	1,0588

Функции F1, F2, GM, индекс Жаккара и CEN неадекватно реагируют на ошибки при дисбалансе классов (см. табл. 4 и 5).

Функции DP и DOR в табл. 5 при ошибке 0,01 % в большем классе и 39 % в меньшем (суммарная величина ошибок 39,01 %) равны 0,9849 и 1,0241, а при ошибке 0,39 % в большем классе и 1 % в меньшем (суммарная величина ошибок 1,39 %) – 1,0060 и 1,0588 соответственно, т. е. их значения очень близки. В то же время функции DP и DOR в табл. 5 имеют более низкие оценки при ошибке 0,1 % в большем классе и при ошибке 39 % в меньшем классе (суммарная величина ошибок 39,1 %). Значения функций DP и DOR равны 0,8665 и 0,8294 соответственно. Эти функции инвариантны к дисбалансу классов относительно суммарного процента ошибок, однако в силу существенной нелинейности в вычислении они плохо оценивают результаты классификации при близких значениях суммарных процентов ошибок в классах.

Функции AUC, каппа Коэна, MCC и индекс Юдена корректнее других оценивают результаты классификации сбалансированных данных (см. табл. 3 и 4). Однако результаты классификации несбалансированных данных, приведенные в табл. 5, показывают, что каппа Коэна и MCC более чувствительны к дисбалансу классов, чем AUC и индекс Юдена. Две последние функции линейно зависимы друг от друга согласно формуле индекс Юдена = 2·AUC – 1 и дают наиболее корректные оценки результатов классификации (см. табл. 5).

Заключение. В работе выполнен сравнительный анализ 17 функций, применяемых для оценки бинарных классификаторов по матрице ошибок. Показано, что между отдельными оценочными функциями существуют простые линейные зависимости: FPR = 1 – Specificity, AUC = (Sensitivity + Specificity) / 2, индекс Юдена = Sensitivity + Specificity – 1 или 2·AUC – 1, индекс Жаккара = $F1 / (2 - F1)$.

Многие из рассмотренных функций, например Accuracy, F1, GM, AUC, каппа Коэна, MCC, CEN, DP, DOR, инвариантны к транспонированию матрицы ошибок. Это свойство позволяет вычислять их, не уточняя, как записаны данные в матрице ошибок.

Проанализированы результаты бинарной классификации сбалансированных и несбалансированных данных. Показано, что для оценки результатов классификации сбалансированных классов (при соотношении размеров не более пяти) не стоит использовать функцию энтропия ошибки, обозначенную как CEN [11]. В работе [14] также не рекомендуют применять функцию CEN для оценки результатов бинарной классификации.

Все классические функции, такие как Sensitivity, Specificity, Precision, Accuracy, F1, F2, GM и индекс Жаккара, очень чувствительны к дисбалансу классифицируемых данных и искажают оценки при ошибках классификации объектов меньшего класса. Чувствительность к дисбалансу имеется у коэффициента корреляции Мэтьюса и каппа Коэна. Экспериментально показано, что такие функции, как энтропия ошибки (CEN), степень разделимости (DP) и диагностическое отношение шансов (DOR), не стоит использовать для оценки бинарной классификации несбалансированных классов. Две последние функции абсолютно инвариантны к дисбалансу классифицируемых данных, но плохо оценивают варианты с примерно равным суммарным процентом ошибок классификации.

Индекс Юдена имеет диапазон значений [–1, +1], а функция AUC [0, +1]. При приведении диапазона значений индекса Юдена к [0, +1] он совпадает с функцией AUC. В статье [19] функция, использованная для бинарной классификации и совпадающая с AUC, названа сбалансированной правильностью (balanced Accuracy). Таким образом, AUC – это наиболее подходящая из известных оценочная функция для сравнения результатов классификации по матрице ошибок как сбалансированных, так и несбалансированных данных.

References

1. Zhuravlev Y. I. On the algebraic approach to solving problems of recognition and classification. *Problems of cybernetics*, Moscow, Nauka, 1978, vol. 33, pp. 5–68.

2. Haixiang G., Shang J., Mingyun G., Yuanyue H., Bing G. Learning from class-imbalanced data: Review of methods and applications. *Expert Systems with Applications*, 2017, vol. 73, pp. 220–239.

3. Choi S. S., Cha S. H., Tappert C. C. A survey of binary similarity and distance measures. *Journal of Systemics, Cybernetics and Informatics*, 2010, vol. 8(1), pp. 43–48.

4. Canbek G., Sagiroglu S., Temizel T. T., Baykal N. Binary classification performance measures/metrics: A comprehensive visualized roadmap to gain new insights. *International Conference on Computer Science and Engineering, Antalya, Turkey, 5–8 October 2017*. Antalya, 2017, pp. 821–826.

5. Sokolova M., Lapalme G. A systematic analysis of performance measures for classification tasks. *Information Processing & Management*, 2009, vol. 45, no. 4, pp. 427–437.

6. Valverde-Albacete F. J., Peláez-Moreno C. 100 % classification accuracy considered harmful: the normalized information transfer factor explains the accuracy paradox. *PLoS One*, 2014, vol. 9(1), 10 p. https://doi.org/10.1371/journal.pone.0084217

7. Powers D. M. *What the F-measure doesn't measure: Features, Flaws, Fallacies and Fixes*, 2015. Available at: https://arxiv.org/abs/1503.06410 (accessed 17.11.2019).

8. Fawcett T. An introduction to ROC analysis. *Pattern Recognition Letters*, 2006, vol. 27, no. 8, pp. 861–874.

9. Cohen J. A coefficient of agreement for nominal scales. *Educational and Psychological Measurement*, 1960, vol. 20, no. 1, pp. 37–46.

10. Matthews B. Comparison of the predicted and observed secondary structure of T4 phage lysozyme. *Biochimica et Biophysica Acta – Protein Structure*, 1975, vol. 405, no. 2, pp. 442–451.

11. Wei J. M., Yuan X. J., Hu Q. H., Wang S. Q. A novel measure for evaluating classifiers. *Expert Systems with Applications*, 2010, vol. 37, no. 5, pp. 3799–3809.

12. Blakeley D. D., Oddone E. Z., Hasselblad V., Simel D. L., Matchar D. B. Noninvasive carotid artery testing: a meta-analytic review. *Annals of Internal Medicine*, 1995, vol. 122, no. 5, pp. 360–367.

13. Youden W. J. Index for rating diagnostic tests. *Cancer*, 1950, vol. 3, no. 1, pp. 32–35.

14. Glas A. S., Lijmer J. G., Prins M. H., Bonsel G. J., Bossuyt P. M. The diagnostic odds ratio: a single indicator of test performance. *Journal of Clinical Epidemiology*, 2003, vol. 56, no. 11, pp. 1129–1135.

15. Davis J., Goadrich M. The relationship between Precision-Recall and ROC curves. *Proceedings of the 23rd International Conference on Machine Learning, 25–29 June 2006, Pittsburgh, Pennsylvania, USA*. Pittsburgh, 2006, pp. 233–240.

16. Boughorbel S., Jarray F., El-Anbari M. Optimal classifier for imbalanced data using Matthews Correlation Coefficient metric. *PloS One*, 2017, vol. 12(6). https://doi.org/10.1371/journal.pone.0177678

17. Jurman G., Riccadonna S., Furlanello C. A comparison of MCC and CEN error measures in multi-class prediction. *PloS One*, 2012, vol. 7, no. 8, e41882. https://doi.org/10.1371/journal.pone.0041882

18. Pepe M. S., Janes H., Longton G., Leisenring W., Newcomb P. Limitations of the odds ratio in gauging the performance of a diagnostic, prognostic, or screening marker. *American Journal of Epidemiology*, 2004, vol. 159, no. 9, pp. 882–890.

19. Mower J. P. PREP-Mt: predictive RNA editor for plant mitochondrial genes. *BMC Bioinformatics*, 2005, vol. 6, art. 96, pp. 1–15. https://doi.org/10.1186/1471-2105-6-96

Информация об авторах

Старовойтов Валерий Васильевич – доктор технических наук, профессор, главный научный сотрудник, Объединенный институт проблем информатики Национальной академии наук Беларуси, Минск, Беларусь.
E-mail: valerys@newman.bas-net.by

Голуб Юлия Игоревна – кандидат технических наук, доцент, старший научный сотрудник, Объединенный институт проблем информатики Национальной академии наук Беларуси, Минск, Беларусь.

Information about the authors

Valery V. Starovoitov, Dr. Sci. (Eng.), Professor, Chief Researcher, The United Institute of Informatics Problems of the National Academy of Sciences of Belarus, Minsk, Belarus.
E-mail: valerys@newman.bas-net.by

Yuliya I. Golub, Cand. Sci. (Eng.), Associate Professor, Senior Researcher, the United Institute of Informatics Problems of the National Academy of Sciences of Belarus, Minsk, Belarus.

