СИСТЕМНЫЙ АНАЛИЗ И ПРИКЛАДНАЯ ИНФОРМАТИКА
№ 2, 2018

SYSTEM ANALYSIS AND APPLIED INFORMATION SCIENCE
No 2, 2018

Международный Научно-технический журнал

Издается с декабря 2012 года

Учредитель

Белорусский национальный технический университет

Главный редактор

Сергей Васильевич Харитончик

Редакционная коллегия

В. Ф. Голиков (зам. главного редактора), В. А. Богуш, Т. В. Борботько, В. Б. Байбурин (РФ), Д. Ю. Большаков (РФ), Л. С. Герасимович, Н. Н. Гурский, Ю. М. Захарик, И. А. Каляев (РФ), Г. О. Кипиани (Грузия), Э. Г. Лазаревич, В. А. Липницкий, А. А. Лобатый, В. А. Мищенко, Е. И. Никифорович (Украина), А. А. Прихожий, И. А. Сатиков, В. В. Старовойтов, П. П. Урбанович, А. Патрин (Польша), Ю. Н. Петренко (ответственный секретарь), Н. Н. Ташатов (Казахстан), А. В. Чигарев, Д. К. Щеглов (РФ)

International Science and Technique Journal

Published since December, 2012

Founnder

Belarusian National Technical University

Editor-in-chief

Sergei V. Kharytonchyk

Editorial board

V. Golikov (deputy editor-in-chief), V. Bogush, T. Borbotko, V. Baiburin (RF), D. Bolshakov (RF), N. Gurskiy, L. Gerasimovich, J. Zaharik, I. Kalyaev, G. Kipiani (Georgia), E. Lazarevich, V. Lipnitsky, A. Lobaty, V. Mishchenko, E. Nikiforovich (Ukraine), A. Prihozhy, I. Satikov, V. Starovoytov, P. Urbanovich, A. Patrin (Poland), Y. Petrenko (executive secretary), N. Tashcatov (Kazakhstan), A. Chigarev, D. Shcheglov (RF)

Журнал включен в "Перечень научных изданий Республики Беларусь для опубликования результатов диссертационных исследований".

Журнал включен в международные каталоги и базы данных:

- Российский индекс научного цитирования (РИНЦ)
- Научная электронная библиотека eLIBRARY.RU
- Электронно-библиотечная система (ЭБС) издательства Лань
- DOAJ https://doaj.org/toc/2414-0481
- Google Scholar
- Киберленинка
- EBSCO
- BASE Search
- OpenAIRE
- WorldCat
- OpenDOAR
- ROAR

Содержание

СИСТЕМНЫЙ АНАЛИЗ

Прихожий А. А., Ждановский А. М.
Метод оценки квалификации и оптимизация состава профессиональных групп программистов 4

УПРАВЛЕНИЕ ТЕХНИЧЕСКИМИ ОБЪЕКТАМИ

Михайлов В. Г.
Анализ методов получения продольных профилей дорог..... 13

ОБРАБОТКА ИНФОРМАЦИИ И ПРИНЯТИЕ РЕШЕНИЙ

Романчак В. М.
Аппроксимация сингулярными вейвлетами 23

Рудикова Л. В., Данильчик В. В.
О подходах к созданию системы автоматизации, связанной с социально-экономическими перемещениями людей..... 29

Contents

SYSTEM ANALYSIS

Prihozhy A., Zhdanouski A.
Method of qualification estimation and optimization of professional teams of programmers 4

MANAGEMENT OF TECHNICAL OBJECTS

Mikhailov V. G.
The analysis of methods of reception of longitudinal profile of roads..... 13

DATA PROCESSING AND DECISION-MAKING

Romanchak V. M.
Approximately singular wavelet 23

Rudikova L. V., Danilchik V. V.
On the creation of the automation system related to social-economic movements of people..... 29

ЗАЩИТА ИНФОРМАЦИИ

Липницкий В. А., Середа Е. В.
Свойства g-орбит двойных ошибок и их инвариантов в бчх-кодах 40

Соколов А. В., Жданов О. Н.
Класс совершенных троичных решеток 47

INFORMATION SECURITY

Lipnickij V., Serada A.
Properties of groups g of double errors and its invariants in bch codes 40

Sokolov A.V., Zhdanov O. N.
The class of perfect ternary arrays 47

Ответственный секретарь редакции
Петренко Ю. Н.

Технический редактор
Лакин В. И.

Адрес редакции
ул. Франциска Скорины 25/3, Минск, 220114,
Республика Беларусь
Тел. +375 17 267-66-84
e-mail: CA_PI@bntu.by

Executive secretary of the editorial board
Y. Petrenko

Technical Editor
V. Lakin

Editorial board address
25/3 Franciska Skariny str., Minsk, 220114,
Republic of Belarus
Tel. +375 17 267-66-84
e-mail: CA_PI@bntu.by

Свидетельство о государственной регистрации средства массовой информации № 1540 от 08.06.2012, выданное Министерством информации Республики Беларусь

Подписано в печать 16.07.2018. Формат бумаги 60×84 1/8. Бумага офсетная.
Отпечатано на ризографе. Усл. печ. л. 6,57. Уч.-изд. л. 2,55. Тираж 100 экз. Заказ 630.
Отпечатано в БНТУ. Лицензия ЛП № 02330/74 от 03.03.2014

220013, г.Минск, пр. Независимости, 65.

© Системный анализ и прикладная информатика, 2017

СИСТЕМНЫЙ АНАЛИЗ

SYSTEM ANALYSIS

УДК 004.4-004.9

А.А. ПРИХОЖИЙ, А.М. ЖДАНОВСКИЙ

МЕТОД ОЦЕНКИ КВАЛИФИКАЦИИ И ОПТИМИЗАЦИЯ СОСТАВА ПРОФЕССИОНАЛЬНЫХ ГРУПП ПРОГРАММИСТОВ

Белорусский национальный технический университет

Рассматривается проблема формирования и оптимизации команд программистов с учетом квалификации и уровня владения технологиями и инструментами программирования. Известные технологические среды для организации работы команд, такие как Agile, формулируют лишь общие требования и принципы формирования коллективов и распределения работ между ними. Предлагается метод формализации оценки квалификации отдельных программистов и целых программистских групп. Исходными являются данные о наиболее востребованных технологиях и инструментах программирования, их рейтинге, а также результаты опроса программистов об уровне владения ими. Квалификация группы программистов оценивается с учетом требований к конкретному проекту как величина, интегрирующая три составляющие: среднюю квалификацию программистов, включаемых в группу; квалификацию группы по лучшим представителям по каждой из технологий; пороговые значения уровней квалификации программистов и групп программистов по каждой из технологий, а также пороговые значения интегрированной квалификации, отражающие специфику конкретного проекта. Вклад каждой составляющей определяется варьируемыми. весовыми коэффициентами. Метод положен в основу генетического алгоритма, выполняющего поиск количества, размера и состава программистских групп, которые имеют максимальную суммарную квалификацию. Разработано программное обеспечение и проведены вычислительные эксперименты на выборке программистов, окончивших белорусские университеты. Полученные результаты демонстрируют реальную способность системы находить количество, состав и размеры групп программистов, увеличивающие суммарную квалификации групп до 30% при минимизации числа незадействованных разработчиков. Результаты доказывают практическую значимость разработки в сфере технологий и средств управления профессиональными коллективами программистов.

Ключевые слова: *Программист, технология, инструментарий, квалификация, группа программистов, состав группы, оптимизация.*

Введение

Технология Agile [1] гибкой разработки программного обеспечения позволяет вырабатывать требования и находить решения благодаря совместным усилиям групп разработчиков и заказчиков. Она базируется на адаптивном планировании, эволюционном развитии, постоянном совершенствовании, быстром и гибком реагировании на изменения. Хотя Agile используется во многих средах разработки, она требует дальнейшего развития для распределенных команд программистов. Правильное сочетание экспертов имеет решающее значение при включении разработчиков в команды. Неправильное распределение работ может исключить подключение ведущих специалистов. Поручение работы команде, которой трудно найти подходящего специалиста, увеличивает общие затраты на набор персонала и выполнение работ, затрудняет правильный подбор людей в распределенную команду.

Успех распределенного коллектива программистов в реализации крупного проекта сильно зависит от адекватности используемых технологий и инструментов программирования, а также от умения эффективно декомпозировать проект на части. Эти части должны быть поручены тем группам программистов, которые обладают необходимыми для этого знаниями и технологиями. Проблема оптимального разбиения программистов на группы сформулирована в работе [2]. Она является многофакторной и слабо структурированной. В [2] учтены следующие факторы: производительность каждого программиста, способность пар программистов увеличивать или снижать производительность в процессе совместной работы, возрастание

затрат на интерфейсы между программистами при увеличении числа программистов в группе. На решение подобного рода проблем ориентированы эволюционные методы оптимизации [3, 4]. В работе [5] предложен генетический алгоритм решения проблемы, однако он не учитывает уровень владения программистами технологиями и инструментами программирования, необходимыми для работы над проектом.

В данной статье анализируются современные технологии и инструменты программирования, оценивается уровень владения ими каждым из программистов и целыми программистскими группами, оптимизируется размер и состав программистских групп.

Рейтинг технологий и инструментов программирования

Анализ результатов исследований компании RedMonk [6] о популярности языков и инструментальных средств программирования и результатов исследований организации IEEE Spectrum [7] о рейтинге языков позволил разработать таблицу, описывающую множество T из 16 основных технологий и инструментов. Для каждой технологии указан рейтинг, показывающий значимость и широту применения технологии, а также требование обязательного владения ею хотя бы одним членом группы программистов. По назначению все множество технологий делится на 6 подмножеств. Системы контроля версий и управления проектами включают Git, Tortoise SVN, VJR и TFS с рейтингом 0.3 каждая. К средам разработки относятся Visual Studio и Eclipse, рейтинг обоих 0.6. Системы управления базами данных представлены Oracle SQL (рейтинг 0.5) и Microsoft SQL Server (рейтинг 0.6). Языки программирования представлены Java, C#, Visual Basic, C++, Java Script и XSL с рейтингом 1.0, 0.9, 0.7, 0.9, 0.8 и 0.6 соответственно. Операционные системы представлены Windows и Linux с рейтингом 0.6 и 0.5 соответственно. Следует подчеркнуть, что высокий рейтинг технологии показывает необоснованность создания коллективов программистов, в которых нет ни одного эксперта по данной технологии.

Ключевые технологии и инструменты программирования

№	Название	Код	Рейтинг	Обязать
1	Git	VGT	0.3	нет
2	Tortoise SVN	VTS	0.3	нет
3	TFS	VTF	0.3	нет
4	Jira	VJR	0.3	нет
5	Visual Studio	DVS	0.6	да
6	Eclipse	DEC	0.6	да
7	Oracle SQL	OBM	0.5	нет
8	Microsoft SQL Server	DBM	0.6	нет
9	Java	LJ	1.0	да
10	C#	LC#	0.9	да
11	Visual Basic	LVB	0.7	нет
12	C++	LCP	0.9	да
13	Java script	LJS	0.8	да
14	XSL	LXS	0.6	нет
15	Windows	OSW	0.6	да
16	Linux	OSL	0.5	да

Уровень владения программистом технологией / инструментом

Для решения второй задачи оценки уровня владения программистами технологиями и инструментами использован метод опроса. Каждому из опрашиваемых программистов предложено заполнить анкету, в которой он указывает уровень *level* владения каждой из технологий. Уровень *level* определяется по пятибалльной шкале: 0 – отсутствие знания технологии; 0.25 – минимальное знание; 0.5 – промежуточные навыки; 0.75 – расширенный опыт владения технологией; 1 – знания и опыт эксперта. Экспертом считается программист, который владеет теоретическими экспертными знаниями, разработал не менее двух крупных проектов и проработал не менее двух лет с данной технологией. Программист обладает расширенными навыками, если выполняются два критерия из трех, и обладает промежуточными навыками, если выполняется один из критериев.

Результаты опроса 24 программистов (множество P) с высшим образованием, окончивших белорусские университеты и работающие в программистских фирмах, представлены на рис. 1, где строки соответствуют программистам, столбцы – технологиям из таблицы. На пересечении строки p и столбца t стоит прямоугольник, высота которого указывает на один из пяти уровней 0, 0.25, 0.5, 0.75 и 1 владения программистом p технологией t. Отсутствие прямоугольника означает нулевой уровень. Строки с большей суммарной площадью прямоугольников показывают более квалифицированных программистов. Столбцы с боль-

шей площадью прямоугольников указывают на более востребованные и значимые технологии.

Квалификация программиста

Квалификация программиста $p \in P$ с учетом уровня знания/владения технологиями из множества T оценивается по отношению к максимальному уровню знания/владения выражением

$$Qualif(p) = \sum_{t \in T} rank(t) \cdot factor(p,t) \Big/ MaxQualif \quad (1)$$

где

$$factor(p,t) = \begin{cases} level(p,t), \text{ если } level(p,t) \geq RL_t^p \\ 0, \text{ в противном случае} \end{cases} \quad (2)$$

и

$$MaxQualif = \sum_{t \in T} rank(t) \quad (3)$$

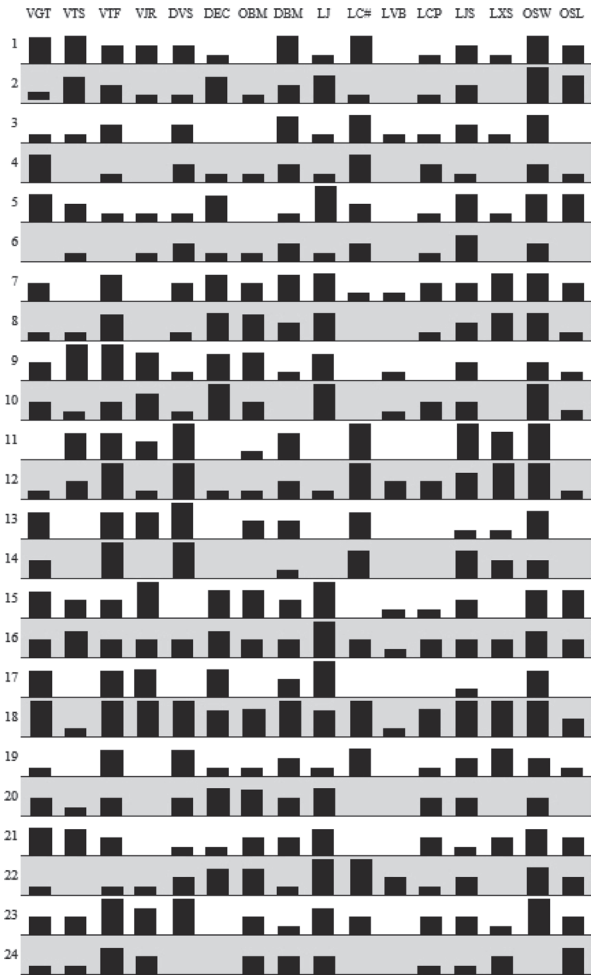


Рис. 1. Уровень 24 программистов владения 16 технологиями

Значение $rank(t)$ из диапазона [0, 1] берется из таблицы. Значение $level(p, t)$ из диапазона [0, 1] определяется результатами опроса, представленными на рис. 1. Пороговое значение RL_t^p уровня $level(p, t)$ позволяет снизить шансы допуска к работе над проектом программистов, обладающих недостаточно высоким уровнем квалификации. Значение выбирается из диапазона [0, 1]. Если $RL_t^p \cong 0$, то к проекту могут подключаться начинающие программисты или программисты, владеющие частью технологий. Если $RL_t^p \cong 1$, то проект ориентирован на разработку экспертами. Как следствие, значение $Qualif(p)$ находится в диапазоне [0, 1]. Согласно формуле (1), программисты, владеющие предпочтительно технологиями с высоким рейтингом, обладают более высокой квалификацией по сравнению с программистами, владеющими предпочтительно технологиями с низким рейтингом.

Рис. 2 показывает квалификацию $Qualif(p)$ каждого из 24 программистов в отношении значимости/владения всеми 16 технологиями с учетом их рейтинга. Значение квалификации находится в диапазоне [0, 1] и является относительным к максимальному значению $MaxQualif = 9{,}5$. Лидером в квалификации является программист с номером 18, за ним идут программисты с номерами 12 и 16.

Квалификация группы программистов

Пусть все множество P программистов разбито на k групп с образованием множества $G = \{g_1, \ldots, g_k\}$. Программисты группы g образуют множество P_g. Средняя квалификация группы g, включающая n_g программистов, определяется как среднее значение квалификаций $Qualif(p)$ по всем программистам $p \in P_g$:

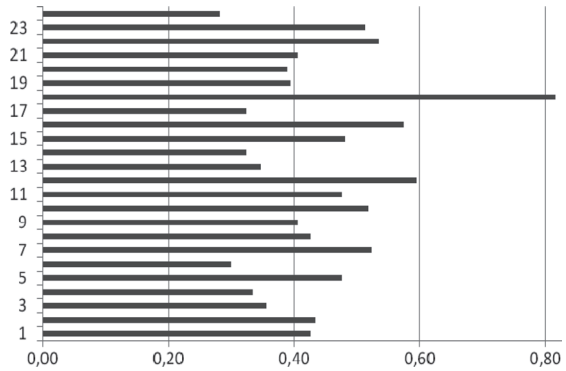


Рис. 2. Квалификация каждого из 24 программистов, усредненная по 16 технологиям

$$Qualif^{avg}(g) = \sum_{p \in P_g} Qualif(p) \Big/ n_g \qquad (4)$$

Помимо средней квалификации $Qualif^{avg}(g)$, важнейшим параметром, характеризующим группу g, является квалификация $Qualif^{best}(g)$ по лучшим представителям, которая определяется формулами (5) и (6).

$$Qualif^{best}(g) = \begin{cases} 0, \text{ если } \exists t, oblgt(t) \text{ и } mxlevel(g,t) < RL_t^g \\ \dfrac{\sum_{t \in T} rank(t) \cdot mxlevel(g,t)}{MaxQualif}, \text{ иначе} \end{cases} \qquad (5)$$

$$mxlevel(g,t) = \max_{p \in P_g} \left(level(p,t) \right) \qquad (6)$$

Формула (5) использует следующие величины: $oblgt(t)$ – предикат, принимающий значение истина, если технология является обязательной для группы (таблица); $mxlevel(g, t)$ – уровень лучшего представителя группы g по технологии t; RL_t^g – пороговое значение уровня лучшего представителя по технологии t.