ISSN 1816-0301 (Print)
ISSN 2617-6963 (Online)

ЗАЩИТА ИНФОРМАЦИИ

INFORMATION PROTECTION

УДК 004.056.5
https://doi.org/10.37661/1816-0301-2020-17-1-102-108

Поступила в редакцию 16.12.2019
Received 16.12.2019

Принята к публикации 21.02.2020
Accepted 21.02.2020

Усиление секретности криптографического ключа, сформированного с помощью синхронизируемых искусственных нейронных сетей

М. Л. Радюкевич[1]✉, В. Ф. Голиков[2]

[1]Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации», Минск, Беларусь
✉E-mail: 1218a@list.ru

[2]Белорусский национальный технический университет, Минск, Беларусь

Аннотация. Рассматриваются основные варианты формирования общего секрета с использованием синхронизируемых искусственных нейронных сетей и возможные модели поведения криптоаналитика. Для решения задачи повышения конфиденциальности формируемого общего секрета, если он будет использоваться в качестве криптографического ключа, предлагается применять смешивание некоторого числа результатов отдельных синхронизаций (свертку). В качестве функции смешивания рассматривается свертка векторов весовых коэффициентов сетей побитовым сложением по модулю 2 всех результатов отдельных синхронизаций. Показывается, что вероятность успеха криптоаналитика уменьшается экспоненциально с увеличением количества слагаемых в свертке и может быть выбрана сколь угодно малой. При этом закон распределения сформированного ключа после свертки близок к равномерному, а равномерность возрастает с увеличением количества слагаемых в свертке.

Ключевые слова: синхронизируемые искусственные нейронные сети, общий секрет, криптографический ключ, функция сжатия, криптоанализ

Для цитирования. Радюкевич, М. Л. Усиление секретности криптографического ключа, сформированного с помощью синхронизируемых искусственных нейронных сетей / М. Л. Радюкевич, В. Ф. Голиков // Информатика. – 2020. − Т. 17, № 1. – С. 102–108. https://doi.org/10.37661/1816-0301-2020-17-1-102-108

Enhancing the secrecy of a cryptographic key generated using synchronized artificial neural networks

Maryna L. Radziukevich[1]✉, Vladimir F. Golikov[2]

[1]Scientific Production-Republican Unitary Enterprise "Research Institute for the Technical Protection of Information", Minsk, Belarus
✉E-mail: 1218a@list.ru

[2]Belarusian National Technical University, Minsk, Belarus

Abstract. The main options for the formation of a shared secret using synchronized artificial neural networks and possible patterns of behavior of a cryptanalyst are considered. To solve the problem of increasing the confidentiality of the generated shared secret, if it is used as a cryptographic key, it is proposed to use the mixing a certain number of results of individual synchronizations (convolution). As a mixing function, we

consider the convolution of the vectors of network weights by bitwise addition modulo 2 of all the results of individual synchronizations. It is shown that the probability of success of a cryptanalyst is reduced exponentially with an increase of the number of terms in the convolution and can be chosen arbitrarily small. Moreover, the distribution law of the generated key after convolution is close to uniform and the uniformity increases with the number of terms in the convolution.

Key words: synchronized artificial neural networks, shared secret, cryptographic key, compression function, cryptanalysis

For citation. Radziukevich M. L., Golikov V. F. Enhancing the secrecy of a cryptographic key generated using synchronized artificial neural networks. *Informatics*, 2020, vol. 17, no. 1, pp. 102−108 (in Russian). https://doi.org/10.37661/1816-0301-2020-17-1-102-108

Введение. Формирование общего секретного числа с помощью синхронизируемых искусственных нейронных сетей (СИНС) предложено в работах [1, 2], анализировалось в статье [3], развивалось и конкретизировалось в публикациях [4–6]. Основное достоинство данной технологии в случае ее использования в криптографических приложениях состоит в простоте реализации и исключении применения классических однонаправленных математических функций, обеспечивающих конфиденциальность формируемых криптографических ключей. Между тем процесс формирования общего секретного числа по технологии СИНС носит стохастический характер, поэтому уровень его секретности может оказаться недостаточным для использования в ответственных криптосистемах [6]. Для преодоления указанного недостатка представляет интерес модификация технологии СИНС.

Основные варианты формирования общего секрета и модели поведения криптоаналитика.

Протокол AB-1 включает несколько пунктов:

1. Абоненты A и B, формирующие общее секретное число с помощью СИНС [7], выбирают предельное число тактов синхронизации d, обеспечивающее при выбранных параметрах своих ИНС (n – количество входов каждого персептрона, K – количество персептронов, $\pm L$ – интервал возможных значений весовых коэффициентов персептронов) достижение полной синхронизации сетей с высокой вероятностью при следующем условии:

$$P(t_{AB} \le d) \ge P_{\text{тр}},$$

где t_{AB} – число тактов синхронизации, при котором весовые коэффициенты (ВК) сетей A и B будут равны друг другу; $P_{\text{тр}}$ – требуемая вероятность синхронизации. Число d определяется по результатам моделирования для сетей с выбранными параметрами [7].

2. Абоненты A и B случайным образом выбирают начальные значения ВК $\vec{W}^A(0)$, $\vec{W}^B(0)$ и проводят d тактов синхронизации, а также фиксируют значения векторов ВК своих сетей $\vec{W}^A(d)$, $\vec{W}^B(d)$, не оглашая их.

3. Абоненты A и B определяют совпадение полученных векторов одним из возможных способов. Например, абонент A может зашифровать сформированным ключом некий секретный текст и отправить его B. Если B правильно его расшифрует, то ключи совпадают. Возможен вариант, когда абонент A по договоренности с B выбирает надежный алгоритм шифрования и шифрует им $\vec{W}^A(d)$, используя в качестве ключа часть этого вектора. Абонент B, действуя аналогично, расшифровывает и сравнивает полученный результат с $\vec{W}^B(d)$. Если оказалось, что $\vec{W}^A(d) = \vec{W}^B(d)$, то общий секрет $S^{AB} = \vec{W}^A(d) = \vec{W}^B(d)$.

4. Если окажется, что $\vec{W}^A(d) \ne \vec{W}^B(d)$, то сеанс синхронизации повторяется с новыми значениями $\vec{W}^A(0)$, $\vec{W}^B(0)$ до тех пор, пока не закончится успешно.

Оценим необходимое количество синхронизаций сетей A и B для получения хотя бы одного успеха. Поскольку каждая синхронизация проводится в одинаковых условиях, а вероятность успеха каждой синхронизации $P_{AB} = P(t_{AB} \le d)$ и синхронизации не зависят друг от друга, то количество успешных синхронизаций имеет биномиальный закон распределения вероятностей

$$P(i = l) = C_m^l \; P_{AB}^l \; (1 - P_{AB})^{m-l},$$

где m – количество синхронизаций; l – количество успешных синхронизаций, l = 0, 1, 2, …, m.

Вероятность получения хотя бы одного успеха в серии из m определяется выражением

$$P(l \geq 1) = \sum_{l=1}^{m} C_m^l \; P_{AB}^l \; (1 - P_{AB})^{m-l} = 1 - P(l = 0) = 1 - (1 - P_{AB})^m.$$

Если задать нижнюю границу $P_{\text{тр}}$ этой вероятности, то можно рассчитать число синхронизаций m_{AB}, которое обеспечит появление хотя бы одной успешной синхронизации:

$$1 - (1 - P_{AB})^{m_{AB}} \; \geq P_{\text{тр}},$$

где $m_{AB} \geq \frac{\ln(1-P_{\text{тр}})}{\ln(1-P_{AB})}$.

На практике синхронизации можно проводить последовательно до первого успеха, а значение m_{AB} просто указывает на возможное их число. В табл. 1 приведены значения m_{AB} для различных вероятностей P_{AB} и $P_{\text{тр}}$.

Таблица 1

Количество сеансов синхронизации для обеспечения необходимых значений вероятностей

P_{AB} \ $P_{\text{тр}}$	0,70	0,80	0,90	0,95	0,99
0,90	2	2	1	1	1
0,95	3	2	2	1	1
0,99	4	3	2	2	1

Протокол ABE-1 заключается в следующем. Криптоаналитик *E*, прослушивая канал связи между *A* и *B*, синхронизирует свою сеть, например, с сетью *A*. Для сеанса, в котором оказалось, что *A* и *B* достигли синхронизации и подтвердили, что $\vec{W}^A(d) = \vec{W}^B(d)$, криптоаналитик *E* проверяет совпадение $\vec{W}^E(d)$ с $\vec{W}^A(d)$, если это возможно при выбранном *A* и *B* варианте сравнения, либо предполагает, что $\vec{W}^E(d) = \vec{W}^A(d)$. Вероятность совпадения $\vec{W}^E(d)$ с $\vec{W}^A(d)$ обозначим как $P_{EA} = P(t_{EA} \leq d)$. Результаты имитационного моделирования [7] показывают, что эта вероятность существенно зависит от параметров сети, выбранных *A* и *B*. Структура сети криптоаналитика *E* и ее параметры, как это указывалось ранее, должны быть полностью идентичны структуре и параметрам сетей абонентов *A* и *B*, а поскольку абоненты *A* и *B* хотят защитить конфиденциальность формируемого секрета от *E*, то они должны, учитывая наличие сети криптоаналитика *E*, выбирать такие параметры, которые обеспечивают высокие значения P_{AB} при минимально возможных значениях P_{EA}. Однако при относительно приемлемом предельном числе тактов $d \leq 5000$ не удается снизить вероятность P_{EA} меньше чем до (0,01–0,05), что может не соответствовать заданным криптографическим требованиям.

Повышение секретности. Из изложенного выше следует актуальность задачи повышения конфиденциальности формируемого общего секрета, если он будет использоваться в качестве криптографического ключа. Идея такого метода в самом обобщенном виде в терминах информационно-вероятностного подхода изложена в работе [8]: «…усиление секретности – это искусство выделения секретной совместно используемой информации, возможно, для использования в качестве криптографического ключа, из большого объема совместно используемой информации, которая является частично секретной». Иначе говоря, если *A* и *B* имеют общую секретную информацию *W*, а *E* известна ее некоторая часть *V* (*A* и *B* не знают, какая), то, преобразовав *W* специальным образом, можно свести *V* к сколь угодно малой величине, пожертвовав размером *W*.