Согласно формуле (5), квалификация по лучшим представителям $Qualif^{best}(g)$ получает нулевое значение, если существует хотя бы одна обязательная для группы технология t, для которой $oblgt(t)$ истинно, а уровень $mxlevel(g, t)$ лучшего представителя группы g меньше порогового значения RL_t^g. Это объясняется тем, что группа не способна выполнять проекты без высококвалифицированных специалистов по ключевым технологиям.

Взвешенная квалификация $Qualif^{w}(g)$ группы g оценивается в виде суммы квалификации $Qualif^{best}(g)$ по лучшим представителям с весом λ и средней квалификации $Qualif^{avg}(g)$ с весом $1 - \lambda$:

$$Qualif^{w}(g) = \lambda \cdot Qualif^{best}(g) + (1 - \lambda) Qualif^{avg}(g). \qquad (7)$$

Взвешенная квалификация при $0 \le \lambda \le 1$ может принимать любое значение в диапазоне [0, 1]. Чем больше значение λ, тем больший вес придается квалификации по лучшим представителям, и наоборот, чем меньше значение λ, те больший вес придается средней квалификации программистов группы. Средняя квалификация отражает состояние дел на текущий момент. Квалификации по лучшим представителям показывает возможности роста членов команды, ориентирующихся и подтягивающихся к экспертам по технологиям, которые входят в состав группы и являются образцовым примером.

Очевидно, что группы с низкой квалификацией не могут быть признаны работоспособными, а участие таких групп в работах над проектом является необоснованным или, по крайней мере, спорным. Исключение появления таких групп формализуется понятием пороговой взвешенной квалификации:

$$Qualif(g) = \begin{cases} Qualif^{w}(g), \text{ если } Qualif^{w}(g) \ge RQ^g \\ 0, \text{ в противном случае.} \end{cases} \qquad (8)$$

Пороговое значение квалификации RQ^g рекомендуется предпочтительно выбирать из диапазона от 0.5 до 1.0 в зависимости от требований к проекту и технологиям его разработки, а также от ожидаемого качества будущих результатов проектирования. В дальнейшем под квалификацией группы программистов будем понимать пороговую взвешенную квалификацию.

Группа g называется избыточной по квалификации, если в ней найдется программист $p \in g$ такой, что $Qualif(g \setminus \{p\}) \ge Qualif(g)$. Другими словами, квалификация группы g после вывода из нее программиста p оказывается не ниже квалификации до вывода программиста. Такое может произойти при выполнении двух условий:

1. Программист p не является единственным лучшим представителем группы g ни по одной технологии $t \in T$.

2. Квалификация $Qualif(p)$ программиста p ниже средней квалификации $Qualif^{avg}(g)$ группы g.

Если множество программистов разбито на множество G групп, то общая квалификация всех групп оценивается в виде суммы пороговой взвешенной квалификации по всем группам:

$$Qualification(G) = \sum_{g \in G} Qualif(g) \qquad (9)$$

Общая квалификация групп $Qualification(G)$ принимает значение в диапазоне от $k \cdot RQ^g$ до k, где k – число групп.

Задача оптимизации размера и состава программистских групп

Определим оптимизируемый параметр, критерий оптимизации и допустимое множество

задачи оптимизации. Оптимизируемым параметром является суммарная квалификация всех групп *Qualification*(*G*). Целевую функцию запишем в виде:

$$\max_{G\in\Omega} \; Qualification(G) \qquad (10)$$

где Ω – множество всех возможных разбиений *G* программистов из множества *P* на группы.

Сформулируем допустимое множество через систему ограничений, описываемых в виде требования к программистам и группам программистов по владению технологиями и инструментами программирования.

Требование 1. Оно относится к минимально-пороговому уровню RL_t^p владения технологией *t* каждым программистом *p* из множества *P*. Требование к минимальному уровню по всем технологиям представим вектором $RL^p = \{RL_1^p, \ldots, RL_m^p\}$. Реальный уровень L_t^p определяется выражением:

$$L_t^p = rank(t)\cdot level(p,t) \qquad (11)$$

Требование 2. Оно относится к минимально-пороговому уровню RL_t^g владения технологией *t* лучшим представителем группы программистов $g \in G$. Для всех технологий минимально-пороговый уровень представляется вектором $RL^g = \{RL_1^g, \ldots, RL_m^g\}$. Реальный уровень L_t^g владения лучшим представителем группы *g* технологией *t* определяется выражением:

$$L_t^g = rank(t)\cdot \max_{p\in P_g}\left(level(p,t)\right) \qquad (11)$$

Требование 3. Оно относится к минимально-пороговой взвешенной квалификации RQ^g каждой группы программистов $g \in G$. Требуемая минимальная квалификация одинакова для всех групп. Реальная взвешенная квалификация $Qualif^w(g)$ группы оценивается формулой (7).

Решение задачи оптимизации генетическим алгоритмом

Генетический алгоритм (GA) реализует случайный процесс эволюции популяции хромосом с целью нахождения наилучшего по совокупной квалификации разбиения программистов на группы. Хромосома строится из генов, соответствующих программистам. Значение гена есть номер группы, в которую включается программист. Фитнес функцией является общая квалификация *Qualification*(*G*). Генетическая операция скрещивания рекомбинирует участки двух хромосом и переводит программистов из одних групп в другие группы в хромосомах-потомках. Ее выполнение может привести к исчезновению групп в хромосомах-потомках. Нормализация хромосом выполняется перенумерацией групп. Операция мутации переводит случайным образом одного или больше программистов в другие группы. Операция селекции выбирает родителей по правилу рулетки и выбирает хромосомы для замены худших родителей в популяции. Хромосома с наибольшим значением функции полезности является решением оптимизационной задачи.

Результаты вычислительных экспериментов

Для проведения вычислительных экспериментов использовано разработанная программа, реализующая генетический алгоритм. Установлены следующие требования: ограничение снизу на квалификацию RL^p = {0.1, 0, 0.1, 0, 0.3, 0.25, 0, 0.15, 0.6, 0, 0, 0.25, 0, 0.2, 0.4, 0.2} программиста по каждой из 16 технологий, перечисленных в таблице; ограничение снизу на квалификацию RL^g = {0.2, 0, 0.2, 0, 0.4, 0.3, 0, 0.3, 0.75, 0.4, 0, 0.5, 0, 0.3, 0.5, 0.25} группы программистов по каждой из 16 технологий; ограничение снизу на пороговую взвешенную квалификацию $RQ^g = 0.5$ группы программистов по всем технологиям; вес $\lambda = 0.7$ квалификации группы по лучшим представителям во взвешенной квалификации группы.

Результаты экспериментов представлены на рис. 3–7. Рис. 3–5 показывают динамику работы генетического алгоритма в процессе эволюции популяции хромосом. Суммарная по всем группам пороговая взвешенная квалификации выросла (рис. 3) с 3.5 до 5.04 на протяжении 25 поколений. Рост составил около 30%. За это время число групп, удовлетворяющих всем выдвинутым требованиям по квалификации, увеличилось с 5 до 8 (рис. 4, сплошная линия), а число включенных в них программистов возросло с 15 до 23 (рис. 5, сплошная линия). Число групп, не удовлетворяющих требованиям, колебалось от 1 до 2 (рис. 4, пунктирная линия), а число попавших в них программистов колебалось от 9 до 1 (рис. 5, пунктирная линия). В итоге, эволюционный процесс сопровождался устойчивым ростом суммарной

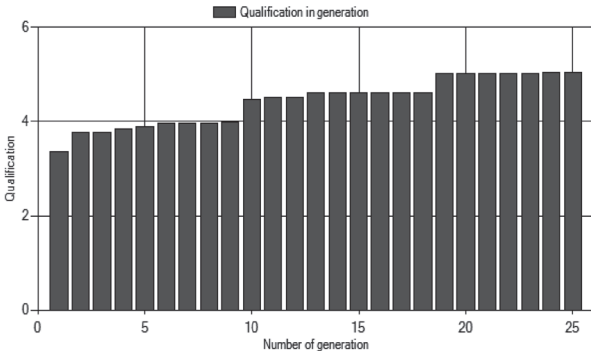


Рис. 3. Зависимость суммарной по всем группам пороговой взвешенной квалификации *Qualification*(*G*) от номера поколения в GA

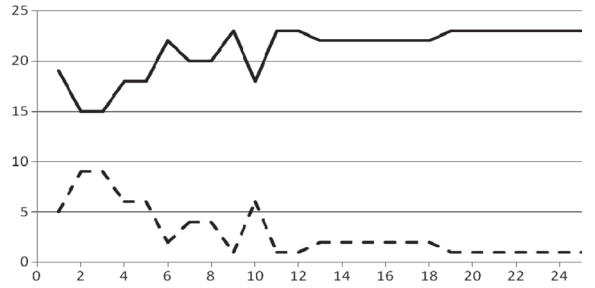


Рис. 5. Число программистов в группах, удовлетворяющих требованиям (сплошная), и в резерве (пунктирная) в зависимости от номера поколения в GA

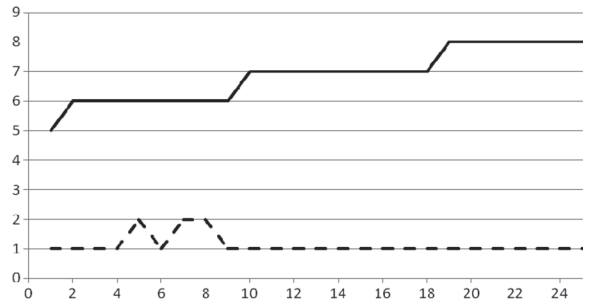


Рис. 4. Число групп, удовлетворяющих требованиям (сплошная) и неудовлетворяющих требованиям (пунктирная), в зависимости от номера поколения в GA

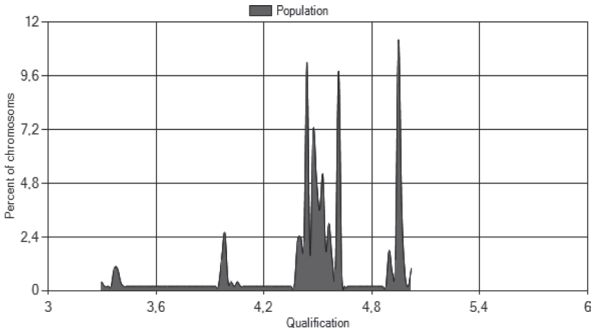


Рис. 6. Доля в % числа хромосом с лучшим значением функции полезности в популяции в зависимости от номера поколения в GA

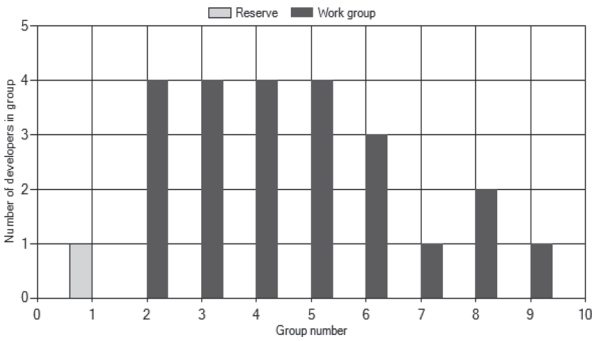


Рис. 7. Распределение программистов по группам в оптимальном решении (группа 1 – резерв)

пороговой взвешенной квалификации групп, представленных лучшими хромосомами, доля которых от размера популяции показана на рис. 6.

Лучшее распределение программистов по группам представлено на рис. 7. Всего сформировано 8 групп с суммарным уровнем квалификации 5.04 и средним уровнем 0.63, из которых 4 группы включают по 4 программиста, одна – 3 программиста, одна – 2 программиста, и две группы включают по 1 программисту. Неиспользованным (в резерве) оказался только один программист.

Заключение

Предложен метод оценки квалификации групп разработчиков по уровню знания и владения технологиями и инструментами программирования. Разработан генетический алгоритм оптимизации размера, состава и количества групп, максимизирующий суммарную квалификацию групп и минимизирующий число незадействованных в них программистов. Дальнейшие исследования будут направлены на интеграцию факторов квалификации и производительности групп программистов.

Литература

1. **Joshi, S.** Agile Development - Working with Agile in a Distributed Team Environment / S. Joshi // MSDN Magazine, 2012, Vol.27, No.1, pp.1–6.

2. **Прихожий, А. А.** Конспект лекций по дисциплине «Моделирование и оптимальное проектирование технических систем» / А.А. Прихожий // БНТУ, кафедра ПОВТиАС, 2013, с. 58–69.

3. **Barricelli, N. A.** Symbio genetic evolution processes realized by artificial methods / N.A. Barricelli // Methodos, 1957, pp. 143–182.

4. **Müller, J. P., Rao, A. S., Singh, M. P.** A-Teams: An Agent Architecture for Optimization and Decision-Support, Proceedings 5th International Workshop, ATAL'98 Paris, France, July 4–7, 1998, pp. 261-276.

5. **Прихожий, А. А.** Эволюционный метод оптимизации состава групп разработчиков с целью сокращения затрат и времени на выполнение проекта / А.А. Прихожий, А.М. Ждановский // Материалы научно-технической конференции «Информационные технологии в технических и социально-экономических системах», Минск, РИВШ, 2016. – С. 16-20.

6. **Red Monk** [Электронный ресурс] / сайт аналитической компании Red Monk. – Режим доступа: http://redmonk.com/sogrady/2016/07/20/language-rankings-6-16/. – Дата доступа: 26.02.2017.

7. **Cass, S.** The 2016 Top Programming Languages [Электронный ресурс] / IEEE Spectrum, 2016. – Режим доступа: http://spectrum.ieee.org/ computing/software/the-2016-top-programming-languages. – Дата доступа: 26.02.2017.

References

1. **Joshi, S.** Agile Development - Working with Agile in a Distributed Team Environment / S. Joshi // MSDN Magazine, 2012, Vol.27, No.1, pp.1–6.

2. **Prihozhy, A.** Lecture notes on "Modeling and Optimization for Engineering Systems Design" / A. Prihozhy // BNTU, Software for Computers and Automated Systems Dpt., 2013, pp. 58–69.

3. **Barricelli, N. A.** Symbio genetic evolution processes realized by artificial methods / N.A. Barricelli // Methodos, 1957, pp. 143–182.

4. **Müller, J. P., Rao, A. S., Singh, M. P.** A-Teams: An Agent Architecture for Optimization and Decision-Support, Proceedings 5th International Workshop, ATAL'98 Paris, France, July 4–7, 1998, pp. 261–276.

5. **Prihozhy, A.** Evolutionary Method of Software Teams Optimization for Reducing Time and Resources of Project Execution / A. Prihozhy, A. Zhdanouski // Proc. Conf. "Information Technologies in Engineering and Business", Minsk, RIHS, 2016, pp.16–20.

6. **Red Monk** [Электронный ресурс] / сайт аналитической компании Red Monk. – Режим доступа: http://redmonk.com/sogrady/2016/07/20/language-rankings-6-16/. – Дата доступа: 26.02.2017.

7. **Cass, S.** The 2016 Top Programming Languages [Электронный ресурс] / IEEE Spectrum, 2016. – Режим доступа: http://spectrum.ieee.org/computing/software/the-2016-top-programming-languages. – Дата доступа: 26.02.2017.

Поступила	*После доработки*	*Принята к печати*
20.03.2018	*12.04.2018*	*01.06.2018*

Prihozhy A., Zhdanouski A.

METHOD OF QUALIFICATION ESTIMATION AND OPTIMIZATION OF PROFESSIONAL TEAMS OF PROGRAMMERS

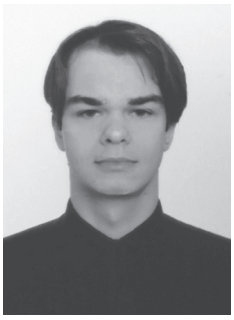
prihozhy@yahoo.com

The problem of building and optimizing the teams of programmers taking into account the qualification and the level of skills in programming technologies and tools is considered. Known technological environments for the management of teamwork, such as Agile, formulate only general requirements and principles for building the teams and the distribution of work between them. A method for formalizing and evaluating the qualification of individual programmers and entire groups of pro-grammers has been proposed. The input data are attributes of the most popular technologies and programming tools, includ-ing technology rating, as well as the results of a survey of programmers on their level of skills. The qualification of a group of programmers is evaluated taking into account the requirements for a particular project, which integrates three components: the average qualification of programmers included in the group; the qualification of the group with respect to the best repre-sentatives for each of the technologies; threshold values of the levels of programmer qualification and group qualification for each of the technologies, as well as threshold values of the integrated qualification, reflecting the specifics of the given project. The contribution of each component is determined by appropriate weights. The proposed method is a basis for a genetic algo-rithm that performs the search for the number, size and staff of groups of programmers which yield a maximum of total quali-fication. Software has been developed and computer experiments have been carried out on a set of programmers who graduat-ed from Belarusian universities. The obtained results demonstrate the real ability of the system to find the number, size and staff of groups of programmers, which increase the overall qualification of groups by 30% while minimizing the number of unemployed developers. The results prove the practical importance of the method and software in the field of technologies and tools for the management of professional teams of programmers.

Keywords: *Programmer, technology, tool, qualification, skills, programmer team, team staff, optimization.*

Прихожий Анатолий Алексеевич – профессор кафедры программного обеспечения вычислительной техники и автоматизированных систем БНТУ, доктор технических наук (1999), профессор (2001). Научные интересы в области языков программирования и описания цифровой аппратауры, распараллелтвающих компиляторов, инструментальных средств проектирования программных и аппаратных систем на логическом, поведенческом и системном уровнях. Имеет более 300 научных публикаций в Восточной и Западной Европе, США и Канаде.

Anatoly Prihozhy is a full professor at the Computer and system software department of Belarusian national technical university, doctor of science (1999) and professor (2001). His research interests include programming and hardware description languages, parallelizing compilers, and computer aided design tools for software and hardware at logic, high and system levels. He has over 300 publications in Eastern and Western Europe, USA and Canada.



Ждановский Арсений Матвеевич – аспирант кафедры «Программное обеспечение вычислительной техники и автоматизированных систем» БНТУ, инженер программист компании «EPAM Systems», научные интересы в области языков и технологий программирования и методов оптимизации.

Zhdanouski Arseni is a postgraduate of the Computer and system software department of Belarusian national technical university, and a software engineer at EPAM Systems. His research interests include programming languages and techlogies and methods of optimization**.**

УПРАВЛЕНИЕ ТЕХНИЧЕСКИМИ ОБЪЕКТАМИ

MANAGEMEMENT OF TECHNICAL OBJECTS

УДК 629.113.073

В. Г. МИХАЙЛОВ

АНАЛИЗ МЕТОДОВ ПОЛУЧЕНИЯ ПРОДОЛЬНЫХ ПРОФИЛЕЙ ДОРОГ

Проведен анализ методов получения продольных профилей дороги важных для проведения моделирования движения автомобиля на основе геодезических карт, замеров дорог с помощью геодезического оборудования, использования мобильных лаборатории, радарного сканирования земли, считывания данных с электронного блока управления автомобиля и дана оценка их точности. Отмечено, что перечисленные способы трудоемки и затратны и не всегда обеспечивают необходимой точности. Так в случае использования общедоступных данных радарного сканирования земли со спутников погрешность может достигать 30–50%. Хотя в будущем по мере совершенствования точности зондирования и доступности информации данный способ представляется наиболее перспективным.

Предложен метод регистрации продольных профилей/уклонов больших участков дорог в процессе движения автомобиля на основе микроконтроллера Arduino Due, датчиков ускорений и углов наклона MPU-6050 и записи данных на SD-карту, рассмотрено применение комбинированной обработки информации на основе разработанных программ на языке С в самом микроконтроллере и в модуле S-Function Builder в пакете Matlab/Simulink.

С помощью предложенных методов проведена регистрация профиля дороги сложного характера протяженностью 10 км. Для сравнения построен профиль этой же дороги методом использования карты радарного сканирования земли и проведено сравнение их данных.

Выявлено хорошее совпадение характера изменения профиля дороги, средне-квадратических и максимальных значений высот профиля дороги, полученных по предложенным методам (расхождение 7–20%).

Ключевые слова: *Автомобиль, продольный уклон дороги, моделирование уклонов дороги и внешнего возмущения, микроконтроллер Arduino, Matlab/Simulink.*

Введение

В настоящее время при проектировании автомобилей все чаще используют методы виртуального моделирования на основе пакетов MS-Adams и MatLab/SimuLink с применением численных методов на основе известного нелинейного дифференциального уравнении второго порядка [1–7]. Это позволяет более тщательнее проработать конструкцию еще на стадии проектирования.

Большинство расчетов, выполняемых на этих пакетах, сводится к простейшему определению максимальной скорости, времени и пути разгона. Сейчас наибольший интерес представляет моделирование движения автомобиля с учетом реальных условий, для которых необходимо задавать конкретные реализации профилей/уклонов дороги [3, 5, 6].

Это обусловлено широким внедрением автоматических и роботизированных трансмиссий, для которых все более актуальным становится вопрос управления ими с помощью микропроцессорных систем и решения задачи синтеза, отработки алгоритмов управления двигателем и трансмиссией. Благодаря этому можно достигнуть экономии топлива, уменьшить динамические нагрузки на трансмиссию, что положительно скажется на ее долговечности. Сейчас параметр наклона дороги начинают учитывать в системах управлении такими трансмиссиями (пример, АКПП Тойота).

Необходимые для решения задач моделирования тяговой динамики автомобиля данные по продольным профилям/уклонам дорог можно получить следующими способами:

– на основе геодезических карт дорог и их высот занести информацию в массив данных и использовать ее при расчетах. Данный способ является наиболее трудоемким, т. к. придется обработать большие массивы информа-

ции и занести ее в базу данных. Сложность еще заключается в том, что упомянутые выше пакеты не рассчитаны на работу с существующими базами данных. Обычно используется массив Matlab (до 20 значений) либо MS Excel при работе с Matlab, ограниченный по объему (1024 значений), шаг задается 200–300 м. Кроме того проектные институты и эксплуатационные дорожные организации, располагающие такой документацией не охотно предоставляют ее или отказывают из соображений мер безопасности коммуникаций;

– провести собственные замеры дорог с помощью геодезического оборудования: теодолитов, мерной рейки, что очень трудоемко и небезопасно с условиях интенсивного транспортного движения;

– использовать дорогостоящие мобильные лаборатории, позволяющие фиксировать наклоны дорог в процессе движения с помощью гироскопов с записью на компьютерную технику с последующей обработкой. Возможен вариант применения «качающегося маятника» [3, 7], однако он в последнее время не используется и нет данных его использования в этом качестве;

– использовать данные космического радарного сканирования земли [8, 5], имеющиеся в интернете. К сожалению, точность общедоступных данных по высоте составляет 15–20 м. Хотя сейчас имеются спутники, обеспечивающие точность по высоте 5–10 м, но их данные носят закрытый характер. Недостатком метода является то, что могут быть взяты данные по пятну сканирования, приходящиеся на кюветы, насыпи, откосы, обочины, из-за невысокой точности определения координат дорожного полотна маршрута движения и точек шагов замеров. Все это в совокупности может привести к погрешности 30–50%. Тем не менее данный способ в будущем представляется наиболее перспективным и он сейчас широко применяется в ОИМ НАН РБ, Минском автозаводе и Нижегородском политехническом университете при расчетах тяговой динамики в дорожных условиях [5, 6].

В работах [9–11] предложен метод получения уклонов дорог основанный на регистрации параметров CAN шины электронного блока управления силовым агрегатом движущегося автомобиля и положения автомобиля на трассе с помощью датчика GPS. Полученные данные (скорость, крутящий момент, текущая передача КПП, координаты точек сканирования GPS) записывались на laptop. Регистрация параметров производилась с шагом 12,5 м. Длина записанного участка составляла 15 км. Число точек сканирования 1200. Затем на основе обработки этих данных рассчитывался угол наклона дороги, используя тяговый баланс сил автомобиля и значение его массы без учета аэродинамического фактора. В дальнейшем полученный массив данных используется в задачах тяговой динамики автомобилей фирмы Volvo.

Недостатком метода является необходимость использования laptop или ноутбука, конверторов сигнала с CAN шины на USB, разработка специального программного обеспечения считывания данных, фильтрации и обработки сигнала, оцениваемое в 3–5 тысяч долларов и более, невысокая скорость передачи данных через конвертор OBD-USB подключаемый к компьютеру (обычно 9600 бит/с). Хотя скорость передачи данных внутри CAN шины 250000 бит/с и более. Кроме того трудно оценить получаемую точность предложенного метода, так как не учитывается аэродинамический фактор и колебания автомобиля, доля которых в зависимости от скорости может достигать 30–50%.

Рассмотренные выше способы трудоемки и затратны. Учитывая, что для моделирования требуются записи больших участков дорог, необходим иной и более дешевый способ регистрации параметров дорог.

В настоящее время появились дешевые (35 долларов США) микроконтроллеры (МК) Arduino и датчики к ним (MPU-6050), позволяющие провести замеры продольных уклонов и профиля дорог в процессе движения автомобиля. Встроенные преобразователи сигналов с датчиков MPU-6050, позволяют одновременно регистрировать ускорения и наклоны в 3-х осях с более высокой частотой сканирования (при разгоне МК до 300 Гц), в то время как у датчика наклона (Bosh MM5.10) мотоцикла DUCATI KTM 1190, подключаемого к CAN-шине – 15 Гц.

Поэтому разработка методов регистрации продольных профилей дорог с помощью модулей Arduino, получения на их основе данных

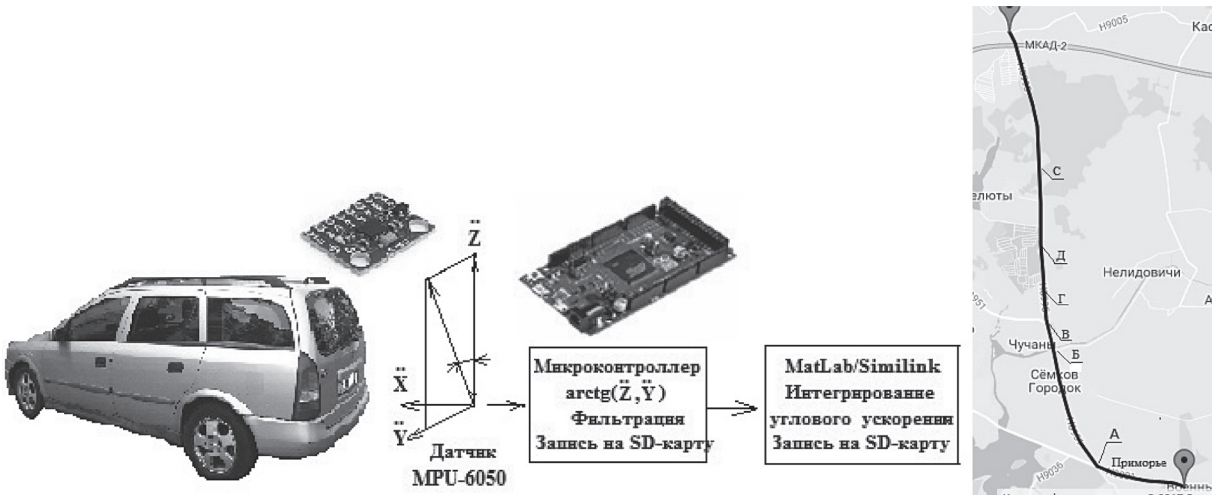


Рис. 1. Схема записи и обработки параметров дороги и маршрут движения

и сравнение с методом на основе карты радарного сканирования земли представляется актуальной задачей.

Методика измерений наклона дороги

Для получения данных по продольному профилю дорог (рис. 1) использовалась следующая аппаратура: микроконтроллер Arduino Due, два датчика MPU-6050 (погрешность 0,2%).

Методика измерений заключалась в замерах и регистрации ускорений и углов наклона на кузове и над задней осью по двум осям X и Y (рис. 1), получении **arctg** углового наклона, фильтрации сигналов с помощью фильтра Калмана или экспонентной фильтрации и записи их на SD-карту [12]. Также проверена возможность получения данных по углам наклона на основе интегрирования ускорений неподрессоренной массы автомобиля (на колесе) и последующего дифференцирования. Принято допущение, что перемещение оси колеса соответствует высоте профиля дороги. Запись параметров производилась при постоянной скорости движения 72 км/ч (20 м/с) в раннее утреннее время, когда менее загружены трассы. Выбор скоростей движения определялся исходя из аналогичных соображений метода IRI (80 км/ч) по оценке ровности дорог – несоздания помех движению. За счет подбора параметров и настройки программного обеспечения Arduino Due достигнута высокая частота опроса при использовании двух датчиков MPU-6050–154 Гц (против стандартных 20 Гц на одном датчике), соответствующая шагу 0,125 м.

Используя текущие значения ускорений и данных гироскопа по указанным осям с помощью функции arctg(α) = $X\Big/\sqrt{x^2+z^2}$ в микроконтроллере определялось значение ускорения углового поворота кузова автомобиля, которое корректировалось на основе данных гироскопа. Затем путем его фильтрации (сглаживания) в МК и пакете Mathlab/Simulink определялся угол наклона кузова, который принимался за угол наклона дороги. Это является одним из способов получения наклона профиля дороги, необходимого для моделирования тяговой динамики.

Для устранения шумов и дрейфа сигнала датчиков MPU-6050 использован метод экспонентного сглаживания [12] исходя из информации на форумах Arduino, что разница в точности в сравнении с методом Калмана, применяемых в системах радиолокации, не столь значительна (до 2%). Использованный метод экспонентного сглаживания оказался на 28% быстрее (обеспечивал частоту регистрации 154 Гц), чем метод Калмана (120 Гц). Для экспонентного сглаживания использовалось интегрирование, которое производилось:

– непосредственно на микроконтроллере с помощью численного метода Эйлера, как наиболее простого и менее затратного по ресурсам;

– и в пакете Mathlab/Simulink.

Фрагмент реализации экспонентного сглаживания в микроконтроллере приведен ниже.

```
yglx1_t = (atan2(vax1, vaz1))*57,3;
          // 57,3 = rad2degree
```

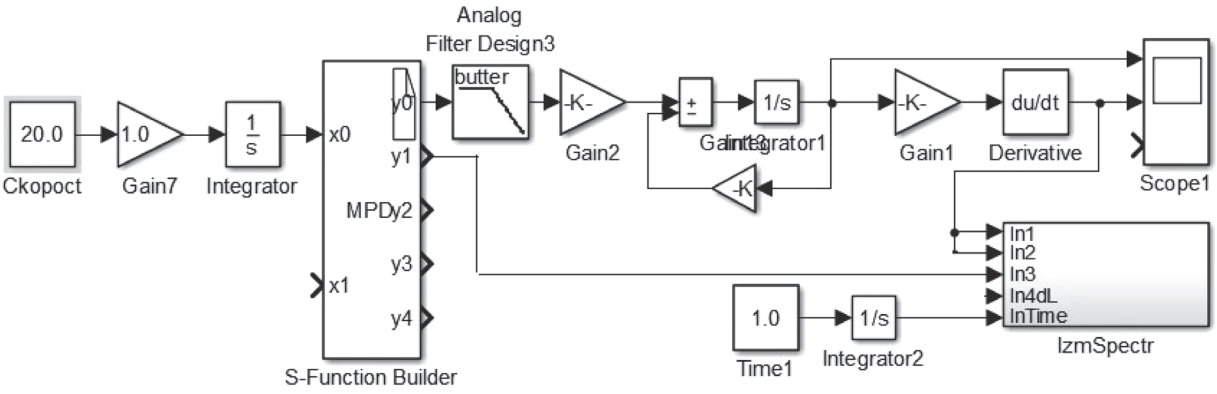


Рис. 2. Блок-схема реализации обработки высоты и углов наклона дороги

$$yglx1 = Filter_gain*yglx1_g + 0{,}05*yglx1_t;$$
$$// \ 0{,}05 = (1\text{-}Filter_gain)$$

где yglx1_g – угол наклона, получаемый с гироскопа, vax1, vaz1 – величина ускорений в плоскостях *X*, *Z*, yglx1_t – значение экспоненциального сглаживания угла наклона, yglx1 – полученное значение угла наклона при экспоненциальном сглаживании, Filter_gain = 0,05 – коэффициент фильтра сглаживания.

Общий объем разработанной программы для микроконтроллера, включая программную автобалансировку нуля датчиков (пяти параметров), исключение зависания протокола $i2C^2$, составил 576 строк текста. Регистрация данных с датчика производилась на SD-карту в виде структуры бинарного файла. Далее с помощью программы на языке С в блоке модуля S-Function Builder они заносились в электронный массив данных MatLab/SimuLink и использовались в этом пакете. Блок-схема получения профиля дороги приведена на рис. 2.

С помощью константы «Скорость» и интегратора «Integrator» задается скорость движения (считывания массива данных ускорений или углов уклона). С помощью блоков SrArif и SrKvadr производился расчет среднеквадратических и максимальных значений высот и углов наклонов дороги.

Проведение и результаты замеров профиля дорог

Для проведения замеров выбран участок маршрута (рис. 1) под Минском: Военный городок – Приморье – Семков городок – Чучаны – МКАД2 длиной 10 км. Данный маршрут характерен значительными перепадами высот, разным качеством покрытия, проездом через 3 населенных пункта, наличием двух поворотов. Он наиболее подходит для моделирования тяговой динамики специальных машин, включая штабные. Полученные замеры 10-ти километрового участка дороги сравнивались с данными на основе карты радарного сканирования с помощью программы на сайте [8] с шагом замеров 100 м. Полученные по карте значения 100 точек высот занесены в массив программы S-Function Builder и обработаны с помощью MatLab/Simulink и представлены на рис. 3. И здесь же представлены данные полученные интегрированием ускорений неподрессоренной массы.

Дополнительно проведена оценка точности предложенных методов и использованных для этого устройств, показавшая на стенде в статике при угле наклона до 10° (по линейности характеристики) погрешность не более 1–2%, а по результатам преодоления одиночного подъема дороги (6%) погрешность 3–4%.

Как видно из рис. 3 наблюдается одинаковый характер изменения продольного профиля дороги и близкое совпадение высот (с расхождением 8–20%) за исключением участков точек Г, Д, С, имеющих на карте постоянство высоты профиля. Провал характеристики на этих участках обуславливается экспонентным сглаживанием, вызывающим разряд значений интеграторов при отсутствии изменений (при ровном участке). При появлении дальнейшего наклона происходит нарастание его величины.