Постановка задачи усиления секретности следующая. Абоненты *A* и *B* сформировали секретный ключ *W* в виде битовой строки размером *n*. Криптоаналитик *E*, прослушивая процесс формирования ключа, имеет информацию *V*, коррелированную с *W* и дающую знание *t* бит из *n*, т. е. условная энтропия для криптоаналитика $H(W/V) \geq n - t$. Абоненты *A* и *B* хотят публично выбрать функцию сжатия g: $\{0, l\}^n$ в $\{0, l\}^b$, чтобы частичная информация *E* о *W* и ее полная информация о g дали произвольно мало информации о $K = g(W)$.

В работе [8] доказано, что при наличии некоторых ограничений можно выбрать функцию сжатия *G*, назначив $s < n - t$, и преобразовать $\{0,1\}^n$ в $\{0,1\}^b$, где $b = n - t - s$. Увеличивая *s* и публично выбирая функцию сжатия g из множества *G*, можно экспоненциально уменьшать информацию *E* о новом значении ключа *K*, правда, меньшего размера. Этот подход конкретизирован для формирования общего ключа с использованием квантового канала [9] и интерпретирован в монографии [10]. Применительно к рассматриваемой задаче исходная ситуация следующая. Абоненты *A* и *B* согласно протоколу *AB*-1 сформировали битовые строки S^A, S^B, по их мнению, секретным образом. Однако криптоаналитик *E*, используя протокол *ABE*-1, сформировал битовую строку S^E, которая с вероятностью P_{EA} совпадает с S^A. Для использования идеи повышения секретности абоненты *A* и *B* вместо одной строки формируют *r* строк, повторяя *r* раз пп. 1 и 2 протокола *AB*-1, но без проверки совпадения битовых строк для каждого сеанса. Абоненты *A* и *B* предполагают, что некоторое число строк S^A может совпадать с S^E, и, чтобы исключить это, сжимают полученные строки в итоговую строку заданного размера:

$$\{S_1^A, S_2^A, \ldots, S_r^A\}^{rb} \to \{K^A\}^b, \quad \{S_1^B, S_2^B, \ldots, S_r^B\}^{rb} \to \{K^B\}^b,$$

где b – длина $S_i^{A(B)}$ в битах. Далее *A* и *B* проверяют идентичность сформированных строк K^A и K^Bодним из способов, описанных ранее, а в случае совпадения имеют общий секрет $K^{AB} = K^A = K^B$.

При такой стратегии абонентов *A* и *B* криптоаналитик *E* вынужден выполнять те же операции, что *A* и *B*, в итоге получает $\{S_1^E, S_2^E, \ldots, S_r^E\}^{rb} \to \{K^E\}^b$ и может сравнить K^E с K^B. Однако строка $\{S_1^E, S_2^E, \ldots, S_r^E\}^{rb}$ с высокой вероятностью содержит хотя бы один элемент S_i^E, не совпадающий с S_i^A. Таким образом, параметр *r* в данном алгоритме имеет смысл параметра *s* из работы [8].

Анализ безопасности сформированного секрета. Оценим безопасность K^{AB}. Так как *A* и *B* провели *r* независимых сеансов синхронизации, не проверяя их результатов, вероятность того, что все сеансы закончились успехом, определяется выражением

$$P_{AB,r} = \prod_{i=1}^{r} P_{ABi} = (P_{AB})^r.$$

Согласно протоколу *AB*-1 следует обеспечить $P_{AB,r} \geq P_{\text{тр}}$. Для этого может понадобиться $m_{AB,r}$ серий по *r* синхронизаций в каждой. По аналогии с m_{AB} получим неравенство

$$m_{AB,r} \geq \frac{\ln(1 - P_{\text{тр}})}{\ln(1 - P_{AB,r})}.$$

В табл. 2 приведены значения $m_{AB,r}$, рассчитанные для вероятности $P_{\text{тр}} = 0{,}95$ и различных значений r и P_{AB}.

Таблица 2

Количество сеансов синхронизации *A* и *B* при различных значениях *r* для обеспечения необходимых значений вероятностей

r \ P_{AB}	0,8	0,90	0,95	0,99
5	8	4	3	1
10	27	7	4	2
20	259	24	7	2
50	209 895	580	38	4

Криптоаналитик E участвует во всех сеансах синхронизаций, которые проводят A и B, и останавливается в той серии, когда A и B получили K^{AB}. Вероятность того, что значение K^E совпадет со значением K^{AB}, определяется выражением $P_{EA,r} = \prod_{i=1}^{r} P_{EAi} = (P_{EA})^r$. Значения этой вероятности приведены в табл. 3.

Таблица 3

Вероятность совпадения значения K^E со значением K^{AB} при разных значениях P_{EA} и r

P_{EA} \ r	5	10	20	50
0,01	$1{,}0 \cdot 10^{-10}$	$1{,}0 \cdot 10^{-20}$	$1{,}0 \cdot 10^{-40}$	$1{,}0 \cdot 10^{-100}$
0,05	$3{,}1 \cdot 10^{-7}$	$9{,}7 \cdot 10^{-14}$	$9{,}5 \cdot 10^{-27}$	$8{,}8 \cdot 10^{-66}$
0,10	$1{,}0 \cdot 10^{-5}$	$1{,}0 \cdot 10^{-10}$	$1{,}0 \cdot 10^{-20}$	$1{,}0 \cdot 10^{-50}$
0,20	$3{,}2 \cdot 10^{-4}$	$1{,}0 \cdot 10^{-7}$	$1{,}0 \cdot 10^{-14}$	$1{,}1 \cdot 10^{-35}$

Если, например, абоненты A и B выбрали K = 3, N = 1000, L_1 = 8, L_2 = –7, d = 3500, $P_{\text{тр}}$ = 0,95, а по результатам моделирования P_{AB} = 0,951 и P_{EA} = 0,043, то при r = 50 необходимое количество серий синхронизаций m_{AB} = 38. При этом $P_{EA,r} = 8{,}8 \cdot 10^{-66}$.

Таким образом, величина $P_{EA,r}$ зависит от r экспоненциально и может быть выбрана сколь угодно малой путем увеличения r, в то время как для A и B вероятность успешного сеанса поддерживается за счет увеличения m_{AB}. Вместе с тем надо иметь в виду, что описанный эффект будет иметь место при таких параметрах сетей абонентов A и B, когда имеет место $P_{EA,r} \ll 1$, а $P_{AB,r} \approx 1$.

Возникает вопрос о выборе вида функции $K = g(S_1, S_2, \ldots, S_r)$, т. е. выборе функции свертки, и о плате за полученное увеличение конфиденциальности. В качестве функции свертки можно выбирать любое преобразование, свертывающее множество размером rb в r, при котором выходная величина зависит от всех битов входной. Таким свойством обладают, например, хеш-функции, в том числе и стандартизованного типа (СТБ 34.101.31–2011. Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности). Однако стандартизованные хеш-функции имеют стандартные размеры выходных величин, которые будут ограничивать размер сформированного секрета, поэтому можно использовать и другие преобразования. Например, можно применять свертку побитовым сложением по модулю 2 всех битов множества $\{S_i\}$:

$$K^{A(B)} = \sum_i^r S_i^{A(B)} (\text{mod } 2).$$

В результате получаем битовую последовательность длиной b, в которой каждый бит – сумма битов по модулю 2 из r слагаемых.

Размер сформированного секрета в битах будет равен размеру вектора ВК сетей абонентов A и B, который легко может быть изменен в случае необходимости изменением K или N. Важным положительным моментом является то, что закон распределения сформированного ключа близок к равномерному, причем равномерность возрастает с ростом r. В табл. 4 приведены значения отклонений частот повторения десятичных чисел, составляющих K^{AB}, от равномерного значения, выраженные в процентах. Данные отклонения были получены моделированием для K = 3, N = 1000, $L_1 = -7$, L_2 = 8, d = 3500, $r = 10$. В табл. 4 значение Δ_i рассчитывается по формуле

$$\Delta_i = \frac{(f_i - f_0)}{f_0} \cdot 100,$$

где f_i – частота i-го значения, f_0 – частота при равномерном распределении $f_0 = \frac{1}{L_2 - L_1 + 1} = 0{,}0625$, j_i – значение чисел из диапазона $[L_1, L_2]$. (Отрицательные значения чисел из всего диапазона $j_{i\,\text{исх}}$ переведены в положительные для правильности подсчета при моделировании.)

Таблица 4

Отклонение вероятности от равномерного распределения

j_i	0	1	2	3	4	5	6	7
$j_{i\text{исх}}$	0	1	2	3	4	5	6	7
Δ, %	–0,04	–0,17	0,26	0,34	–0,26	0,21	–0,27	–0,08
j_i	8	9	10	11	12	13	14	15
$j_{i\text{исх}}$	8	–1	–2	–3	–4	–5	–6	–7
Δ, %	–0,03	–0,42	0,35	0,41	–0,16	0,03	–0,03	0,38

Незначительная неравномерность, зафиксированная при моделировании, скорее всего, объясняется его ограниченным объемом (10^3 серий по 10 сеансов в каждой).

Заключение. Для решения задачи повышения конфиденциальности формируемого общего секрета, если он будет использоваться в качестве криптографического ключа, предлагается применять функцию сжатия g. В настоящей работе в качестве функции сжатия была рассмотрена свертка побитовым сложением по модулю 2 всех элементов множества $S_i^{A(B)}$. Таким образом, вероятность успеха $P_{EA,r}$ криптоаналитика зависит от величины r экспоненциально и может быть выбрана сколь угодно малой за счет увеличения r, в то время как для абонентов A и B вероятность успешного сеанса поддерживается за счет увеличения m. Закон распределения сформированного ключа после функции сжатия близок к равномерному, причем равномерность возрастает с увеличением r.