Результаты сравнения методов получения продольного профиля дорог, включая влияние коэффициентов сглаживания, приведены в таблице. Скорость изменения продольного профиля по карте радарного сканирования получена путем дифференцирования *dh*/*dt*. При сравнении необходимо учитывать фактор вли-

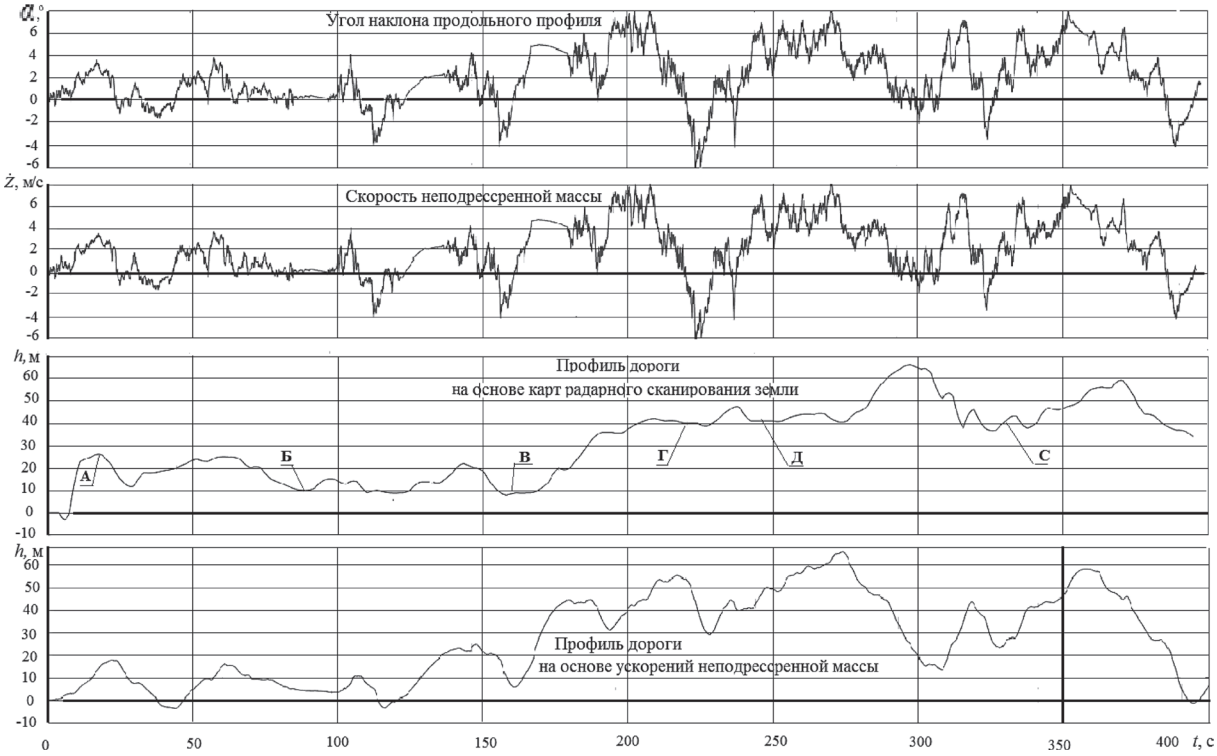


Рис. 3. Сравнение продольных профилей на основе радарного сканирования земли и интегрирования ускорений и углов дороги

яния воздействия микропрофиля дороги, особенно на скорость неровности.

Как видно из таблицы при использовании метода замеров на основе ускорений неподрессоренной массы при $K = 0{,}1$ получается хорошее совпадение по максимальным и среднеквадратичным значениям высот продольных профилей. В то же время по скорости/углу наклона (среднеквадратичным значениям) имеет место расхождение до 40–50% при одновременном хорошем совпадении по максимальным значениям скоростей. Последнее можно

Результаты сравнения методов получения продольного профиля дорог

Метод получения	Высота h, м		Скорость по $\dot{Z}$, м/с		Скорость по dh/dt, м/с	
	s	$\max_h$	s	$\max_v$	s	$\max_v$
По карте	35,4	66			1,1	8,04
при K сглаживания	На основе ускорений неподрессоренной массы					
0,11	24,3	52,4	3,15	8,4	1,65	7,3
0,105	26,5	56,8	3,25	8,65	1,69	7,5
0,1	28,9	61,5	3,4	8,9	1,74	7,67
0,1, фильтр $f = 2$ рад/с	28,9	61,5	3,37	8,36	1,68	5,77
0,1, фильтр $f = 3$ рад/с	28,9	61,5	3,37	8,36	1,703	6,16
На основе ускорений подрессоренной массы при $k = 0{,}1$						
	9,6	34,7	1,1	4,5	2,36	2,56
По углу наклона подрессоренной массы						
Фильтр $f = 1$ рад/с			2,07	5,5		
Фильтр $f = 2$ рад/с			2,46	8,96		
Фильтр $f = 3$ рад/с			2,72	11,2		
Фильтр $f = 5$ рад/с			2,8	14,0		
Фильтр $f = 150$ рад/с			3,8	14,0		

П р и м е ч а н и е. Значение скорости изменения профиля является значением угла наклона в градусах.

объяснить воздействием микронеровностей дороги, вызывающих увеличение ее скорости, отрывами колес от неровностей дороги, о чем свидетельствуют значительные отрицательные пиковые значения ускорений, превышающих 9,81 м/с^2.

Дополнительно проведена оценка возможности использования угла наклона дороги на основе значений скорости перемещения неподрессоренной массы учитывая, что производная функции в точке равна тангенсу угла наклона касательной, проведенной в точке и при малых значениях углов имеет место линейная зависимость tg от угла. Скорость изменения высоты профиля дороги есть ничто иное как тангенс изменения высоты дороги и его угол, то есть $\mathrm{tg}(v) = \alpha$. Отсюда продольный угол наклона дороги $\alpha = \mathrm{arctg}(v)$, где $\upsilon = \dot{q}$ – скорость изменения высоты профиля/неровности. Из графика видно, что значения угла наклона и скорости получаются одинаковыми, что позволяет использовать физическое значения скорости вместо угла наклона.

Как показало проведенное исследование использование метода замеров на основе ускорений позволяет получать продольный профиль дороги, который путем некоторых дополнительных математических преобразований (учета характеристик шины и ускорений подрессоренной массы) одновременно является и микропрофилем дороги. Это позволяет в дальнейшем решать задачи нагруженности автомобиля и оценки его долговечности.

Полученные данные показали, что непосредственно ускорения подрессоренной массы нельзя использовать для определения высот продольного профиля, так как осциллограмма по профилю получается хорошо центрированной и их значения малы.

Метод по углу наклона подрессоренной массы свидетельствует о необходимости использования фильтра низких частот с частотой среза $f = 2$ рад/с.

При использовании широкой полосы $f =$ 150 рад/с значения получаются большими (в 1,5 раза) чем при $f = 2$ рад/с.

В целом предложенные методы получения по ускорениям неподрессоренной массы и углам наклона вполне могут использоваться в практике моделирования тяговой динамики автомобиля. Их точность находится на уровне методов использования радарного сканирования земли и сканирования данных CAN-шины, применяемого на фирме Volvo.

Наиболее простым и дешевым способом получения продольного профиля дорог является использование данных радарного сканирования земли. Однако данный способ необходимо сочетать с использование S-Function Builder, чтобы можно занести в массив большой объем данных.

Наибольший интерес в перспективе представляет применение метода использование ускорений неподрессоренной массы автомобиля или получения путем математических преобразований объединенного макро и микропрофиля дороги в виде большого единого массива данных. В этот массив можно включить данные о дорожных условиях, что позволило бы решать более широкий круг задач как тяговой динамики, так и нагруженности автомобиля и оценки его долговечности.

Заключение

1. Проведенный анализ методов получения продольных профилей дороги на основе геодезических карт, осуществления замеров дорог с помощью геофизического оборудования использования мобильных лаборатории, радарного сканирования земли, считывания данных с электронного блока автомобиля показал, что они не всегда обеспечивают необходимой точности и трудоемки и затратны. В случае использования общедоступных данных радарного сканирования земли со спутников погрешность может достигать 30–50%. Хотя в будущем по мере совершенствования точности зондирования и доступности данный способ представляется наиболее перспективным для решения задач тяговой динамики автомобиля.

2. Для проведения работ по автоматизации и управления трансмиссий автомобилей на основе микроконтроллеров требуются записи больших участков дорог, для чего необходим иной и более дешевый способ регистрации параметров дорог.

3. Предложен метод регистрации уклонов больших участков дорог в процессе движения автомобиля на основе микроконтроллера Arduino Due, датчика ускорений и углов наклона MPU-6050 и записи данных на SD-карту.

4. Использование предложенного метода замеров на основе ускорений неподрессоренной массы обеспечивает хорошее совпадение по характеру изменения, максимальным и среднеквадратичным значениям высот продольных профилей и могут использоваться в практике моделирования тяговой динамики автомобиля. В его массив можно включить данные о дорожных условиях, что позволило бы решать более широкий круг задач, как тяговой динамики, так и нагруженности автомобиля и оценки его долговечности.

ЛИТЕРАТУРА

1. **Высоцкий, М. С.** Основы проектирования модульных магистральных автопоездов/ М. С. Высоцкий, С. И. Кочетов, С. В. Харитончик / Объединенный институт т машиностроения НАН РБ // Минск: Беларуская навука, 2011, С. 391.

2. **Гришкевич, А. И.** Динамика автомобиля / А. И. Гришкевич, И. С. Цитович. – М.: Машиностроение, 1986. С. 205.

3. **Гришкевич А. И.** Исследование динамики движения армейских автомобилей по дорогам с неровной поверхностью: Дис. докт. тех. наук: 05.05.03 Минск, 1973. – С. 353.

4. **Белоусов, Б. Н.** Прикладная механика наземных тягово-транспортных средств с механтронными системами. Монография. – Под общ. редакцией д.т.н. проф. Б. Н. Белоусова М.: Агроконсальт, 2013–612 с.: 62 ил.

5. **Выгонный, А. Г.** Закон переключения передач, оптимальный по тягово-скоростным и топливо экономическим показателям магистрального автопоезда/ А. Г. Выгонный, О. С. Руктешель, Р. Э. Шейбак // Актуальные вопросы машиностроения 2015, Т. 4, С. 182–188.

6. **Выгонный, А. Г.** Сравнительный анализ многокритериальной и однокритериальной оптимизации параметров двигателя и трансмиссии магистрального автопоезда/ А. Г. Выгонный, М. М. Дечко, А. А. Дюжев, С. В. Харитончик // Механика машин, механизмов и материалов, 2014, № 4. С. 40–46.

7. **Хачатуров А. А.** Динамика системы дорога–шина–автомобиль–водитель / под ред. Хачатурова А. А. . – М.: Машиностроение, 1976. – 535 с.

8. **Карта** для определения высоты местности и профиля высот http://22dx.ru/online/karta-vy-sot/ [Электронный ресурс] / http:// www.vhfdx.ru/karta-vyisot // – Режим доступа: 24.12.2017.

9. **Per** Sahlholm Piecewise Linear Road Grade Estimation /Per Sahlholm, Ather Gattami, Karl Henrik Johansson /Scania CV AB, 2ACCESS Linnaeus Centre Royal Institute of Technology, Swedem,2011. KTH – School of Electrical Engineering SE-100 44 Stockholm, Sweden TRITA-EE 2011:007. P. 16.

10. **Per** Sahlholm Road Grade Estimation for Look-ahead Vehicle Control/Per Sahlholm _ Karl Henrik Johansson __ _ Scania CV AB, SE-151 87 Sodertalje, Sweden /_ Royal Institute of Technology (KTH), SE-100 44, Stockholm. P. 7.

11. **Hong** S Road Grade and Vehicle Parameter Estimation for Longitudinal Control Using GPS/ Hong S. Bae1, Jihan Ryu and J. Christian Gerdes. Road Grade Estimation for Look-ahead Vehicle Control Per Sahlholm _ Karl Henrik Johansson ___ Scania CV AB, SE-151 87 Sodertalje, Sweden, Royal Institute of Technology (KTH), SE-100 44, Stockholm, P. 7.

12. **Михайлов, В. Г.** Считывание, первичная обработка ускорений и углов наклона с MPU-6050 и запись бинарных данных на SD карту Arduino Due [Электронный ресурс]/ https:// rep.bntu.by/handle/data/26742 // – Режим доступа: 24.12.2017.

REFERENCES

1. **Vysotsky, M. S.** Base of designing of modular main lorry convoys / M. S. Vysotsky, S. I. Kochetov, S. V. Haritonchik / Incorporated institute т mechanical engineering of NAN RB // Minsk: Belarus Science, 2011, C. 391.

2. **Grishkevitch A. I.** Dynamics of the car / A. I. Grishkevich, I. S. Tsitovich. – M: Mechanical engineering, 1986. P. 205.

3. **Grishkevitch A. I.** Probe of dynamics of movement of army cars on roads Dis a rough surface: Dis. Doctor. Tech. Sciences: 05.05.03 Minsk, 1973. – P. 353.

4. **Belousov, V. N.** The applied mechanics of land tjagovo-vehicles with механтронными systems. The monography. – under Edition d.t.sci. Prof. B. N. Belousova M: Agrokonsalt, 2013 – P. 612: 62 silt.

5. **Vygonni, A. G.** law of a gear shift, optimum on on tjagovo-speed and fuel to economic indicators of the main lorry convoy / of A. G. Vygonnyj, O. S. Rukteshel, R. E. Shejbak// Pressing questions of mechanical engineering 2015, T. 4, C. 182–188.

6. **Vygonni, A.** The Comparative analysis многокритериальной and однокритериальной optimisation of parametres of the engine and transmission of the main lorry convoy / of A. G. Vygonnj, M. M. Dechko, A. A. Djuzhev, S. V. Haritonchik// Mechanics of cars, gears and materials, 2014, № 4. P. 40–46.

7. **Hachaturov A. A.** Dynamics of system road-tyre-car-driver / under the editorship of Hachaturova A. A. – M: Mechanical engineering, 1976. – P. 535.

8. Card for determination of height of terrain and a profile of heights [the Electronic resource] / <http://www.vhfdx.ru/karta-vyisot> // - The Access mode: 12/24/2017.

9. **Per** Sahlholm Piecewise Linear Road Grade Estimation /Per Sahlholm, Ather Gattami, Karl Henrik Johansson /Scania CV AB, 2ACCESS Linnaeus Centre Royal Institute of Technology, Swedem,2011. KTH – School of Electrical Engineering SE-100 44 Stockholm, Sweden TRITA-EE 2011:007 P. 16.

10. **Per** Sahlholm Road Grade Estimation for Look-ahead Vehicle Control/Per Sahlholm _ Karl Henrik Johansson __ Scania CV AB, SE-151 87 Sodertalje, Sweden /_ Royal Institute of Technology (KTH), SE-100 44, Stockholm P. 7.

11. **Hong** S Road Grade and Vehicle Parameter Estimation for Longitudinal Control Using GPS/ Hong S. Bae1, Jihan Ryu and J. Christian Gerdes. Road Grade Estimation for Look-ahead Vehicle Control Per Sahlholm _ Karl Henrik Johansson ___ Scania CV AB, SE-151 87 Sodertalje, Sweden, Royal Institute of Technology (KTH), SE-100 44, Stockholm, P. 7.

12. **Mikhailov, V. G.** Reading, preprocessing of accelerations and slope angles with MPU-6050 and record of the binary data on SD a card Arduino Due / [the Electronic resource] / https://rep.bntu.by/handle/data/26742 // – The Access mode: 24.12.2017.

Поступила *20.03.2018*

После доработки *18.05.2018*

Принята к печати *01.06.2018*

Mikhailov V. G.

THE ANALYSIS OF METHODS OF RECEPTION OF LONGITUDINAL PROFILE OF ROADS

sapr7@mail.ru

The analysis of methods of reception of longitudinal biases/profile of road important for carrying out of modelling of movement of the vehicle on the basis of geodetic charts, gaugings of roads by means of the geodetic equipment, use mobile laboratories is carried out, radar scanning of the earth, data read-out from the electronic control package of the car and the estimation of their accuracy is given. It is noticed that the listed modes are labour-consuming and Expenses and not always provide necessary accuracy. So in case of use of the popular data of radar scanning of the earth from companions the error can reach 30–50%. Though in the future in process of perfection of accuracy of sounding and availability of the information the given mode is represented to the most perspective.

The method of registration of cross-sections/biases of the big sites of roads in the course of movement of the vehicle on the basis of microcontroller Arduino Due, the gauge of speedups and discharge angles MPU-6050 and data recording on a SD-card is offered, application of the combined processing of the information on the basis of the developed programs in language With in the microcontroller and in module S-Function Builder in package Matlab/Simulink is considered.

By means of the offered methods registration of biases of road of difficult character by extent of 10 km is spent. And for the same road the method of use of a chart of radar scanning of the earth constructs a road cross-section. Comparison of results of methods of use of speedups and radar scanning of the earth is spent.

Good coincidence of character of change of a cross-section of road and sredne-quadratic and maximum values of heights of a cross-section of the road, received on the offered methods (a toe-out of 7–20%) is revealed.

Keywords: *the Car, a longitudinal profile/bias of road, modelling of biases of road and external indignation, microcontroller Arduino, MatLab/SimuLink.*

Владимир Георгиевич Михайлов канд. техн. наук, РБ, Минск. Специалист в области разработки систем CALS/PLM (PDM, ERP), программирования в Windows, Linux/Raspbian, Arduino/ Raspberry, автомобилестроения, моделирования динамических систем в пакетах MATLAB\SIMULIK, оценки напряженно-деформированного состояния в пакете ANSYS, испытаний подвесок, рам ТС, пневматики, гидравлики, тензометрирования.