Список использованных источников

1. Kanter, I. The Theory of Neural Networks and Cryptography, Quantum Computers and Computing / I. Kanter, W. Kinzel. − 2005. – Vol. 5, no. 1. – P. 130−140.

2. Kinzel, W. Neural cryptography / W. Kinzel, I. Kanter // 9th Intern. Conf. on Neural Information Processing, Singapore, 2002. – Singapore, 2002. – Vol. 3. – P. 1351–1354.

3. Ruttor, A. Dynamics of neural cryptography / A. Ruttor, I. Kanter, W. Kinzel // Physical Review E. – 2007. – Vol. 75, iss. 5. – P. 1–9.

4. Плонковски, М. Криптографическое преобразование информации на основе нейросетевых технологий / М. Плонковски, П. П. Урбанович ; под ред. И. М. Жарского // Труды БГТУ. Сер. VI. Физико-математические науки и информатика. – Минск : БГТУ, 2005. – С. 161–164.

5. Голиков, В. Ф. О некоторых проблемах в задачах распределения криптографических ключей с помощью искусственных нейронных сетей / В. Ф. Голиков, Н. В. Брич, В. Л. Пивоваров // Системный анализ и прикладная информатика. – 2014. – № 1–3. – С. 42–46.

6. Голиков, В. Ф. Атака на синхронизируемые искусственные нейронные сети, формирующие общий секрет, методом отложенного перебора / В. Ф. Голиков, А. Ю. Ксеневич // Доклады БГУИР. – 2017. – № 8. – С. 48–53.

7. Голиков, В. Ф. Формирование общего секрета с помощью искусственных нейронных сетей / В. Ф. Голиков, М. Л. Радюкевич // Системный анализ и прикладная информатика. – 2019. – № 2. – С. 49–56.

8. Generalized privacy amplification / C. H. Bennett [et al.] // IEEE Transaction on Information Theory. – 1995. – Vol. 41, no. 6. – P. 1915–1923.

9. Боумейстер, Д. Физика квантовой информации / Д. Боумейстер, А. Экерт, А. Цайлингер. – М. : Постмаркет, 2002. – 276 с.

10. Килин, С. Я. Квантовая криптография: идеи и практика / С. Я. Килин, Д. Б. Хорошко, А. П. Низовцев. – Минск : Беларус. навука, 2007. – 391 с.

References

1. Kanter I., Kinzel W. *The Theory of Neural Networks and Cryptography, Quantum Computers and Computing*, 2005, vol. 5, no. 1, pp. 130−140.

2. Kinzel W., Kanter I. Neural cryptography. *9th International Conference on Neural Information Processing, Singapore, 2002*. Singapore, 2002, vol. 3, pp. 1351–1354.

3. Ruttor A., Kanter I., Kinzel W. Dynamics of neural cryptography. *Physical Review E*, 2007, vol. 75, iss. 5, pp. 1–9.

4. Plonkovski M., Urbanovich P. P., Zharsky I. M. (ed.). Kriptograficheskoye preobrazovaniye informatsii na osnove neyrosetevykh tekhnologii [Cryptographic transformation of information based on neural network technology]. Trudy Belorusskogo gosudarstvennogo tehnologicheskogo universiteta. Ser. VI. Fiziko-matematicheskiye nauki i informatika [*Proceedings of the Belarusian State Technical University. Ser. VI. Physics and Mathematics and Computer Science*]. Minsk, Belarusian State Technical University, 2005, pp. 161–164 (in Russian).

5. Golikov V. F., Brich N. V., Pivovarov V. L. O nekotorykh problemakh v zadachakh raspredeleniya kriptograficheskikh klyuchey s pomoshch'yu iskusstvennykh neyronnykh setey [About some problems in the distribution of cryptographic keys using artificial neural networks]. Sistemnyy analiz i prikladnaya informatika [*System Analysis and Applied Informatics*], 2014, no. 1–3, pp. 42–46 (in Russian).

6. Golikov V. F., Ksenevich A. Yu. Ataka na sinkhroniziruyemyye iskusstvennyye neyronnyye seti, formiruyushchiye obshchiy sekret, metodom otlozhennogo perebora [Attack on synchronized artificial neural networks, forming a common secret, by delayed brute force method]. Doklady Belorusskogo gosudarstvennogo universiteta informatiki i radiojelektroniki [*Reports of the Belarusian State University of Informatics and Radioelectronics*], 2017, no. 8, pp. 48–53 (in Russian).

7. Golikov V. F., Radziukevich M. L. Formirovaniye obshchego sekreta s pomoshch'yu iskusstvennykh neyronnykh setey [The formation of a common secret using artificial neural networks]. Sistemnyy analiz i prikladnaya informatika [*System Analysis and Applied Informatics*], 2019, no. 2, pp. 49–56 (in Russian).

8. Bennett C. H., Brassard G., Crepeau C., Maurer U. M. Generalized privacy amplification. *IEEE Transaction on Information Theory*, 1995, vol. 41, no. 6, pp. 1915–1923.

9. Boumeyster D., Ekert A., Tsaylinger A. Fizika kvantovoy informatsii. *Physics of Quantum Information*. Moscow, Postmarket, 2002, 276 p. (in Russian).

10. Kilin S. Ya., Khoroshko D. B., Nizovtsev A. P. Kvantovaya kriptografiya: idei i praktika. *Quantum cryptography: Ideas and Practice*. Minsk, Belaruskaya navuka, 2007, 391 p. (in Russian).

Информация об авторах

Радюкевич Марина Львовна, магистр технических наук, начальник испытательной лаборатории по требованиям безопасности информации, Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации», Минск, Беларусь, победитель конкурса молодых ученых на XXIV научно-практической конференции «Комплексная защита информации».
E-mail: 1218a@list.ru

Голиков Владимир Федорович, доктор технических наук, профессор кафедры «Информационные технологии в управлении», Белорусский национальный технический университет, Минск, Беларусь.

Information about the authors

Maryna L. Radziukevich, Master Sci. (Eng.), Head of the Testing Laboratory for Information Security Requirements, Scientific Production-Republican Unitary Enterprise "Research Institute for the Technical Protection of Information", Minsk, Belarus, Winner of the competition of young scientists at the XXIV scientific-practical conference "Comprehensive information protection."
E-mail: 1218a@list.ru

Vladimir F. Golikov, Dr. Sci. (Eng.), Professor of the Department of Information Technologies in Management, Belarusian National Technical University, Minsk, Belarus.

ISSN 1816-0301 (Print)
ISSN 2617-6963 (Online)
УДК 004.021
https://doi.org/10.37661/1816-0301-2020-17-1-109-118

Поступила в редакцию 01.10.2019
Received 01.10.2019

Принята к публикации 04.02.2020
Accepted 04.02.2020

Алгоритм хеширования на основе SHA-3 с использованием хаотических отображений

А. В. Сидоренко✉, М. С. Шишко

Белорусский государственный университет, Минск, Беларусь
✉E-mail: sidorenkoa@yandex.ru

Аннотация. Описан алгоритм хеширования данных, основанный на методе хеширования SHA-3 (Secure Hash Algorithm-3). Для увеличения производительности при сохранении безопасности хеширования в алгоритме использованы хаотические отображения. Проведено тестирование исходного и модифицированного алгоритмов на устойчивость к коллизиям, которое показало малую вероятность коллизий. Сделан статистический анализ выходных последовательностей, а также производительности алгоритмов. Проведено тестирование алгоритма с помощью набора статистических тестов SP 800-22, которое показало, что двоичная последовательность, генерируемая предложенным алгоритмом, близка к случайной. Протестирована также производительность алгоритма: скорость хеширования модифицированного алгоритма увеличилась на 60 % по сравнению со скоростью хеширования обычного SHA-3.

Ключевые слова: хеширование, шифрование, динамический хаос, лавинный эффект, статистический криптоанализ

Для цитирования: Сидоренко, А. В. Алгоритм хеширования на основе SHA-3 с использованием хаотических отображений / А. В. Сидоренко, М. С. Шишко // Информатика. – 2020. − Т. 17, № 1. – С. 109–118. https://doi.org/10.37661/1816-0301-2020-17-1-109-118

Hashing technique based on SHA-3 using chaotic maps

Alevtina V. Sidorenko✉, Maksim S. Shishko

Belarusian State University, Minsk, Belarus
✉E-mail: sidorenkoa@yandex.ru

Abstract. New hashing technique based on SHA-3 (Secure Hash Algorithm-3) is introduced. Chaotic maps are used in this technique to enhance performance without losing security. Introduced algorithm was tested for resistance against collisions, statistical analysis of output sequences was performed, hashing performance was evaluated. The testing showed a low collision probability. The testing corresponds the standards of National Institute of Standards and Technology and showed that output sequences are close to random. Performance testing showed 60 % enhancement in comparison with plain SHA-3.