Tel.: + 375-(029)785–09–16. E-mail: sapr7@mail.ru.

Mikhailov Vladimir (S'72–M'76–SM'80) received the D. degree (Cand. Tech. Sci., mechanical Engineering) from the Belarussian Polytechnical institute of Belarus, Minsk, in 1982.

He was a Senior Research and Engineer-designer at Minsk Automobile plant, from 1972 to 1984, Leading Research, Chief of Research laboratory in CenterSystem, Minsk (design and development ERP) from 1984 to 1991, and was leading Engineer-designer at Minsk Wheel plant from 1994 to 2010, from 2010 to 2017 was a leading engineer of Open Stock Company «Midivisana», Republic Belarus, Minsk. His research interests include design and development of Software PDM, ERP, application Oracle on C++, PL/SQL, Java, programming MC, modeling dynamic systems, vibration.

The expert in the field of system engineering CALS/PLM (PDM, ERP), programming MC, Windows, Linux/Raspbian, Arduino/Raspberry, motor industry, modeling of dynamic systems in packets MATLAB\SIMULIK (with S-Function Builder), estimations of the intense-deformed state in packet ANSYS, to tests of suspension, frames of the vechicle, a pneumatics, hydraulics.

ОБРАБОТКА ИНФОРМАЦИИ И ПРИНЯТИЕ РЕШЕНИЙ

DATA PROCESSING AND DECISION-MAKING

УДК 519.6

В. М. РОМАНЧАК

АППРОКСИМАЦИЯ СИНГУЛЯРНЫМИ ВЕЙВЛЕТАМИ

Задача аппроксимации является актуальной практически для любого инженерного исследования. В этой связи представляют интерес универсальные методы аппроксимации. В работе развивается метод непараметрической аппроксимации – метод сингулярных вейвлетов. Метод включает в себя эффективный численный алгоритм, основанный на суммировании рекуррентной последовательности функций. Универсальность алгоритма означает, что его можно применять для приближения одномерных и многомерных функций, в системах поддержки принятия решений, при обработке стохастической информации, распознавании образов, решении краевых задач.

Во введении поясняется идея метода сингулярных вейвлетов – объединить теорию вейвлетов с ядерными оценками регрессии типа Надарая-Ватсона. Обычно ядерные оценки рассматриваются как пример непараметрического оценивания. Однако один параметр – параметр размытости, все же присутствует в традиционном алгоритме ядерной регрессии. Выбор оптимального значения этого параметра является сложной математической задачей и этому вопросу посвящены многочисленные работы. При аппроксимации по методу сингулярных вейвлетов происходит суммирование ядерных оценок типа Надарая-Ватсона по параметру размытости, что в значительной степени снимает проблему оптимального выбора этого параметра.

В основной части работы формулируются теоремы, которые определяют свойства регуляризованного вейвлет-преобразования. Впервые получены достаточные условия равномерной сходимости вейвлет ряда. Для иллюстрации эффективности численного алгоритма аппроксимации рассмотрен пример квази-интерполяции функции Рунге вейвлетами с равномерным распределением узлов интерполяции.

Ключевые слова: *вейвлет преобразование, окно Парзена–Розенблатта, непараметрическая аппроксимация, ядерная оценка Надарая–Ватсона.*

Введение

Распространение методов непараметрической аппроксимации объясняется возможностью их применения для построения сложных математических моделей [1]. В прикладных работах используют аппроксимацию ядерными функциями [2], [3], [4], [5] и аппроксимацию вейвлетами [6], [7], [8]. В данной работе развивается метод сингулярных вейвлетов, в котором используется вейвлет преобразование с ядерными функциями.

Метод сингулярных вейвлетов был предложен и сформулирован нами в работах [9], [10]. Пусть $\psi(x)$ – это базисный вейвлет [6] («маленькая волна», «всплеск»). В вейвлете варьируют значения параметра масштабирования a и параметра сдвига b:

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

В теории вейвлетов рассматривают скалярное произведение действительной функции $f(t)$ и вейвлет функции (1), которое называют вейвлет-преобразованием:

$$Wf(b,a)=\frac{1}{a}\int_{-\infty}^{\infty} f(t)\psi\left(\frac{t-b}{a}\right)dt\,. \qquad (2)$$

Можно показать, что если функция $\psi(x)$ в среднем равна нулю,

$$\int_{-\infty}^{\infty}\psi(t)\,dt=0, \qquad (3)$$

то в преобразовании (2) «малый всплеск» приводит к «маленькой волне», т. е. функция $Wf(b, a)$ для малых a будет близка к нулю [7]. Если базисный вейвлет $\psi(t)$ в среднем не равен нулю, то назовем такой вейвлет сингулярным. Если вейвлет является сингулярным («большой всплеск»), то преобразование $Wf(b, a)$ может привести к «большой волне», т. е. функция $Wf(b, a)$ не будет стремиться к нулю при малых a.

Аппроксимация сингулярными вейвлетами, основывается на регуляризации вейвлет преобразования (2) по формуле:

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

Если вейвлет не является сингулярным, то регуляризованное вейвлет преобразование (4) совпадает с вейвлет преобразованием (2). Но для сингулярного вейвлета «большой всплеск» по-прежнему будет приводить к «маленькой волне», т.е. функция $W(f-f(b))(b, a)$ для малых a будет близкой к нулю. В качестве вейвлета в преобразовании $W(f-f(b))(b, a)$ можно взять дельта-образные функции, которые применяют при ядерной оценке регрессии [2], например вейвлетом может быть функция плотности стандартного нормального распределения. Тогда, если интеграл в выражении (4) заменить суммой и считать преобразование $W(f-f(b))(b, a)$ достаточно малой величиной, получим непараметрическую ядерную оценку Надарая–Ватсона [3], [4]:

$$f(b)\approx\frac{\sum_{i=1}^{n}f(t_i)\psi\left(\frac{t_i-b}{a}\right)}{\sum_{i=1}^{n}\psi\left(\frac{t_i-b}{a}\right)}. \quad (5)$$

Для ядерной оценки (5) существенно условие положительности ядра. Мы видим, что регуляризация вейвлет преобразования позволяет объединить теорию вейвлетов с ядерными оценками регрессии. Такое объединение названо нами методом сингулярных вейвлетов.

Сингулярный вейвлет

Определение. Пусть $\psi(t)$ – убывающая на бесконечности функция, причем такая, что

$$\psi(t)\le\frac{q}{1+t^2}, \quad (6)$$

q – некоторая константа, $q > 0$, для которой существует конечное среднее значение. Такую функцию будем называть базисным вейвлетом. Базисный вейвлет $\psi(t)$ равный нулю в среднем (условие (3)) будем называть классическим, а не равный нулю – сингулярным. Базисный сингулярный вейвлет, удовлетворяющий условию нормировки,

$$\int_{-\infty}^{\infty}\psi(t)dt=1, \quad (7)$$

будем называть *дельта-вейвлетом*.

Для дельта-вейвлета, регуляризация (4) равна разности вейвлет-преобразования и значения функции $f(b)$: $W(f-f(b))(b, a) = Wf(b, a) - f(b)$. Для классического вейвлета регуляризация (4) совпадет с вейвлет-преобразованием: $W(f-f(b))(b, a) = Wf(b, a)$. В работе [10] доказаны теоремы.

Теорема 1. Пусть ψ – базисный сингулярный вейвлет. Если функция $\psi(t)$ четная, $\psi(t) \in L^2$, $t\psi(t) \in L^1$, тогда для любой непрерывной в точке t функции $f(t)$ из $L^2(R)$:

$$f(t)=\frac{1}{C}\int_0^{\infty}\int_{-\infty}^{\infty}\frac{1}{a^2}W(f-f(b))f(b,a)\psi\left(\frac{t-b}{a}\right)dbda$$

где

$$C=2\pi\int_0^{\infty}\frac{\big(\Psi(u)-\Psi(0)\big)\Psi(u)}{u}du$$

причем

$$|C|<\infty, \quad (8)$$

где $\Psi(x)$ – преобразование Фурье для функций $\psi(t)$:

$$\Psi(x)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}\psi(t)e^{ixt}dt.$$

Теорема 2. Пусть $f(t) \in L^1$, $\psi(t)$ – базисный дельта-вейвлет, тогда преобразования $W(f-f(b))(b, a)$ в каждой точке непрерывности функции $f(b)$ при $a \to 0$, $a > 0$ стремится к нулю: $W(f-f(b))(b, a) \to 0$.

Последовательность вейвлет-преобразований

Лемма. Если функция $f(x) \in L^1$ и непрерывна в точке x, то преобразование $F(x) = W(f-f(x))(x, a)$ непрерывно в точке x и $F(x) \in L^1$, [10].

Введем последовательность регуляризованных вейвлет-преобразований $F^k(x)$:

$$F^{k+1}(x)=F^k(x)-WF^k(x,a_k), \quad (9)$$

где $WF^k(x,a_k)=\frac{1}{a_k}\int_{-\infty}^{\infty}F^k(t)\psi\left(\frac{t-x}{a_k}\right)dt$ – вейвлет преобразование, $k = 0, 1, ..., K-1$, $F^0(x) = f(x)$ – начальная функция. Тогда справедлива следующая теорема.

Теорема 3. Для непрерывной в точке x функции $f(x)$ существует разложение по формуле

$$f(x)=\sum_{k=0}^{K\text{-}1}WF^k(x,a_k)+F^K(x), \quad (10)$$

где a_k – произвольная последовательность действительных чисел, $a_k > 0$, k – номер преобразования, $F^K(x) = W(F^{K-1} - F^{K-1}(x))(x, a_{K-1})$ – остаточный член, $F^K(x) \to 0$, при $a_{K-1} \to 0$, K – порядок аппроксимации.

Доказательство проиллюстрируем на примере разложения второго порядка, $K = 2$. В этом случае рекуррентные формулы (9) имеют вид

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

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

Сложив эти равенства, получим

$$F^2(x) = F^0(x) - WF^1(x, a_0) - WF^0(x, a_1)$$

и

$$f(x) = WF^0(x, a_0) + WF^1(x, a_1) + F^2(x).$$

Причем функции $F^1(x)$, $F^2(x)$ – принадлежат пространству $L^1[A, B]$ и непрерывны в точке x (на основании Леммы). Остаточный член $F^2(x)$ можно сделать сколь угодно малым, подходящим выбором a_1 на основании Теоремы 1. Для произвольного порядка K, формула доказывается аналогично. В случае $K = 1$ разложение (10) совпадает с оценкой регрессии Надарая-Ватсона.

Равномерная сходимость вейвлет-ряда

Пусть $F^k(x)$ – последовательность вейвлет-преобразований (9) с начальной функцией $F^0(x) = f(x)$ и

$$WF^k(x, a_k) = \frac{1}{a_k} \int_{-\infty}^{\infty} F^k(t) \psi\left(\frac{t - x}{a_k}\right) dt. \quad (11)$$

Ряд

$$\sum_{k=0}^{\infty} WF^k(x, a_k), \quad (12)$$

будем называть вейвлет-рядом.

В формуле (10) значение функции $f(x)$ равно частичной сумме вейвлет-ряда (12) и остаточного члена. Рассмотрим, при каких условиях вейвлет-ряд (12) сходится равномерно.

Теорема 4. (**Достаточное условие равномерной сходимости.**) Пусть начальная функция, $F^0(x) = f(x)$, для ряда (12) удовлетворяет условию Липшица, $|f(x) - f(y)| < A|x - y|, x, y \in R$, A – постоянная и $\psi(u)$ – положительный дельта-вейвлет, $u\psi(u) \in L^1$. Вейвлет-ряд (12) сходится равномерно для всех $x \in R$, если $a_k = a_0 q^k$, $a_k > 0$, $k = 0, 1, –$, где $0 < q < 1/2$.

Доказательство. Запишем регуляризованное вейвлет-преобразование (9) в виде

$$F^{k+1}(x) = \int_{-\infty}^{\infty} \left(F^k(x) - F^k(x + a_k u)\right) \psi(u)\, du, \quad (13)$$

где $F^0(x) = f(x)$, $k = 0, 1, \ldots$.

Тогда

$$\left|F^{k+1}(x + \Delta x) - F^{k+1}(x)\right| \le$$

$$\int_{-\infty}^{\infty} \left(\left|F^k(x + \Delta x) - F^k(x)\right| + \right. \quad (14)$$

$$\left.\left|F^k(x + a_k u + \Delta x) - F^k(x + a_k u)\right|\right) \left|\psi(u)\right| du.$$

В частном случае для $k = 0$ из неравенства (14) и условия Липшица $|f(x + \Delta x) - f(x)| < A|\Delta x|$ и $|f(x + a_1 u + \Delta x) - f(x + a_1 u)| < A|\Delta x|$, получим

$$\left|F^1(x + \Delta x) - F^1(x)\right| \le 2A\left|\Delta x\right| \int_{-\infty}^{\infty} \left|\psi(u)\right| du = 2A\left|\Delta x\right|, \quad (15)$$

для положительного дельта-вейвлета

$$\int_{-\infty}^{\infty} \left|\psi(u)\right| du = 1.$$

Далее, для $k = 1$ на основании (14) с учетом (15), будет выполняться

$$\left|F^2(x + \Delta x) - F^2(x)\right| \le 2^2 A\left|\Delta x\right|.$$

Аналогично в общем случае

$$\left|F^k(x + \Delta x) - F^k(x)\right| \le 2^k A\left|\Delta x\right| \quad (16)$$

Теперь для $F^{k+1}(x)$ в формуле (13) с помощью оценки (16), получим

$$\left|F^{k+1}(x)\right| \le \int_{-\infty}^{\infty} \left|F^k(x) - F^k(x + a_k u)\right| \left|\psi(u)\right| du \le$$

$$2^k A a_k \int_{-\infty}^{\infty} |u| \left|\psi(u)\right| du,$$

$k = 0, 1, 2, \ldots$, и, следовательно,

$$\left|F^{k+1}(x)\right| \le 2^k a_k C, \quad (17)$$

где $C = A \int_{-\infty}^{\infty} |u| \left|\psi(u)\right| du$.. Если $a_k = a_0 q^k$, $k = 0, 1, \ldots$, где $0 < q < 1/2$, тогда ряд (12) сходится равномерно на основании (17), поскольку в этом случае $F^{K+1}(x) \to 0$. Аппроксимация дельта-вейвлетами (12) может служить обоснованием численного алгоритма дискретной аппроксимации.

Алгоритм аппроксимации

Пусть задан набор точек x_i, $i = 0,1, ..., n$, а также значения функции y_i в этих точках. Требуется построить функцию $f(x)$, проходящую близко к значениям y_i в точках x_i, $f(x_i) \approx y_i$, $i = 1, ..., n$.

Присваиваем начальные значения y_i коэффициентам вейвлета нулевого порядка W_i^0:

$$W_i^0 = y_i, \; i = 1, ..., n.$$

Вычисляем коэффициенты регуляризованного вейвлет-преобразования, используя дискретный аналог формулы (9):

$$W_j^k = W_j^{k-1} - \frac{\sum\limits_i W_i^{k-1} \psi\left(\dfrac{x_i - x_j}{a_{k-1}}\right)}{\sum\limits_i \psi\left(\dfrac{x_i - x_j}{a_{k-1}}\right)} \qquad (18)$$

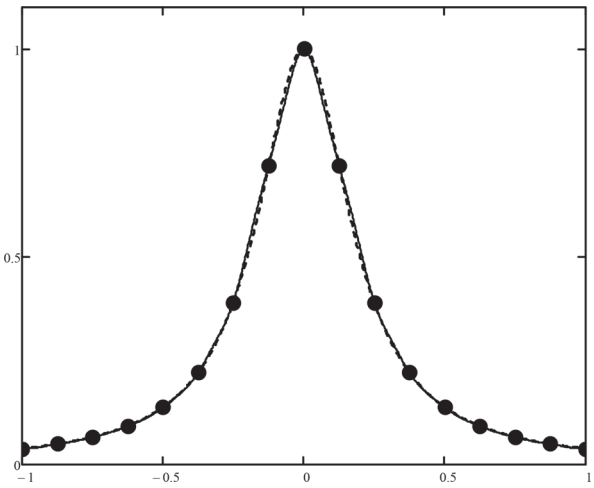
здесь $k = 1, ... K - 1$, W_i^k – значения коэффициентов вейвлета k-го порядка в точке x_i, $i, j = 1, ..., n$, $a_k = \alpha 2^{-k}$, α – постоянная.

Восстанавливаем функцию $f_K(x) \approx f(x)$ во всех точках интервала $[A, B]$, используя аналог формулы (10):

$$f_K(x) = \sum_{k=1}^{K} \frac{\sum\limits_i W_i^{k-1} \psi\left(\dfrac{x_i - x}{a_{k-1}}\right)}{\sum\limits_i \psi\left(\dfrac{x_i - x}{a_{k-1}}\right)}. \qquad (19)$$

Пример.

В 1901 г. Рунге исследовал интерполяцию полиномами на отрезке $[-1, 1]$ функции $f(x) = 1/(1 + 25x^2)$ при равномерном распределении узлов сетки и показал, что при бесконечном увеличении степени n интерполяционного полинома P_n последовательность P_n расходится на интервале $[-1, 1]$. Выполним квази-интерполяцию функции Рунге $f(x)$ методом сингулярных вейвлетов**,** равномерно распределив узлы интерполяции на промежутке $[-1, 1]$. Выберем базисный сингулярный вейвлет $\psi(x) = e^{-x^2}$, $x_i = -1 + ih$, $i = 0, 1, ..., 16$, $h = 1/8$, $y_i = f(x_i)$. Найденные значения коэффициентов вейвлетов W_i^k



Аппроксимация функции Рунге

по формуле (18) приведены в таблице (ввиду симметрии представлена только половина коэффициентов, $i = 8, 9, ..., 16$). Номер строки m, $m = 1, 2, ..., 7$, соответствует номеру итерации $k = m - 1$.

Коэффициенты вейвлетов W_i^k

1	0,72	0,39	0,22	0,14	0,09	0,07	0,05	0,04
0,72	0,44	0,11	–0,05	–0,13	–0,17	–0,18	–0,19	–0,19
0,68	0,40	0,08	–0,07	–0,13	–0,16	–0,16	–0,15	–0,15
0,50	0,24	–0,03	–0,12	–0,12	–0,09	–0,06	–0,04	–0,04
0,27	0,06	–0,09	–0,08	–0,04	–0,01	0,01	0,01	0
0,09	–0,01	–0,04	–0,01	0	0	0	0	0
0	0	0	0	0	0	0	0	0

Значения аппроксимирующей функции были рассчитаны по формуле (19). На рисунке представлены график функции Рунге — – $f(x)$, аппроксимирующей функции ---- – $f_K(x)$ и • – узлы интерполяции.

Выводы

В работе развивается новый метод аппроксимации – метод сингулярных вейвлетов, доказано достаточное условие равномерной сходимости вейвлет ряда, приводится пример квази-интерполяции функции.

ЛИТЕРАТУРА

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 / Ann. Math. Statistic. 1962. V. 33. No. 3. P. 1065–1076.

3. **Watson, G. S.** Smooth regression analysis / G. S. Watson // Sankhya. Ser. A. -1964. – V. 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. **Деврой, Л.** Непараметрическое оценивание плотности. L-1 подход: пер. с англ. / Люк Деврой, Ласло Дьерфию- М.: Мир, 1988. – 407 с.

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

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

8. **Фрейзер, М.** Введение в вэйвлеты в свете линейной алгебры: пер. с англ. / М. Фрейзер. – М.: БИНОМ: Лаборатория знаний, 2008. – 487 с.

9. **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 // Доклады акад. наук Республики Беларусь. – 2006. – Т. 50, № 4. – С. 100–104.

10. **Романчак, В. М.** Аппроксимация экспертных оценок сингулярными вейвлетами / В. М., Романчак, П. М. Лаппо / Вестник Гродненского государственного университета. Серия 2: Математика. Физика. Информатика, вычислительная техника и управление/ Изд. Гродненский государственный университет имени Янки Купалы. – Гродно, 2017. – Т. 7, № 1. – С. 132–139.

REFERENCES

1. **Hardle, W.** Prikladnaja neparametricheskaja regressija. Applied nonparametric regression. Moscow, 1993, 349 p.

2. **Parzen E.** On estimation of a probability density function and mode // Ann. Math. Statistic. 1962. V. 33. No. 3. P. 1065–1076.

3. **Watson G. S.** Smooth regression analysis. Sankhya, Ser. A., 1964, vol. 26, pp. 359–372.

4. **Nadaraya E. A.** Ob ocenke regressii. About a regression assessment. Probability theory and its application,1964, vol. 9, no. 1, pp. 157–159.

5. **Devroye, L.** Neparametricheskoe ocenivanie plotnosti. L-1 podhod. Nonparametric Density Estimation: The L1. / Devroye, L. & L. Gyorfi. – Moscow, 1988, 407 p.

6. **Chui K.** Vvedenie v vejvlety. Introduction in wavelet. Moscow, 2001, 412 p.

7. **Daubechies I.** Desjat' lekcij po vejvletam. Ten Lectures on Wavelets, Izhevsk, 2001. – 464 c

8. **Frazier M.** Vvedenie v vjejvlety v svete linejnoj algebry. An introduction to wavelet through linear algebra./ Moscow, 2008, 487 p.

9. **Serenkov P. S., Ramanchak 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. Reports of the academician of sciences of Republic of Belarus, 2006, vol. 50, no. 4, pp. 100–104.

10. **Ramanchak V. M., Lappo P. M.** Approksimacija jekspertnyh ocenok singuljarnymi vejvletami. Approximation of expert estimates by singular wavelets. Bulletin of the Grodno State University. Series 2: Mathematics. Physics. Informatics, Computer Science and Management, 2017, vol. 7, no. 1, pp. 132–139.

Поступила	*После доработки*	*Принята к печати*
22.03.2018	*14.05.2018*	*01.06.2018*

Romanchak V. M.
vmracer@yandex.by, Romanchak@bntu.by

The problem of approximation is relevant for most engineering applications. In this connection, the universal methods of approximation are of interest. The method of nonparametric approximation is developing in the paper – the method of singular wavelets. The method includes an effective numerical algorithm based on the summation of a recursive sequence of functions. The universal algorithm of approximation makes it possible to apply it to approximate one-dimensional and multidimensional functions, in decision support systems, in the processing of stochastic information, pattern recognition, and solution of boundary-value problems.

The introduction explain the idea of the method of singular wavelets – to combine the theory of wavelets with the Nadaraya-Watson kernel regression estimator. Usually, Nadaraya-Watson kernel regression are considered as an example of nonparametric estimation. However, one parameter, the smoothing parameter, is still present in the traditional kernel regression algorithm. The choice of the optimal value of this parameter is a complex mathematical problem, and numerous studies have been devoted to this question. In the approximation by the method of singular wavelets, summation of Nadaraya-Watson kernel regression estimates with the smoothing parameter takes place, which solves the problem of the optimal choice of this parameter.

In the main part of the paper theorems are formulated that determine the properties of the regularized wavelet transform. Sufficient conditions for uniform convergence of the wavelet series are obtained for the first time. To illustrate the effectiveness of the numerical approximation algorithm, we consider an example of the quasi-interpolation of the Runge function by wavelets with a uniform distribution of interpolation nodes.

Keywords: *Wavelet transform, the Parzen–Rosenblatt window method, nonparametric estimator, Nadaraya-Watson kernel regression*

Романчак Василий Михайлович – доцент кафедры инженерной математики БНТУ, кандидат физ.мат. наук (1987), доцент (1991). Научные интересы в области обработки экспертных оценок и методов непараметрической аппроксимации (метод сингулярных вейвлетов). Опубликовано более 20 журнальных публикаций и монография.

Ramanchak Vasily Mikhaylovich is the associate professor of engineering mathematics of BNTU, the candidate of physical and mathematical sciences (1987), associate professor (1991). Scientific interests in the field of processing of expert estimates and methods of nonparametric approximation (method of singular wavelet). More than 20 journal publications and the monograph are published.

УДК 004.41 : 004.65 : 004.67

Л. В. РУДИКОВА, В. В. ДАНИЛЬЧИК

О ПОДХОДАХ К СОЗДАНИЮ СИСТЕМЫ АВТОМАТИЗАЦИИ, СВЯЗАННОЙ С СОЦИАЛЬНО-ЭКОНОМИЧЕСКИМИ ПЕРЕМЕЩЕНИЯМИ ЛЮДЕЙ

Учреждение образования
«Гродненский государственный университет имени Янки Купалы»

В современных условиях актуальным является разработка общей концепции и реализация системы хранения и анализа данных, связанных с социально-экономическими перемещениями людей. Движение населения, связанное как с долгосрочными, так и краткосрочными миграциями носит возрастающий характер, что непосредственно влияет на различные сферы деятельности как отдельной страны, так и мирового сообщества, в целом. В предлагаемой статье описывается предметная область, связанная с социально-экономическими перемещениями людей, отмечаются ключевые особенности внутренних и внешних миграций. Исходя из предметной области, предлагается общая архитектура универсальной системы накопления и обработки данных, которая базируется на клиент-серверной архитектуре. Для серверной части системы приводится фрагмент модели данных, которая связана с накоплением данных из внешних источников. Предлагаются общие подходы к использованию алгоритмов и необходимых структур данных. Описывается каркас архитектуры системы с возможностью масштабирования как вертикального так горизонтального.

Предлагаемая система организовывает процесс поиска данных и заполнения базы из сторонних источников. Для этого в системе разработан модуль для сбора и преобразования информации из сторонних Интернет-источников и отправки их в базу данных. В работе отмечаются особенности клиентского приложения, которое предоставляет удобный интерфейс для анализа данных в виде диаграмм, графиков, карт и т.п. Система предназначена различных пользователей, заинтересованных в анализе экономико-социальных перемещений, например, туристическим организациям, желающим получить статистику за определенное время, авиакомпаниям, которым открывается возможность планировать рейсы в том или ином направлении, а также государственным структурам с целью анализа миграционных потоков населения и выработке соответствующей стратегии их регулирования.

Ключевые слова: *веб-система, социально-экономические перемещения, модель данных, общая архитектура, алгоритм Бойера-Мура; клиент-сервер; подсистема анализа*

О предметной области исследований, связанной с социально-экономическими перемещениями людей

На сегодняшний день все большее число практиков и научных исследователей используют большие данные для измерения различных аспектов человеческой деятельности, включая мобильность человека. Например, такие наборы данных используются для регионального разграничения в различных масштабах [1, 2], классификации землепользования [3], оптимизации транспортировки и исследований в области транспорта [4], подсчета социально-экономических показателей городских кварталов [5], изучение туристического поведения [6] и многих других социальных наук.

В силу этого актуальным представляется разработка общей концепции и реализация системы складирования и обработки данных, связанных с различными видами деятельности людей, которая может быть рассмотрена в аспекте создания некоторого глобального хранилища данных [7, 8].

Исследование и обобщение предметных областей различной тематики является востребованным направлением исследований [9, 10]. Во-первых, в мире накоплены огромные массивы информации, часто достаточно разрозненной и воспринимаемой в отрыве от общей картины жизнедеятельности общества. Во-вторых, разработаны и разрабатываются различные методы, алгоритмы и методологии анализа

данных [11–13], которые используются для конкретной выборки или совокупности исследуемых данных. В-третьих, имеется достаточное количество необходимого программного обеспечения, технологий и методов формализации массивов данных, которые позволяют структурировать данные определенной тематики. С другой стороны, пример развития Всемирной сети показывает, что в едином информационном пространстве данные, практически, взаимосвязаны, порождены различными видами деятельности общества и следует рассматривать их в контексте цельного представления, но в рамках проекций определенного вида деятельности или взаимодействий.

Рассмотрим основные аспекты предметной области, связанной с социально-экономическими перемещениями людей.

Под перемещением населения или миграцией понимается его «механическое движение» по территории земного шара. Миграции могут бывают внешними и внутренними.

Внутренние миграции связаны с перемещением людей из одного региона страны в другой с целью поиска нового места проживания и/или работы. Внутренние миграции наблюдаются в пределах территории страны своего происхождения (например, миграция из сельской местности в города).

Внутренние миграции рассматривают перемещение людей за пределы своей страны, причем, можно выделить следующие виды внешней миграции:

– *эмиграция* – выезд граждан из своей страны в другую на постоянное жительство или достаточно длительный срок;

– *иммиграция* – въезд граждан в другую страну на постоянное жительство или достаточно длительный срок.

Кроме того, по длительности процесса перемещения миграции могут быть как краткосрочные (например, с целью туризма), так и долгосрочные (работа, учеба и т.п.)

Под *данными об экономико-социальных перемещениях* будем понимать количество людей, переехавших из одного географического региона в другой с учетом различных параметров, связанных с социальным, финансовым, экономическим, культурным и т. п. статусом людей.

Исследование экономико-социальных перемещений людей позволит с высокой степенью достоверности выделить наиболее благоприятные географические объекты для людей в соответствии с определенными критериями их жизни и внутренними установками. Кроме того, возможно отслеживание общемировых тенденций как в плане экономико-социального развития, так и в плане благоприятности регионов для туризма в конкретные периоды времени.

В целом, движение населения носит возрастающий характер. Этому способствует процессы глобализации в современном мире, упрощение визового режима между странами, рост политической миграции и другие факторы. Отметим, что общая статистика не учитывает причины возникновения тех или иных тенденций, отсутствуют конкретные демографические, политические, социальные факторы, которые и являются первопричиной возникновения тех или иных миграционных потоков. Сбор статистических сведений, чаще всего, носит изолированный характер и представляет лишь численные показатели выбранных метрик. Полученные данные принимаются как отображение текущего положения.

Источники данных государственных учреждений, являясь общедоступными, не всегда легко поддаются обработке из-за отсутствия программного интерфейса и специфических форматов хранения. Такие ограничения, как правило, не позволяют легко использовать их при проведении анализа. Кроме возможностей анализа данных возникает также вопрос и отображения их в доступном виде, в частности, в виде различных графических визуализаций.

На основе статистических данных о миграциях и анализа сопутствующих данных возможно создание прогностического аппарата, способного на основе сопутствующих данных предсказать, например, темпы миграции в тот или иной регион.

Таким образом, предлагаемая разработка использует данные об экономико-социальных перемещениях людей. Причем, основным источником демографических и миграционных данных выбран веб-ресурс Организации Объединенных Наций [14], который имеет огромное количество информации о миграционных показателях в различных странах мира. Данные можно получить в виде файла. Этот ресурс является основным источником данных для разрабатываемого приложения.

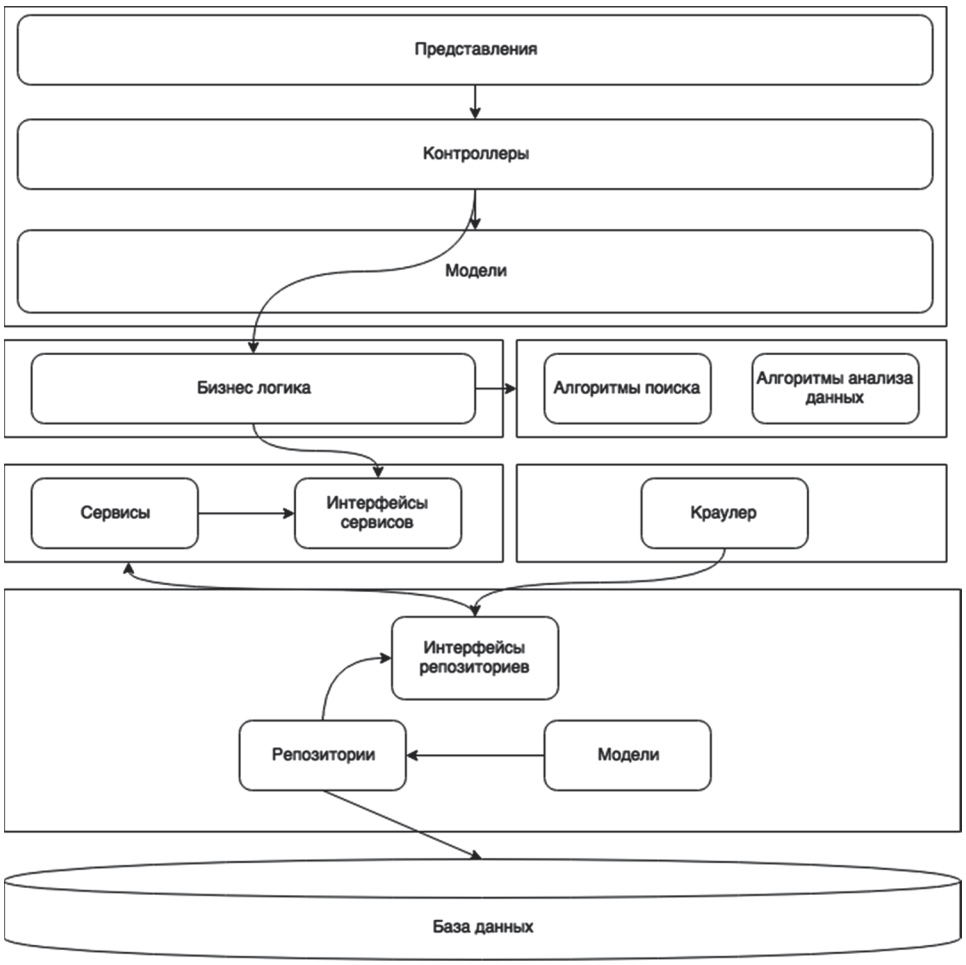


Рис. 1. Общая архитектура реализации

Для изучения внутренней миграции в конкретных странах можно использовать национальных ресурсов, например, таких как сайт европейской статистики Евростат [15] или сайт Национального статистического комитета Республики Беларусь [16http://www.belstat.gov.by/].

Общая архитектура приложения, связанного с миграционными данными

Система обработки социально-экономических перемещений использует клиент-серверной архитектуре и предназначено для предоставления пользователям наиболее актуальных данных экономико-социальных перемещений людей. Приложение организовывает процесс поиска данных и заполнения базы из сторонних источников. Для этого в системе разработан модуль для сбора и преобразования информации из сторонних Интернет-источников и отправки их в базу данных.

Система предоставляет неавторизованному пользователю возможность регистрации в системе, а также – фильтрации и просмотра информации.

Авторизованные пользователь может принимать одну из трех ролей: Администратор, Редактор или Пользователь.

Администратор должен обладать возможностью редактирования данных о пользователях, в том числе создавать новых, либо менять их роли. Остальные возможности Администратор должны совпадать с теми, которые предоставлены Редактору.

Редактор может добавлять, редактировать и удалять контент. В его обязанности входит обновление информации, связанной с экономико-социальными перемещениями людей.

Пользователю предоставляется возможность задания фильтрации данных экономико-социальных перемещений для дальнейшего анализа и визуализации.

Общая архитектура реализации системы и связи между уровнями изображены на рис. 1.