Keywords: hashing, encryption, chaos, avalanche effect, statistical cryptanalisys

For citation: Sidorenko A. V., Shishko M. S. Hashing technique based on SHA-3 using chaotic maps. *Informatics*, 2020, vol. 17, no. 1, pp. 109–118 (in Russian). http://doi.org/10.37661/1816-0301-2020-17-1-109-118

Введение. В последнее время автономные роботы находят все большее применение в решении самых разнообразных задач, таких как ликвидация последствий чрезвычайных ситуаций, охрана территории, проведение медицинских операций, разведка. Для решения поставленной задачи робот оснащается разного рода средствами наблюдения, датчиками, навигационным и иным оборудованием. Данные, полученные с помощью такого оборудования, могут обраба-

тываться бортовым компьютером робота либо передаваться для обработки в пункт управления. В любом случае у робота должен быть способ общения с пунктом управления для получения команд и передачи полезной информации. Проводные технологии передачи данных для этого подходят плохо, так как любые провода существенно уменьшают мобильность робота.

Одним из наиболее перспективных направлений современной робототехники является разработка роботов, способных работать в группе, – так называемых роевых роботов [1, 2]. Их поведение должно быть коллективным для эффективного выполнения задачи. Каждый робот должен четко определять положение в пространстве, ориентацию, вектор направления движения и подзадачу, выполняемую другими участниками роя для того, чтобы корректировать свои действия. Компрометация и подлог информации даже одного участника роя приведут к дестабилизации всей системы и невозможности выполнять поставленную задачу. Поэтому обеспечение безопасности обмена информацией между участниками роя является очень важной задачей.

Совместные методы борьбы с неизвестными средами или синхронизация между различными группами роя способствуют достижению в области проектирования и изготовления таких аппаратных средств, как материнские платы Raspberry Pi 8 или Intel Galileo 9 (URL: https://www.raspberrypi.org/documentation/hardware/computemodule/datasheets/rpi_DATA_CM3plus_1p0.pdf). Они позволяют в настоящее время роботам обеспечивать передачу информации с увеличением возможностей ее обработки в устройствах связи с малой мощностью.

Существенным препятствием для широкомасштабного применения роботов в коммерческих приложениях является невозможность обеспечить их безопасность. В некоторых исследованиях подчеркнута необходимость разработки систем, в которых члены роя могут распознавать своих коллег и доверять им [3–5]. Ошибочное или злонамеренное включение новых членов роя может представлять потенциальный риск для целей роя, а также нарушать его безопасность.

Безопасность в любой информационной среде, включая роботизированные роевые системы, принципиально связана с предоставлением основных услуг, таких как конфиденциальность и целостность данных, аутентификация объектов и источника данных. Роботизированные роевые системы испытывают недостаток практических решений этих проблем. Теме безопасности в современных исследованиях уделяется недостаточное внимание в основном из-за сложных и гетерогенных характеристик роботизированных систем. Технология блокчейна [6] может обеспечить не только надежный peer-to-peer канал связи для агентов роя, но и способ преодоления потенциальных угроз, уязвимостей и атак.

Блокчейн – это новая технология, возникшая в поле биткоинов и демонстрирующая, что с помощью объединения одноранговых сетей с криптографическими алгоритмами группа агентов может достичь соглашения по конкретному положению дел и зафиксировать это соглашение без необходимости контролирующего органа. Комбинация блокчейна с другими распределенными системами, такими как роботизированные роевые системы, может предоставить необходимые возможности для того, чтобы сделать операции внутри роботизированного роя более безопасными, автономными и гибкими [7, 8]. Блокчейн является, по сути, общедоступной хронологической базой данных транзакций, записанных сетью агентов. Отдельные транзакции содержат сведения о том, кто и кому отправил сообщение. Данные сгруппированы в наборы, называемые блоками.

Каждый блок содержит информацию об определенном количестве транзакций (рис. 1), ссылку на предыдущий блок в цепочке блоков и ответ на сложную математическую задачу, известную как «доказательство работы». Концепция доказательства работы используется для проверки данных, связанных с этим конкретным блоком, а также для того, чтобы сделать разбиение на блоки вычислительно «жестким», тем самым не позволяя злоумышленникам изменять блок-цепочку в свою пользу. Она основана на криптографических вычислениях, в частности вычислении значений хеш-функции, которые дают непредсказуемые числовые последовательности. Блокчейн инкапсулирует все транзакции внутри блока в цифровом отпечатке, которым и является хеш. Любые различия во входных данных (порядке транзакций, количестве получателей и полезной информации и т. д.) будут приводить к различиям в выходных

данных (доказательстве работы), и таким образом будет получен другой цифровой отпечаток. Следовательно, одной из ключевых частей технологии блокчейна является хеш-функция.

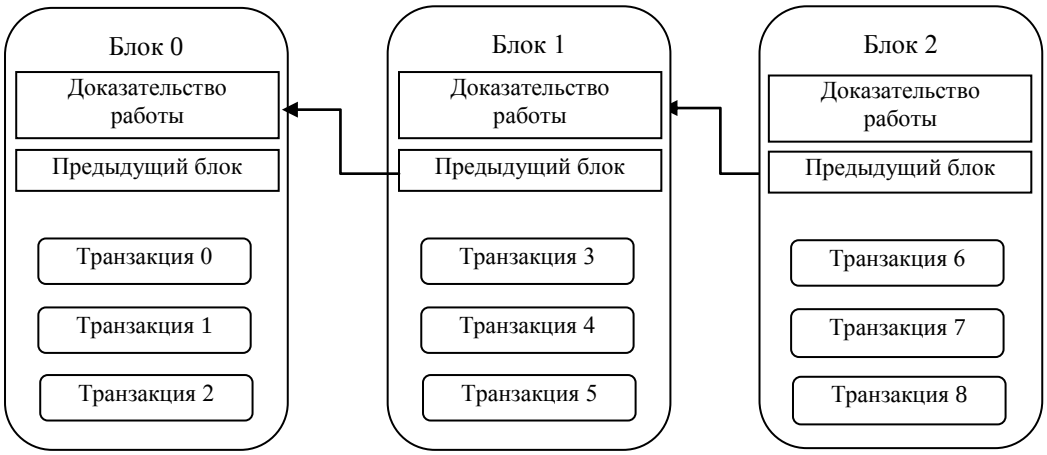


Рис. 1. Простая цепочка блоков блокчейна

Хеш-функции. Существуют два основных типа хеш-функций [9]: ориентированные на данные и ориентированные на безопасность (рис. 2). Хеш-функции, ориентированные на данные, используются в системах, работающих с большими объемами данных для ускорения их поиска, сравнения и выдачи. Они также подразделяются на не зависящие от данных и зависящие от данных хеш-функции. Не зависящие от данных функции хеширования не используют данные для вычисления хеш-суммы. Не зависящие от данных методы хеширования не хранят информацию об обработанных данных для оценки качества хеширования. Часто хеширующие функции являются предопределенными, хотя некоторые из них могут изучать распределения данных для улучшения результатов хеширования, таких как чувствительность к местоположению. Не зависящие от данных хеширующие функции можно разделить на четыре класса, основанные на следующих режимах: случайная проекция, локально-чувствительная проекция, обучающееся хеширование и структурированная проекция.

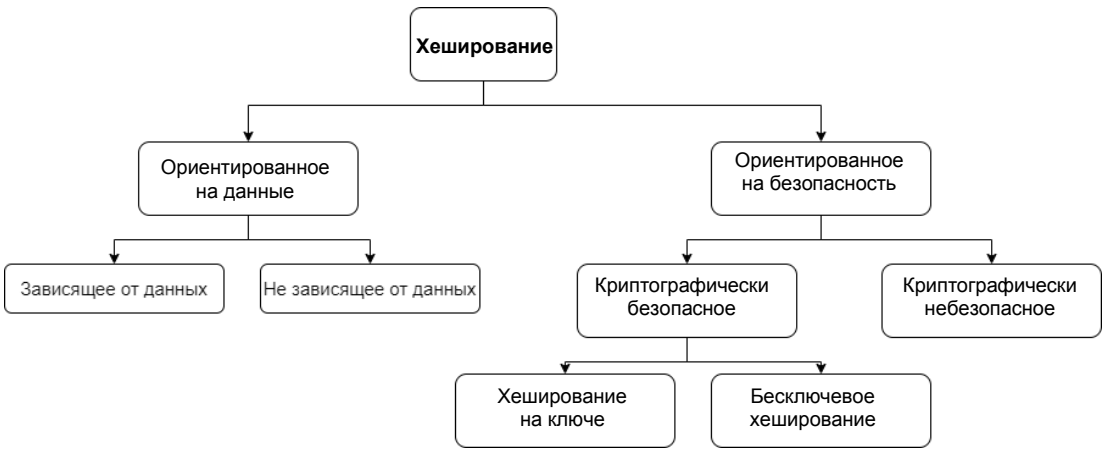


Рис. 2. Классификация хеш-функций

Зависящее от данных хеширование изучает хеширующие функции на основе набора данных, заданного для обучения, поэтому функции хеширования могут найти лучшие компактные коды для всех типов данных. Поскольку зависящие от данных методы хеширования очень чувствительны к базовым данным, они отличаются более быстрым временем запроса и меньшим по-

треблением памяти. Чтобы сохранить информацию о локальности и добиться лучшей избирательности, зависящее от данных хеширование должно точно соответствовать распределению данных в пространстве функций, однозначно определяя семейство хеширующих функций для этого набора обучающих данных. Кроме того, зависящее от данных хеширование обычно рассматривает сходство с особенностями обучающих данных.

Хеширование, ориентированное на безопасность, относится к методам, которые применяются для проверки целостности или аутентификации данных. Поскольку коды хеширования, ориентированного на безопасность, часто вычисляются намного дольше, чем коды хеширования, ориентированного на данные, хеш-таблица, как правило, не требуется или не может поддерживаться. Методы данной категории в первую очередь ориентированы на проблемы, поэтому они часто являются дорогостоящими и менее эффективными по сравнению с методами хеширования, ориентированного на данные.