Система реализована в виде трех уровней, имеющих минимальные связи между собой: уровень базы данных; уровень, включающий доступ к данным; сервисный уровень; уровень, включающий бизнес-логику; уровень взаимодействия с пользователем.

Уровень базы данных представляет собой отдельный сервер, на котором развернута СУБД. Уровень базы данных связан с сервисным проецированием бизнес моделей на реляционные объекты базы данных с помощью Репозитория (компонент Repository). Репозиторий также ответственен за работу с данными (сохранение, обновление, удаление, выборка). Основой репозитория является технология ADO. NET Entity Framework. База данных системы содержит информацию о пользователях системы, контент и статистические данные, связанные с социально-экономическими перемещениями людей.

Слой взаимодействия с базой данных содержит набор классов, представляющих модели данных из доменной области. На уровне этого слоя также реализуются классы-репозитории, инкапсулирующие в себе подключение к базе данных и формирование запросов, представляя для клиента интерфейс, через который открывается возможность произведения CRUD операций над элементами базы данных.

Отдельно в архитектуре выделена система заполнения базы данных. Этот компонент взаимодействует с базой данных через слой взаимодействия и предназначен для формирования консистентных данных. На уровне этого модуля должны быть реализованы классы, взаимодействующие с внешними источниками данных. Задачей таких классов является загрузка специфических данных на сервер, их конвертация, с учетом структуры исходных файлов, а также– запись этих данных базу.

Параллельно со слоем заполнения базы данных находится слой сервисов, на котором представлены модули поиска и кластерного анализа статистических данных социально-экономических перемещений людей. Модуль поиска реализует в себе алгоритм Боейра-Мура, для дальнейшего использования совместно с модулем кластерного анализа при формировании релевантных результатов поиска. Модуль кластерного анализа реализует метод невзвешенного попарного среднего для выделения кластеров на основе статистических данных. Оба модуля инкапсулируются слоем сервисов, который предназначен для предоставления данных внешним клиентам.

В качестве внешнего клиента выступает веб-приложение, которое представлено слоем бизнес логики и слоем представления. Слой бизнес логики взаимодействует со слоем сервисов для получения данных социально-экономических перемещений людей и результаты их анализа. Слой представления предназначен для визуализации полученных данных в виде диаграмм, графиков и таблиц.

Для создания системы используется программная технология. Net Framework компании Microsoft, язык C#, СУБД MS SQL SERVER, различные программные инструменты (Entity Framework, jQuery, amCharts), позволяющие решить поставленные задачи наиболее эффективным способом. В данном разделе описываются выбранные технологии и рассматриваются их основные преимущества.

О подходах к поиску и анализу данных

Алгоритм Боейра-Мура. Для поиска данных выбран алгоритм поиска по подстроке Бойера-Мура ([17], см. рис. 2).

Алгоритм сравнивает один за другим справа налево символы шаблона x, начиная с самого правого, с символами исходной строки y. Если все символы шаблона совпадают с наложенными символами строки, поиск закончен, т.к. подстрока найдена. В случае несовпадения некоторого символа (или полного совпадения всего шаблона) алгоритм использует две предварительно вычисляемых эвристические функции – сдвиг позиции вправо для начала сравнения. Таким образом, для сдвига позиции начала сравнения алгоритм Бойера-Мура выбирает между двумя функциями, которые называются эвристиками хорошего суффикса и плохого символа (другое название – эвристики совпавшего суффикса и стоп-символа). В силу того, что функции эвристические, выбор между ними осуществляется по итоговому значению.

Обозначим через Σ – алфавит. Пусть $|y| = |n|$, $|x| = m$, $|\Sigma| = \sigma$.

Предположим, что в процессе сравнения возникает несовпадение между символом $x[i] = a$ шаблона и символом $y[i+j] = b$ исход-

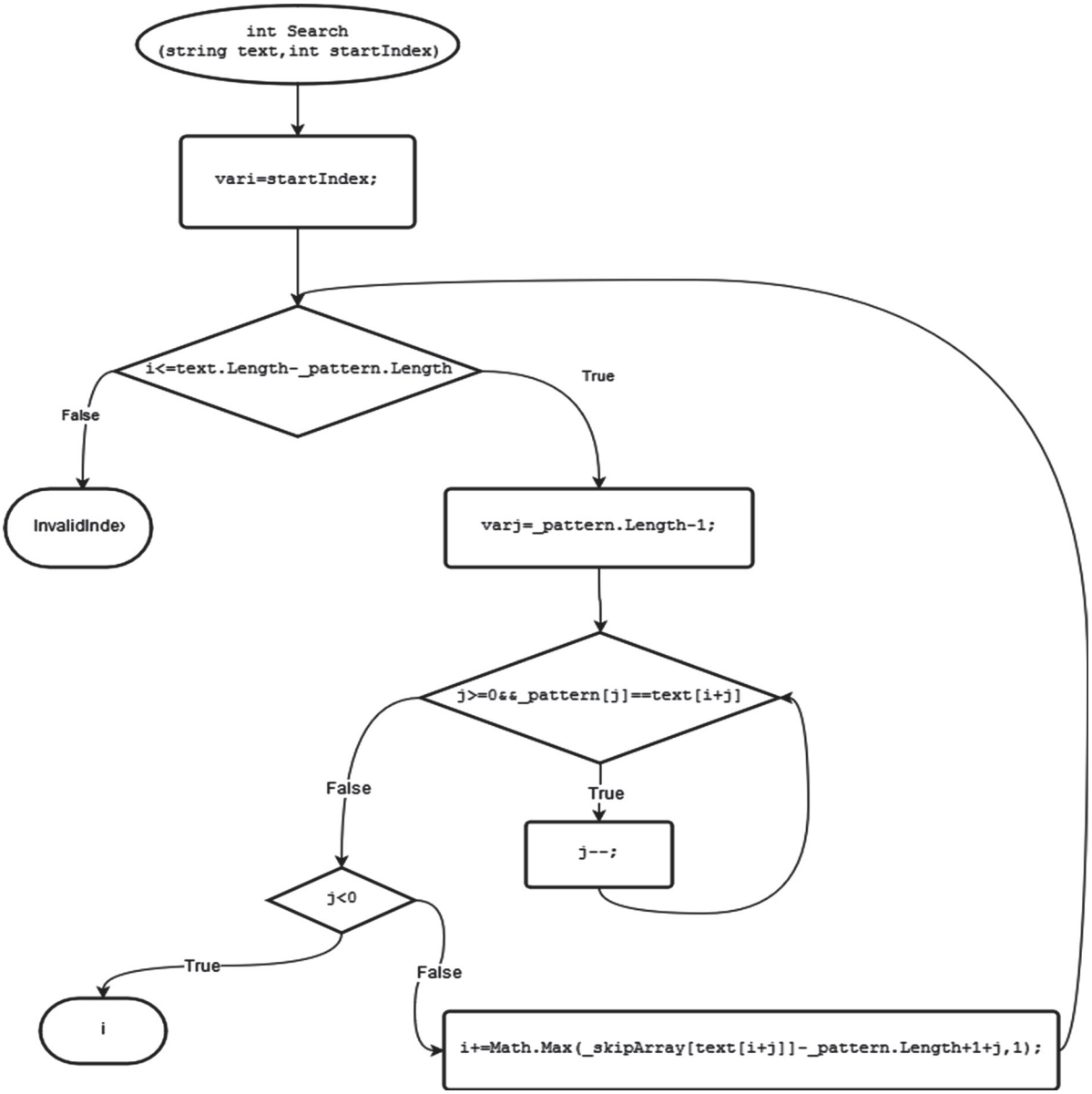


Рис. 2. Блок-схема алгоритма Бойера-Мура

ного текста при проверке в позиции j. Тогда $x[i+1...m-1]=y[i+j+1...j+m-1]=u$, $x[i]\neq y[i+j]$ и $m-i-1$ символов шаблона уже совпало.

Метод невзвешенного попарного среднего. Для анализа данных экономико-социальных перемещений людей был выбран метод невзвешенного попарного среднего для определения кластеров.

Пусть требуется провести классификацию заданного множества объектов методом невзвешенного попарного среднего. Перед началом работы алгоритма рассчитывается *матрица расстояний* между объектами: на каждом шаге в матрице расстояний находится минимальное значение, которое соответствует расстоянию между двумя наиболее близкими кластерами. Найденные кластеры u и v объединяются, образуя новый кластер k. Строки и столбцы, соответствующие кластерам u и v, выбрасываются из матрицы расстояний, и добавляется новая строка и новый столбец, соответствующие кластеру k. В результате матрица сокращается на одну строку и один столбец. Данная процедура повторяется до тех пор, пока не будут объединены все кластеры.

Пусть кластеры u, v и k содержат T_u, T_v и T_k объектов, соответственно. Кластер k образован путем объединения кластеров u и v, тогда $T_k = T_u + T_v$. Необходимо рассчитать удаленность кластера k от некоторого кластера ω.

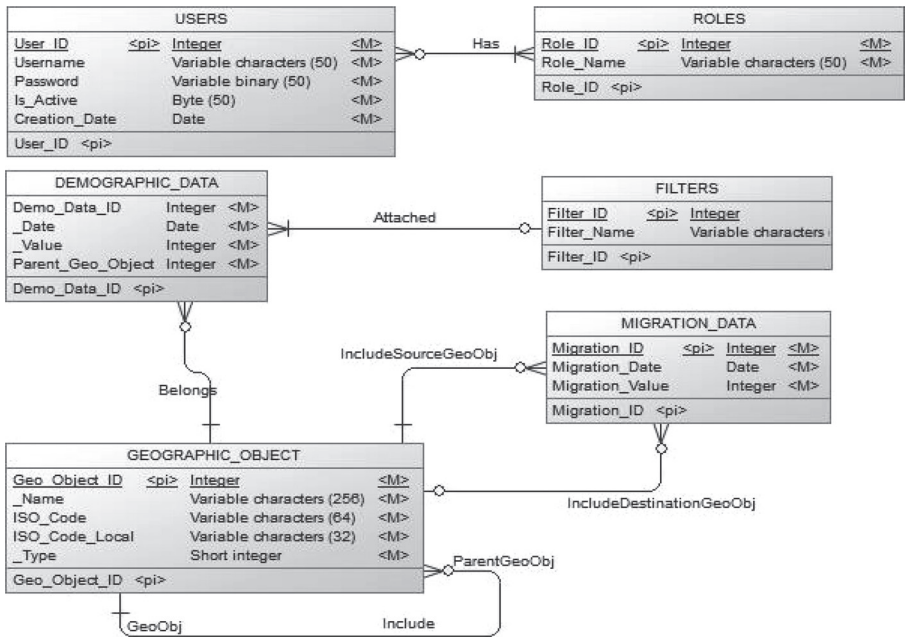


Рис. 3. Фрагмент концептуальной модели данных, связанной с демографическими и миграционными показателями

Расстояние между этими кластерами определяется согласно формуле:

$$D\left((u,v),\omega\right)=\frac{T_u D_{u,\omega}+T_v D_{v,\omega}}{T_u+T_v}.$$

Экспоненциальная аппроксимация линий тренда. Для прогнозирования определенных тенденций в сфере экономико-социальных перемещений людей используются линии трендов, причем, достаточно часто применяется экспоненциальная зависимость.

Экспоненциальная аппроксимация используется, как правило, в силу того, что у вводимых данных скорость возрастания входных данных достаточно велика. Однако существуют и ограничения использования такой аппроксимации, например, входные данные, не могут содержать нулевые или отрицательные характеристики.

В общем виде уравнение для экспоненциальной регрессии имеет следующий вид:

$$y=\alpha e^{\beta x},$$

где y – значение функции, x – область определения функция, α и β – константы.

О концептуальном моделировании данных системы

Для построения модели данных системы [8] использовалась структурна методология и средство автоматизированного проектирования PowerDesigner. Определены сущности системы, их взаимосвязи, ограничения на данные, ограничения целостности и пользовательские ограничения (см. рис. 3).

Отметим, что указанный фрагмент модели данных используется для анализа данных, которые загружаются в систему через автоматизированный поиска.

Для создания системы используется программная технология. Net Framework компании Microsoft, язык C#, СУБД MS SQL SERVER, различные программные инструменты (Entity Framework, jQuery, amCharts), позволяющие решить поставленные задачи наиболее эффективным способом.

Клиентское веб-приложение

Основная задача веб-клиента – это отображение демографических и миграционных данных на интерактивной карте, см., например, рисунок 4 и рис. 5.

Анализируя линии трендов для определенных кластеров можно сделать прогноз о том, в каких пределах будет изменятся количество въезжающих людей в определенный регион. На рисунке 5 представлена карта въезжающих во Французскую Республику. Анализ линий трендов показывает, что кластер стран, состоящий из государств Северной Африки, таких как Марокко и Алжир, будет доминирующим в 2020–2025 годах по количеству выехавших граждан.

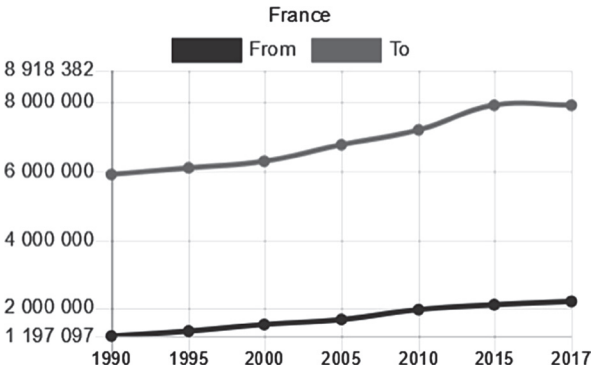


Рис. 4. Линия тренда Французской Республики

Отметим, что веб-клиент содержит также модуль для администратора системы, позволяющий редактировать пользователей и добавлять новые данные для анализа.

На основе кластеризованных данных с помощью GoogleChartsApi можно построить необходимые графики. В листинге приведен пример визуализации данных в виде графика на основе кластеризованных данных.

Листинг 3.8. Реализация построения графика на основе кластеризованных данных

```
// Load the Visualization API and the corechart package.
google.charts.load('current', {'packages':['corechart']});

// Set a callback to run when the Google Visualization API is loaded.
google.charts.setOnLoadCallback(drawChart);

// Callback that creates and populates a data table,
// instantiates the pie chart, passes in the data and
// draws it.
function drawChart() {

var elements = @Html.Raw(JsonConvert. SerializeObject(Model, Formatting. None));
var array = elements.map(function(item) {
return [item[0], parseInt(item[1])];
});

// Create the data table.
var data = new google.visualization. DataTable();
data.addColumn('string', 'Country Name');
data.addColumn('number', 'Number of People');
data.addRows(array);

// Set chart options
var options = {
'title': 'How much people immigrate',
'width': 400,
'height': 300
};

// Instantiate and draw our chart, passing in some options.
var chart = new google.visualization. PieChart(document.getElementById('@guid'));
chart.draw(data, options);
}
```

При реализации клиентского приложения был использован паттерн проектирования MVC. Его концепция позволяет разделить данные, представление и обработку действий пользователя на три отдельных компонента.

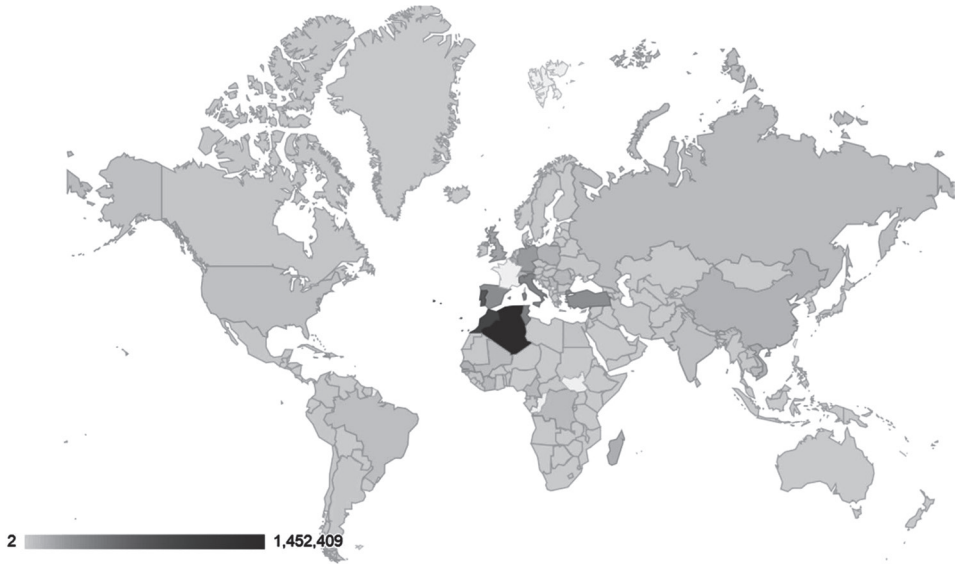


Рис. 5. Карта эмиграций во Французскую Республику

Заключение

Таким образом, актуальным представляется разработка системы, связанной с экономико-социальными перемещениями людей, данные которой будут являться исходной информацией для универсальной системы хранения и обработки данных практико-ориентированной направленности в контексте единого хранилища данных.

Предлагаемая система наряду с использованием в качестве первого уровня общей универсальной системы на основе технологии складирования данных, может быть востребована широким кругом лиц, заинтересованных в экономико-социальных перемещениях, таким как, туристическим организациям, желающим получить статистику за определенное время, авиакомпаниям, которым отрывается возможность планировать рейсы в том или ином направлении, а также государственными структурами с целью анализа миграционных потоков населения и выработке соответствующей стратегии их регулирования.