Криптографически безопасное хеширование (криптографическое хеширование) относится к методам, хеширующая функция которых является односторонней, т. е. по значению хеш-суммы невозможно восстановить данные. При использовании таких методов длина ввода (называемая также «сообщение») является произвольной, а размер вывода (называемый также «дайджест сообщения») фиксирован. Хеш-результаты фиксированного размера применяются в качестве подписи в целях представления исходного сообщения для проверки. В связи с такой чувствительностью к безопасности криптографическое хеширование должно иметь строгий лавинный эффект, который заключается в значительном изменении хеш-выхода (примерно половины выходных битов), если есть даже незначительное изменение на входе (например, одного бита). Для использования в блокчейне важны именно эти особенности для подтверждения подлинности данных.

Хотя криптографически безопасное хеширование обладает хорошими свойствами безопасности, оно часто проводится неэффективно. Для приложений без серьезных проблем безопасности есть более простой механизм хеширования, называемый криптографически небезопасным хешированием или некриптографическим хешированием, который является более практичным. Для некриптографического хеширования, такого как хеш-функция Fowler-Noll-Vo (FNV), основная цель по-прежнему заключается в создании хеш-вывода для проверки, но процесс хеширования не должен учитывать криптографию. В результате становится возможной более быстрая обработка, более низкая вероятность коллизий, более высокая вероятность обнаружения небольших ошибок и более легкое обнаружение коллизий по сравнению с криптографически безопасным хешированием. Этот метод хеширования особенно популярен в приложениях, требующих быстрого поиска или обработки данных.

На данный момент известно множество различных методов хеширования. Стандарты этих методов разрабатываются научным сообществом и выбираются после однораноговых исследований Национальным институтом стандартов и технологий (англ. The National Institute of Standards and Technology, NIST), США. Одной из наиболее широко применяемых хеш-функций является SHA-1, которая используется в большом количестве приложений и протоколов безопасности сети Интернет.

Между тем в 2004 г. хеш-функции MD и SHA-0 были взломаны. Последующая атака на SHA-1 потребовала всего 2^{69} операций (CRYPTO-200), т. е. оказалась в 2000 раз быстрее, чем атака brute force (потребовала 2^{80} операций). Даже если на обычных компьютерах все еще сложно реализовать 2^{69} операций, такой результат, основанный на предыдущей атаке на SHA-0, является очень важным, поскольку варианты SHA-2 алгоритмически близки к SHA-1 и в конечном итоге производят дайджесты сообщений на принципах, аналогичных алгоритмам дайджестов сообщений MD4 и MD5.

В настоящее время необходим новый стандарт хеша, основанный на оригинальных подходах, должны быть найдены новые хеш-функции или улучшены уже существующие.

Предлагаемый алгоритм хеширования на основе SHA-3. В настоящей работе выполняется модификация хеш-функции SHA-3 (URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf), когда к существующей хеш-функции для укрепления ее свойств и увеличения производительности добавляется компонент хаоса.

Алгоритм SHA-3 использует функцию Keccak [10] для перестановки бит внутреннего состояния. Функция Keccak описывается как набор операций перестановки, выполненных над трехмерным массивом бит A, вид и внутренняя индексация которого показаны на рис. 3. Параметры функции обозначаются буквами греческого алфавита θ, ρ, π, χ, ι.

Функция $A' = \theta(A)$ суммирует по модулю два каждый бит внутреннего состояния с каждым битом из двух смежных столбцов (рис. 4):

1. Для всех пар (x, z), $0 \le x < 5$, $0 \le z < w$, $C[x, z] = A[x, 0, z]$ XOR $A[x, 1, z]$ XOR $A[x, 2, z]$ XOR $A[x, 3, z]$ XOR $A[x, 4, z]$.
2. Для всех пар (x, z), $0 \le x < 5$, $0 \le z < w$, $D[x, z] = C[(x - 1) \bmod 5, z]$ XOR $C[(x + 1) \bmod 5, (z - 1) \bmod w]$.
3. Для всех троек (x, y, z), $0 \le x < 5$, $0 \le y < 5$, $0 \le z$, $A'[x, y, z] = A[x, y, z]$ XOR $D[x, z]$.

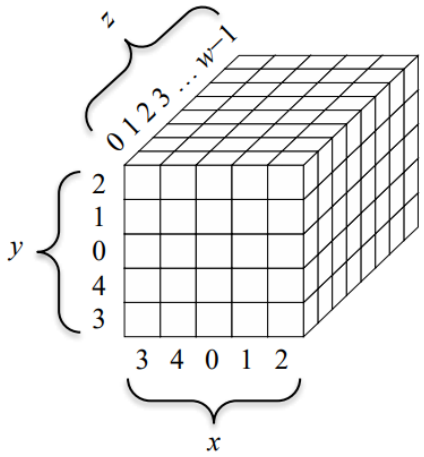


Рис. 3. Общий вид и индексация внутреннего состояния Keccak

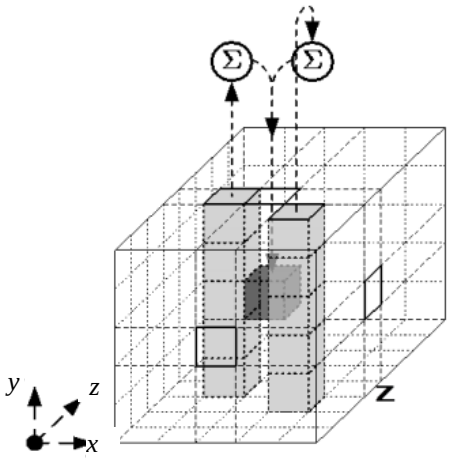


Рис. 4. Графическое представление функции θ(A)

Функция $A' = \rho(A)$ циклически сдвигает строки внутреннего состояния на различное количество бит в зависимости от номера строки (рис. 5).

Для всех z, $0 \le z < w$, $A'[0, 0, z] = A[0, 0, z]$. Пусть $(x, y) = (1, 0)$. Тогда для всех t от 0 до 23 выполняется соотношение: для всех z, $0 \le z < w$, $A'[x, y, z] = A[x, y, (z - (t + 1)(t + 2) / 2) \bmod w]$, $(x, y) = (y, (2x + 3y) \bmod 5)$.

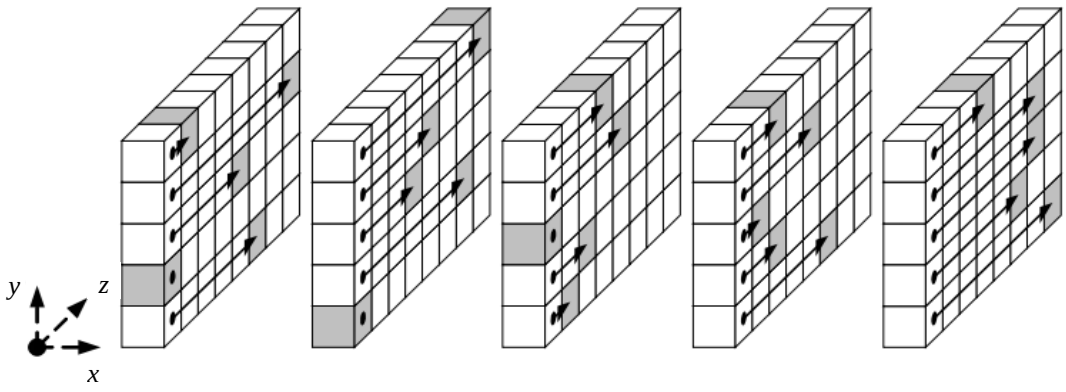


Рис. 5. Графическое представление функции ρ(A)

Функция $A' = \pi(A)$ производит перестановку бит в пределах битовой плоскости по следующему правилу: для каждой тройки (x, y, z), $0 \le x < 5$, $0 \le y < 5$, $0 \le z < w$, выполняется соотношение

$$A'[x, y, z] = A[(x + 3y) \bmod 5, x, z].$$

Функция $A' = \chi(A)$ суммирует по модулю два каждый бит с нелинейной функцией двух других бит той же строки:

$$A'[x, y, z] = A[x, y, z] \text{ XOR } ((A[(x + 1) \bmod 5, y, z] \text{ XOR } 1) * A[(x + 2) \bmod 5, y, z]).$$

Функция $A' = \iota(A)$ модифицирует некоторые биты первой строки в зависимости от текущего раунда, остальные строки при этом остаются неизменными.

В конечном итоге один раунд i_r функции Keccak представляет собой последовательное применение всех пяти функций:

$$\text{Rnd}(A, i\_r) = \iota(\chi(\pi(\rho(\theta(A))))), i_r).$$

В настоящей работе предлагается улучшить алгоритм перестановок, используемый в SHA-3, путем добавления хаотичности в функцию перестановок. Для этого следует модифицировать функцию перестановки Keccak для увеличения лавинного эффекта с помощью хаотического отображения. В оригинальной функции Keccak на шагах ρ и π перестановка элементов промежуточного состояния является предопределенной. Авторы предлагают выбирать индекс элемента для перестановки с помощью хаотического отображения на основании входных данных.

В качестве хаотического отображения используется логистическое отображение λ, которое имеет вид

$$\lambda(x_n) = Mx_n(1 - x_n),$$

где x_n принимает значения от 0 до 1. Параметр M означает скорость размножения (роста популяции). При значениях параметра от 3,57 до 4 система проявляет хаотическое поведение. Применение данного отображения позволяет уменьшить количество раундов перестановки до 12 без потери качества хеширования, что увеличивает производительность алгоритма.

Функция $\rho(A)$ принимает следующий вид: для всех z, $0 \le z < w$, $A'[0, 0, z] = A[0, 0, z]$, $(x, y) = (1, 0)$. Тогда для всех t от 0 до 23 выполняется соотношение: для всех z, $0 \le z < w$, $A'[x, y, z] = A[x, y, [w * \lambda(A[x, y, z] / 2^w)]]$, $(x, y) = (y, (2x + 3y) \bmod 5)$.

Функция $\pi(A)$ принимает следующий вид: для каждой тройки (x, y, z), $0 \le x < 5$, $0 \le y < 5$, $0 \le z < w$, выполняется соотношение

$$A'[x, y, z] = A[\lfloor 5 * \lambda(A[a, y, z] / 2^w) \rfloor, x, z].$$

Тестирование алгоритмов. Для оценки качества модифицированной хеш-функции были проведены следующие тесты: на лавинный эффект, на устойчивость к атаке «дней рождения», тестирование свойств выходной последовательности по методике NIST.

Лавинный эффект – одно из важнейших свойств, которыми должна обладать криптографическая хеш-функция. Он проявляется в том, что изменение значения малого количества битов во входном тексте ведет к «лавинному» изменению значений выходных битов хеш-суммы. Если криптографический алгоритм не обладает лавинным эффектом в достаточной степени, криптоаналитик может сделать предположение о входной информации, основываясь на выходной. Таким образом, достижение лавинного эффекта является важной целью при разработке криптографического алгоритма.

Для тестирования лавинного эффекта описанной выше хеш-функции был составлен словарь из 450 000 уникальных сообщений различной длины. Для каждого сообщения была вычислена хеш-сумма, затем в исходном сообщении изменен один или несколько случайных бит и уже для измененного сообщения рассчитана хеш-сумма. Далее хеш-суммы исходного и измененного

сообщений сравнивались при помощи расстояния Хемминга. В табл. 1 показано распределение количества измененных бит хеша при изменении одного бита сообщения для алгоритмов SHA-2 и SHA-3. Для наглядности эти данные представлены в виде гистограммы (рис. 6), на которой видно, что предлагаемый алгоритм имеет распределение, схожее с SHA-2 и SHA-3.

Таблица 1

Численные значения изменения количества бит
при тестировании лавинного эффекта для трех алгоритмов

Количество бит	Алгоритм хеширования		
	SHA-2	SHA-3 Keccak	SHA-3 Chaotic Keccak
<80	0,0	0,0	0,0
88	1,0	3,0	1,0
96	62,0	52,0	59,0
104	962,0	987,0	1009,0
112	6506,0	6586,0	6614,0
120	17 630,0	17 506,0	17 463,0
128	18 529,0	18 537,0	18 527,0
136	7831,0	7870,0	7799,0
144	1342,0	1309,0	1383,0
152	71,0	82,0	79,0
>160	1,0	3,0	1,0

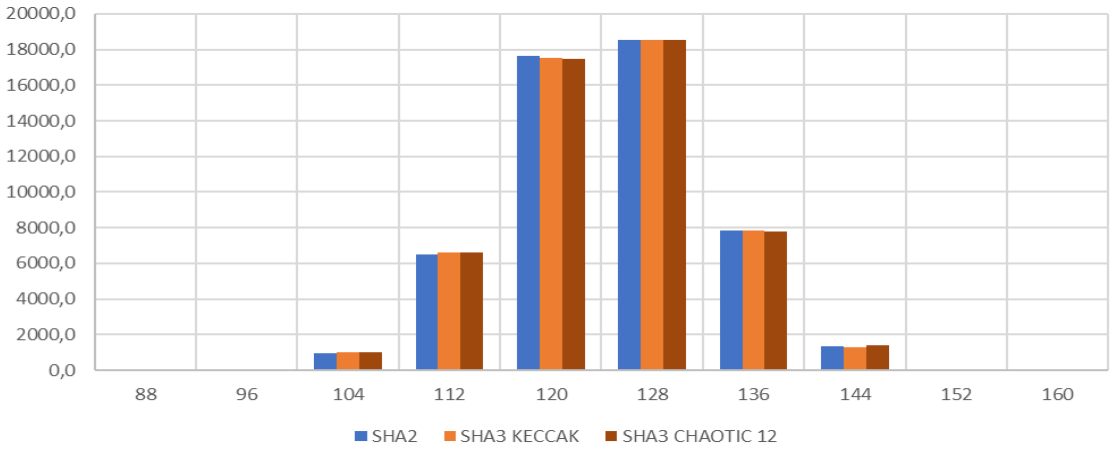


Рис. 6. Гистограмма изменения количества бит при тестировании лавинного эффекта

Затем алгоритм был протестирован на стойкость к атаке «дней рождения». Данная атака основана на парадоксе дней рождения, который заключается в том, что в группе, состоящей из 23 или более человек, вероятность совпадения дней рождения хотя бы у двух человек превышает 50 %. Суть метода состоит в значительном уменьшении количества передаваемых хеш-функции аргументов, необходимых для обнаружения коллизии. Это связано с тем, что если хеш-функция генерирует n-битное значение, то число случайных аргументов хеш-функции, для которого с большой вероятностью будет обнаружена хотя бы одна коллизия хеш-функции (т. е. найдется хотя бы одна пара равных хеш-кодов, полученных на разных аргументах), равно не 2^n, а только около $2^{n/2}$.

Для оценки стойкости хеш-функции к атакам «дней рождения» был использован тот же словарь, что и для проверки лавинного эффекта. Однако теперь был проведен поиск коллизий хеш-сумм для сообщений из словаря, который коллизий не выявил.

Пакет тестов NIST STS был разработан отделом безопасности компьютерных технологий NIST. Полное описание пакета тестов, рекомендации по выбору методики исследований

и интерпретации результатов приведены в публикации (URL: https://nvlpubs.nist.gov/ nistpubs/ legacy/sp/nistspecialpublication800-22r1a.pdf). Последняя на момент исследований версия 2.2.1 пакета есть в открытом доступе. Применительно к исследуемой хеш-функции данный пакет тестов позволяет определить, насколько она статистически безопасна и устойчива к возникновению коллизий.

Всего пакет NIST содержит 15 тестов, однако некоторые из них являются сложными и фактически выборки с последовательностями проходят 188 тестов. Общая структура отдельно взятого теста для каждой последовательности имеет следующий вид:

1. Выдвигаются нулевая гипотеза H_0 (предположение о том, что данная двоичная последовательность S_q случайная) и альтернативная гипотеза H_a (последовательность неслучайная).

2. По последовательности S_q и соответствующим тесту алгоритмам рассчитывается значение статистики теста S.

3. С использованием специальной функции и значения статистики теста рассчитывается значение вероятности $P \in [0, 1]$, которая суммирует силу доказательств против нулевой гипотезы.

4. Значение вероятности P сравнивается с уровнем значимости, который выбирается, как правило, в интервале $\alpha \in [0{,}001;\ 0{,}01]$ и отражает вероятность ошибок первого рода (неправильного отвергания «хорошей» (прошедшей тест) последовательности). Если $P < \alpha$, гипотеза H_0 отвергается и принимается альтернативная гипотеза H_a. В противном случае принимается гипотеза H_0 (последовательность случайная).

В соответствии с рекомендациями NIST тестирование генераторов последовательностей (в рассматриваемом случае – алгоритмов хеширования) с применением пакета тестов в общем случае должно включать ряд этапов:

1. Формирование наборов последовательностей для тестирования. Для исходной версии метода были сформированы шесть выборок из 100 последовательностей длиной по 104 857 600 бит в каждой, т. е. каждая выборка содержала 1 048 576 100 бит. Выборки формировались путем вычисления хеш-значений сообщений длиной по 256 байт для псевдослучайных наборов сообщений, генерируемых линейным конгруэнтным генератором из библиотеки на языке C++.

2. Тестирование выборок пакетом. Для тестирования применялись все 15 (188) тестов пакета с предлагаемыми по умолчанию параметрами. Порядок тестирования последовательностей из выборок был описан выше.

3. Оценку значений вероятности P. Анализ сформированных значений P позволяет вскрыть конкретные дефекты тестируемых последовательностей и хеш-функции в целом.

4. Оценку прохождения теста(ов) последовательностями в выборках путем сравнения значений вероятности P с выбранным уровнем значимости. На этом этапе также вычисляется процент прошедших тест последовательностей в выборке.

5. Интерпретацию полученных результатов. NIST предлагает два основных подхода (которые, однако, не являются исчерпывающими) к оценке качества последовательностей и прохождению теста всей выборкой. Первый подход основан на оценке равномерности распределения значений вероятности P для последовательностей из выборки, второй – на оценке процента прошедших тест последовательностей из выборки. При представлении результатов исследований примем второй подход в качестве основного. Для успешного прохождения каждого отдельного теста всей тестируемой выборкой в соответствии с выбранными по умолчанию параметрами тестирования необходимо, чтобы процент хороших последовательностей в выборке был не менее 96.

В целом при оценке последовательностей и интерпретации результатов могут быть сделаны следующие выводы:

– тестирование не показало отклонений от случайности;

– тестирование четко указывает на отклонение от случайности;

– тестирование безрезультатно.

В табл. 2 приведены результаты тестирования. Модифицированный SHA-3 прошел все тесты, кроме универсального теста Маурера, поэтому последовательность, выдаваемую данным алгоритмом, можно считать случайной.

Таблица 2

Результаты тестирования набором статистических тестов NIST

Тест	Алгоритм хеширования		
	SHA-2	SHA-3	Chaotic SHA-3
Frequency	0,971 699	0,455 937	0,816 537
Block Frequency	0,080 519	0,455 937	0,971 699
Runs	0,935 716	0,946 308	0,213 309
Longest Run	0,334 538	0,924 076	0,262 249
Rank	0,090 936	0,699 313	0,616 305
DFT	0,001 895	0,514 124	0,191 687
Non-Owerlaping Template	0,678 686	0,474 986	0,224 821
Owerlaping Template	0,090 936	0,437 274	0,262 249
Universal	0	0	0
Linear Complexity	0,911 413	0,834 308	0,534 146
Serial	0,000 082	0,000 003	0,494 392
Entropy	0,275 709	0,007 566	0,911 413
Cumulative Sums	0,145 326	0,115 387	0,494 392
Всего пройдено	*11*	*10*	*12*

В работе также была проведена оценка производительности трех алгоритмов. Тестирование проводилось на персональном компьютере под управлением Windows 10 с процессором Intel core i-5 2330M. Самую высокую производительность показал SHA-2 – 77,1 Мб/с, SHA-3 показал наихудшую производительность – 16 Мб/с. Производительность же модифицированного SHA-3 оказалась 26 Мб/с, что на 60 % больше, чем производительность обычного SHA-3.

Заключение. Разработан алгоритм хеширования на основе SHA-3 с использованием хаотических отображений. С целью увеличения производительности в качестве хаотического отображения в функции перестановки используется логистическое отображение.

Для оценки качества модифицированной хеш-функции были проведены тест на лавинный эффект, тест на устойчивость к атаке «дней рождения» и тестирование свойств выходной последовательности по методике NIST. Результаты тестирования лавинного эффекта очень схожи с результатами тестирования SHA-2 и SHA-3 и показывают, что примерно половина битов хеша меняется при изменении одного бита в хешируемых данных. Атака «дней рождения» коллизий не выявила. По результатам тестирования пакетом статистических тестов NIST алгоритм SHA-3 с модифицированной функцией перестановок прошел все тесты, кроме универсального теста Маурера, поэтому последовательность, выдаваемую данным алгоритмом, можно считать случайной.

References

1. Bayindir L. A review of swarm robotics tasks. *Neurocomputing*, 2016, vol. 172, pp. 292–321.

2. Navarro I., Matia F. An introduction to swarm robotics. *ISRN Robotics*, 2013, vol. 2013, pp. 1–10.

3. Higgins F., Tomlinson A., Martin K. M. Survey on security challenges for swarm robotics. *Fifth International Conference on Autonomic and Autonomous Systems, 20–25 April 2009, Valencia, Spain*. Valencia, 2009, pp. 307–312.

4. Priyadarshini I. *Cyber Security Risks in Robotics*, 2017. Available at: https://www.researchgate.net/publication/319354229_Cyber_security_risks_in_Robotics (accessed 21.07.2019).

5. Shah R. *Security Landscape for Robotics*, 2019. Available at: https://arxiv.org/abs/1904.03033v1 (accessed 21.07.2019).

6. Nakamoto S. *Bitcoin: a Peer-to-Peer Electronic Cash System*, 2008, Available at: https://bitcoin.org/bitcoin.pdf (accessed 21.07.2019).

7. Lopes V., Alexandre L. A. *An Overview of Blockchain Integration with Robotics and Artificial Intelligence*, 2018. Available at: https://arxiv.org/abs/1810.00329v1 (accessed 21.07.2019).

8. Ferrer E. C. *The Blockchain: a New Framework for Robotic Swarm Systems*, 2017. Available at: https://arxiv.org/abs/1608.00695v4 (accessed 21.07.2019).

9. Chi L., Zhu X. Hashing techniques: a survey and taxonomy. *ACM Computing Surveys*, 2017, vol. 50, no. 1, pp. 1–36. https://doi.org/10.1145/3047307

10. Bertoni G., Daemen J., Peeters M., Assche van G. *The Keccak Reference*, 2011. Available at: https://keccak.team/files/Keccak-reference-3.0.pdf (accessed 21.07.2019).

Информация об авторах

Сидоренко Алевтина Васильевна, доктор технических наук, профессор кафедры физики и аэрокосмических технологий, факультет радиофизики и компьютерных технологий, Белорусский государственный университет, Минск, Беларусь.
E-mail: sidorenkoa@yandex.ru

Шишко Максим Сергеевич, аспирант кафедры физики и аэрокосмических технологий, факультет радиофизики и компьютерных технологий, Белорусский государственный университет, Минск, Беларусь.
E-mail: maxshishko@yandex.ru

Information about the authors

Alevtina V. Sidorenko, Dr. Sci. (Eng.), Professor of Department of Physics and Aerospace Technology, Faculty of Radiophisics and Computer Technology, Belarusian State University, Minsk, Belarus.
E-mail: sidorenkoa@yandex.ru

Maksim S. Shishko, Postgraduate Student of Department of Physics and Aerospace Technology, Faculty of Radiophisics and Computer Technology, Belarusian State University, Minsk, Belarus.
E-mail: maxshishko@yandex.ru

Правила для авторов

Редакция журнала «Информатика» просит авторов руководствоваться приведенными ниже правилами:

1. Статьи принимаются в редакцию через электронную систему подачи по адресу http://inf.grid.by в формате файлов текстовых редакторов Microsoft Word. Основной текст статьи не должен превышать 17 стр., включая рисунки, таблицы и достаточное количество наиболее актуальных ссылок; обзорной статьи – 10 стр., включая все основные ссылки. Текст набирается с переносами, шрифт Times New Roman 11 пт, интервал между строками одинарный, абзацный отступ 0,5 см, поля по 2,5 см со всех сторон.

Изложенный в статье материал должен быть четко структурированным: введение, цели и задачи, методы, результаты, заключение (выводы).

2. Статьи о результатах работ, проведенных в научных учреждениях, должны иметь разрешение на публикацию (сопроводительное письмо за подписью руководителя или выписку из заседания ученого совета, отдела или кафедры, акт экспертизы).

3. Статья в обязательном порядке должна иметь следующую структуру: индекс по универсальной десятичной классификации (УДК); инициалы и фамилии всех авторов, название статьи, полное название учреждений, где работают авторы, с указанием города, страны, аннотацию (150–250 слов), подрисуночные надписи, названия таблиц и ключевые слова (7–10) на русском и английском языках, адрес электронной почты контактного лица.

4. Аннотация (авторское резюме) должна кратко представлять результаты работы и быть информативной, содержательной. Приветствуется структура аннотации, повторяющая структуру статьи и включающая введение, цели и задачи, методы, результаты, заключение.

5. Формулы, рисунки, таблицы в статье нумеруются в соответствии с порядком их упоминания в тексте. Ссылки на рисунки и таблицы в тексте обязательны. Рисунки должны быть выполнены с хорошим разрешением в масштабе, позволяющем четко различать надписи и обозначения. Подрисуночные подписи с расшифровкой всех позиций, представленных на рисунке, набираются шрифтом гарнитуры основного текста размером 9 пт. Цветные иллюстрации печатаются только в том случае, когда это необходимо для понимания излагаемого материала.

6. Набор формул выполняется в формульном редакторе Microsoft Equation или Math Type. Прямым шрифтом набираются: греческие и русские буквы; математические символы (sin, lg, ∞); символы химических элементов (C, Cl, CHCl3); цифры (римские и арабские); векторы; индексы (верхние и нижние), являющиеся сокращениями слов. Курсивом набираются латинские буквы, символы физических величин (в том числе и в индексе).

7. Сокращения в тексте статьи (за исключением единиц измерения) могут быть использованы только после упоминания полного термина. Единицы измерения физических величин следует приводить в Международной системе единиц (СИ).

8. Цитируемые в статье фамилии авторов теорем, теорий, законов и т. д. следует приводить в скобках на языке оригинала после русского написания. Например, теорема Эйлера (Euler).

9. Список использованной литературы оформляется в соответствии с требованиями Высшей аттестационной комиссии Республики Беларусь (ГОСТ 7.5–2008). Номер литературной ссылки в тексте дается порядковым номером в квадратных скобках. Ссылаться на неопубликованные работы не допускается.

10. Отдельно приводится список цитированных источников в *романском* (латинском) алфавите со следующей структурой: авторы (транслитерация), название статьи в транслитерированном варианте [перевод названия статьи на английский язык в квадратных скобках], название русскоязычного источника (транслитерация) [перевод названия источника на английский язык – парафраз (для журналов можно не делать)], выходные данные с обозначениями на английском языке.

11. Поступившие в редакцию статьи направляются на рецензирование специалистам. Основными критериями целесообразности публикации являются новизна и информативность статьи. Если по рекомендациям рецензента статья возвращается автору на доработку, то переработанная рукопись вновь рассматривается редколлегией. Статьи не по профилю журнала возвращаются авторам после заключения редколлегии.

12. Статьи, направляемые на доработку, должны быть возвращены в исправленном виде с ответами на все замечания.

13. Редакция журнала предоставляет возможность первоочередного опубликования статей, представленных лицами, которые осуществляют послевузовское обучение (аспирантура, докторантура, соискательство) в год завершения обучения.

14. Авторы несут ответственность за направление в редакцию статей, уже опубликованных ранее или принятых к публикации другими изданиями.

15. Редакция оставляет за собой право на редакционные изменения, не искажающие основное содержание статьи. Окончательное решение о публикации принимается редакционной коллегией.

Индексы

00827

для индивидуальных подписчиков

008272

для предприятий и организаций

ИНФОРМАТИКА Т. 17, № 1 январь–март 2020