ЛИТЕРАТУРА

1. **Ratti, C.** Redrawing the map of Great Britain from a network of human interactions // C. Ratti, S. Sobolevsky, F. Calabrese, C. Andris, J. Reades, M. Martino, R. Claxton, S. Strogatz / PloS ONE. – 2010. – V. 5, № 12. – P. 14248.

2. **Hawelka, B.** Geo-located Twitter as proxy for global mobility pattern // B. Hawelka, I. Sitko, E. Beinat, S. Sobolevsky, P. Kazakopoulos, C. Ratti / Cartography and Geographic Information Science. – 2014. – V.41, № 3. – P. 260–271.

3. **Pei, T.** A new insight into land use classification based on aggregated mobile phone data // T. Pei, S. Sobolevsky, C. Ratti, S. L. Shaw, T. Li, C. Zhou / International Journal of Geographical Information Science. – 2014. – V.289, № 9. – P. 1988–2007.

4. **Santi, P.** Quantifying the benefits of vehicle pooling with shareability networks // P. Santi, G. Resta, M. Szell, S. Sobolevsky, S. H. Strogatz, C. Ratti / Proceedings of the National Academy of Sciences. – 2014. – V.111, № 37. – P. 13290–13294.

5. **Hashemian, B.** Socioeconomic characterization of regions through the lens of individual financial transactions // B. Hashemian, E. Massaro, I. Bojic, J. M. Arias, S. Sobolevsky, C. Ratti / PloS ONE. – 2017. – V.12, № 11. – P. 0187031.

6. **Bojic, I.** Scaling of foreign attractiveness for countries and states // I. Bojic, A. Belyi,, C. Ratti, S. Sobolevsky / Applied Geography. – 2016. – № 73. – P. 47–52.

7. **Рудикова, Л. В.** Об общей архитектуре универсальной системы хранения и обработки данных практико-ориентированной направленности // Л. В. Рудикова / Системный анализ и прикладная информатика. – Мн.: БНТУ, 2017. – № 2. – С. 12–19.

8. **Рудикова, Л. В.** О моделировании данных предметных-областей практико-ориентированной направленности для универсальной системы складирования и обработки данных// Л. В. Рудикова, Е. В. Жавнерко / Системный анализ и прикладная информатика. – Мн.: БНТУ, 2017. – № 3. – С. 19–26.

9. **Belyi, A.** Global multi-layer network of human mobility // Alexander Belyi, Iva Bojic, Stanislav Sobolevsky, Izabela Sitko, Bartosz Hawelka, Lada Rudikova, Alexander Kurbatski, Carlo Ratti / International Journal of Geographical Information Science. – 2017. – Volume 31. – P. 1381–1402.

10. **Белый, А. Б.** Данные сервиса Flickr и структура сообществ стран // А. Б. Белый, Л. В. Рудикова, С. Л. Соболевский, А. Н. Курбацкий / Международный конгресс п оинформатике: информационные системы и технологии = International Congress on Computer Sciens : Information Systems and Technologies : материалы Междунар. науч. конгресса, Минск, 24 окт.27 нояб. 2016 г. / БГУ; редкол.: С. В. Абламейко (отв. ред.) [и др.]. – Минск, 2016. – С. 851–855.

11. **Рудикова, Л. В.** О разработке системы для поддержки лазерной экспрессной экспертизы: монография / Л. В. Рудикова. – LAP LAMBERT Academic Publishing, 2014. – 134 с.

12. **Барсегян, А. А.** Методы и модели анализа данных: OLAP и DataMining / А. А. Барсегян, М. С. Куприянов, В. В. Степаненко, И. И. Холод. – СПб.: БХВ-Петербург, 2009. – 336 с.: ил.

13. **Паклин, Н. Б.** Бизнес-аналитика: от данных к знаниям / Н. Б. Паклин, В. И. Орешков. – СПб.: Питер, 2009. – 624 с.

14. **United** Nations [Electronic resource]. – Mode of access: [http://www.tandfonline.com/doi/full/10.1080/13658816.2017.1301455]. – Date of access: [14.02.2018].

15. **Eurostat** [Electronic resource]. – Mode of access: [www.ec.europa.eu/eurostat]. – Date of access: [14.02.2018].

16. **Национальный** статистический комитет Республики Беларусь [Электронный ресурс]. – Режим доступа: [www.ec.europa.eu/eurostat]. – Дата доступа: [14.02.2018].

17. **Алгоритм** Бойера-Мура // Университет ИТМО [Электронный ресурс]. – Режим доступа: [https://neerc.ifmo.ru/wiki/index.php?title=%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC_%D0%91%D0%BE%D0%B9%D0%B5%D1%80%D0%B0-%D0%9C%D1%83%D1%80%D0%B0]. – Дата доступа: [14.02.2018].

REFERENCES

1. **Ratti, C.** Redrawing the map of Great Britain from a network of human interactions // C. Ratti, S. Sobolevsky, F. Calabrese, C. Andris, J. Reades, M. Martino, R. Claxton, S. Strogatz / PloS ONE. – 2010. – V. 5, № 12. – P. 14248.

2. **Hawelka, B.** Geo-located Twitter as proxy for global mobility pattern // B. Hawelka, I. Sitko, E. Beinat, S. Sobolevsky, P. Kazakopoulos, C. Ratti / Cartography and Geographic Information Science. – 2014. – V. 41, № 3. – P. 260–271.

3. **Pei, T.** A new insight into land use classification based on aggregated mobile phone data // T. Pei, S. Sobolevsky, C. Ratti, S. L. Shaw, T. Li, C. Zhou / International Journal of Geographical Information Science. – 2014. – V. 289, № 9. – P. 1988–2007.

4. **Santi, P.** Quantifying the benefits of vehicle pooling with shareability networks // P. Santi, G. Resta, M. Szell, S. Sobolevsky, S. H. Strogatz, C. Ratti / Proceedings of the National Academy of Sciences. – 2014. – V. 111, № 37. – P. 13290–13294.

5. **Hashemian, B.** Socioeconomic characterization of regions through the lens of individual financial transactions // B. Hashemian, E. Massaro, I. Bojic, J. M. Arias, S. Sobolevsky, C. Ratti / PloS ONE. – 2017. – V. 12, № 11. – P. 0187031.

6. **Bojic, I.** Scaling of foreign attractiveness for countries and states // I. Bojic, A. Belyi,, C. Ratti, S. Sobolevsky / Applied Geography. – 2016. – № 73. – P. 47–52.

7. **Rudikova, L. V.** On the general architecture of a universal data storage and processing system of practice-oriented orientation. Rudikova / System Analysis and Applied Informatics. – Mn.: BNTU, 2017. – № 2. – P. 12–19.

8. **Rudikova, L. V.** On modeling data of subject-areas of practice-oriented orientation for a universal system of data warehousing and data processing // L. V. Rudikova, E. V. Zhavnerko / System Analysis and Applied Informatics. – Mn.: BNTU, 2017. – № 3. – P. 19–26.

9. **Belyi, A.** Global multi-layer network of human mobility // Alexander Belyi, Iva Bojic, Stanislav Sobolevsky, Izabela Sitko, Bartosz Hawelka, Lada Rudikova, Alexander Kurbatski, Carlo Ratti / International Journal of Geographical Information Science. – 2017. – Vol. 31. – P. 1381–1402.

10. **Belyi, A. B.** Flickr service data and community structure of countries / A. B. Belyi, L. V. Rudikova, S. L. Sobolevsky, A. N. Kurbatski // International Congress on Computer Sciens: Information Systems and Technologies: materials of International Scientific Congress, Republic of Belarus, Minsk, 24 October. – 27 Nov. 2016. / BSU; rare: S. V. Ablameiko (editorial editors) [and others]. – Minsk, 2016. – P. 851–855.

11. **Rudikova, L.** About laser express expertise system implementation. Monography / Lada Rudikova. – LAP LAMBERT Academic Publishing, 2014. – 134 p.

12. **Barseghyan, A.** Methods and analysis data models: OLAP and DataMining / A. Barseghyan, M. Kupriyanov, V. Stepanenko, I. Kholod – StP.: BHV-Petersburg, 2009. – 336 p.: il.

13. Paklin, N. Business-analytics: from data to knowledge / N. Paklin, V. Oreshkov. – StP.: Piter, 2009. – 624 p.

14. **United** Nations [Electronic resource]. – Mode of access: [http://www.tandfonline.com/doi/full/10.1080/13658816.2017.1301455]. – Date of access: [14.02.2018].

15. Eurostat [Electronic resource]. – Mode of access: [www.ec.europa.eu/eurostat]. – Date of access: [14.02.2018].

16. **National** Statistical Committee of the Republic of Belarus [Electronic resource]. – Mode of access: [www.ec.europa.eu/eurostat]. – Date of access: [14.02.2018].

17. **Algorithm** Boyer-Moore // University ITMO [Electronic resource]. – Mode of access: [https://neerc.ifmo.ru/wiki/index.php?title=%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC_%D0%91%D0%BE%D0%B9%D0%B5%D1%80%D0%B0-%D0%9C%D1%83%D1%80%D0%B0]. – Date of access: [14.02.2018].

Поступила	*После доработки*	*Принята к печати*
22.03.2018	*05.05.2018*	*01.06.2018*

Rudikova L. V., Danilchik V. V.

ON THE CREATION OF THE AUTOMATION SYSTEM RELATED TO SOCIAL-ECONOMIC MOVEMENTS OF PEOPLE

Yanka Kupala State University of Grodno

Nowadays, it is considerable to develop a general concept and implement a system for storing and analyzing data related to socio-economic displacements of people. The population movement, related to long-term and short-term migrations, has an increasing nature, which directly affects the various fields of activity in a single country and the world community as a whole. The proposed article describes the subject area associated with socio-economic displacements of people, the key features of internal and external migrations are noted. Based on the subject area, the general architecture of the universal system of data storage and processing is proposed, which is based on the client-server architecture. A fragment of the data model, associated with the accumulation of data from external sources, is provided. General approaches of algorithms and data structures usage are proposed. The system architecture is described with the possibility of scaling both vertical and horizontal.

The proposed system organizes the process of searching for data and filling the database from third-party sources. To do this, a module for collecting and converting information from third-party Internet sources and sending them to the database has developed. In the paper is noted the feature of the client application, which provides a convenient interface for analyzing data in the form of diagrams, graphs, maps, etc. The system is intended for various users interested in analyzing economic and social transfers, for example, to tourist organizations wishing to obtain statistics for a certain time, to airlines which could plan flights in one direction or another, as well as for state structures with the purpose of analyzing the migration flows of the population and developing appropriate strategy for their regulation.

Keywords: *web-system, socio-economic migration, data model, general architecture, Boyer-Moore algorithm; client-server; analysis subsystem*

Рудикова Лада Владимировна
Ул. Ожешко. 22, 212, Гродно, 230023, Беларусь
Тел. + 375 297 816 355; ГрГУ, зав. кафедрой «Современных технологий программирования», кандидат физико-математических наук

Lada Rudikova is the Head of Modern Programming Technologies Department of Yanka Kupala State University of Grodno (YKSUG). Ph. D. degree in physical and math.

The main line of her scientific researches – management theory, information systems design, databases, CASE, data mining, business intelligence. She actively participates in international conferences. She is the author of more than 280 scientific works and books related to computer technology and data processing, a technical writer of the publishing house «BHV-St. Petersburg». rudikowa@gmail.com

Данильчик Виктор Валерьевич
Ул. Ожешко. 22, 212, Гродно, 230023, Беларусь
Тел. + 375 292 836 000, EPAM Systems, Software Engineer

Viktar Danilchik is the software engineer at EPAM System. Master degree in computer science.

The main line of his scientific researches – object-oriented software design, information systems design, databases, CASE, data mining.
iesekiel@gmail.com

Результаты работы получены в процессе выполнения ГПНИ «Разработка методологии и средств построения универсальных систем хранения, обработки и анализа структурированных данных большого объема практико-ориентированной направленности» (№ гос. регистрации 20162266).

ЗАЩИТА ИНФОРМАЦИИ

INFORMATION SECURITY

УДК 512 (075.8)

В. А. ЛИПНИЦКИЙ[1], Е. В. СЕРЕДА[2]

СВОЙСТВА G-ОРБИТ ДВОЙНЫХ ОШИБОК И ИХ ИНВАРИАНТОВ В БЧХ-КОДАХ

[1]Военная академия Республики Беларусь
[2]Белорусский государственный университет информатики и радиоэлектроники

Цель работы – дальнейшее расширение сферы применения автоморфизмов кодов в методах и алгоритмах коррекции ошибок этими кодами. Эффективность данного подхода продемонстрировала разработанная на рубеже XX и XXI веков белорусской школой помехоустойчивого кодирования теория норм синдромов (ТНС). В основе теории лежит группа Г циклических сдвигов координат векторов. Под ее действием векторы-ошибок разбиваются на непересекающиеся Г-орбиты с четко очерченным спектром синдромов. Это позволило ввести в семействе БЧХ-кодов нормы синдромов, инвариантные относительно действия группы Г. Нормы синдромов явились однозначными характеристиками Г-орбит ошибок любой корректируемой совокупности, а потому стали основой перестановочных норменных методов коррекции ошибок. Перебирая не ошибки, а Г-орбиты ошибок, методы эти действуют на порядок быстрее классических синдромным методов коррекции ошибок, избавлены от громоздкой процедуры решения алгебраических уравнений в полях Галуа, легко реализуемы на ПЛИС.

В работе развивается подобная теория для группы G автоморфизмов БЧХ-кодов, получаемой добавлением к группе Г циклотомической подстановки. Проводится детальное исследование структуры G-орбит ошибок как объединения своих Г-орбит векторов-ошибок; взаимно-однозначного отражения этого строения на структуре спектра норм составляющих Г-орбит. Нормы эти, будучи связанными между собой автоморфизмом Фробениуса в поле Галуа – поле задания БЧХ-кода, составляют полный набор корней единственного неприводимого полинома. Он и является полиномиальным инвариантом своей G-орбиты. Основное внимание в работе сосредоточено на описании свойств и специфики G-орбит двойных ошибок и их полиномиальных инвариантов.

Ключевые слова: *БЧХ-коды, теория норм синдромов, автоморфизмы БЧХ-кодов, норма синдрома, синдром, полиномиальные инварианты норм синдромов.*

Введение

Белорусская алгебраическая школа в лице академиков Чунихина С. А., Супруненко Д. А., Платонова В. П. и их учеников заняла в последней четверти XX века одно из лидирующих мест в математических исследованиях, проводившихся в Советском Союзе. Весом непосредственный вклад этой школы в развитие теории групп, формаций групп, классических и алгебраических групп, ассоциативных колец и алгебр, коммутативных полей и алгебр с делением, алгебраической геометрии. Наработанный потенциал послужил побудительным мотивом для развития различных приложений алгебры, в частности, в помехоустойчивом кодировании.

Систематическое исследование в Республике Беларусь автоморфизмов линейных циклических кодов в 1996–2003 годах привело к:

- детальному описанию Г-орбит векторов-ошибок в названных кодах относительно группы Г циклических сдвигов координат векторов;
- построению адекватной картины в спектрах синдромов Г-орбит ошибок в реверсивных и БЧХ-кодах;
- разработке норм синдромов как инвариантов Г-орбит ошибок, описанию достаточно стройной системы свойств норм синдромов.

Созданная таким образом на рубеже XX и XXI веков теория норм синдромов [1–3] дала норменный метод декодирования ошибок в БЧХ-кодах, а также в реверсивных кодах, действующий на порядок быстрее иных синдромных методов, легко реализуемый на ПЛИС, отлича-

ющийся усеченностью процедуры поиска корректируемой ошибки, конструктивными возможностями расширения спектра корректируемых ошибок [2].

В семействе БЧХ-кодов нечетной длины автоморфизм Фробениуса поля Галуа – поля определения кода – порождает автоморфизмы, называемые циклотомическими подстановками. Они вместе с группой Г образуют некоммутативную группу G автоморфизмов БЧХ-кодов [2–4]. G-орбиты ошибок состоят из специальным образом взаимосвязанных Г-орбит векторов-ошибок [2, 3]. Открытие полиномиальных инвариантов G-орбит ошибок [5] создает хорошие перспективы к декодированию больших спектров ошибок. Продолжая [5], в данной работе исследуются дальнейшие свойства G-орбит ошибок и их полиномиальных инвариантов.

Немного о БЧХ-кодах. В данной работе мы имеем дело с циклическими примитивными двоичными БЧХ-кодами C длиной $n = 2^m - 1$, задаваемыми проверочными матрицами вида

$$H = [\alpha^i, \alpha^{3i}]^T, 0 \le i \le n-1, \qquad (1)$$

где α – корень примитивного неприводимого над $Z/2Z$ полинома степени m, $m \ge 3$, [2–4]. Их минимальное расстояние d равно 5 [4], что позволяет данным кодам корректировать одиночные и двойные ошибки.

Пусть инфокоммуникационная система (ИКС), основанная на БЧХ-коде С, приняла сообщение $\overline{x}$. Приемное устройство ИКС в обязательном порядке вычисляет синдром ошибок $S(\overline{x}) = H\,\overline{x}^T$. В силу формулы (1) этот синдром имеет следующую структуру:

$$S(\overline{x}) = (s_1, s_2)^T,$$

где s_1, s_2 – элементы поля Галуа $GF(2^m)$ из 2^m элементов. Условие $d = 5$ влечет попарное различие синдромов векторов-ошибок весом 1, 2. Несложно заметить, что у всех этих векторов первая компонента синдрома $s_1 \ne 0$.

Неравенство $S(\overline{x}) \ne \overline{0}$ свидетельствует о наличии ошибок в принятом сообщении: $\overline{x} = \overline{c} + \overline{e}$, где $\overline{c}$ – истинное передаваемое сообщение, $\overline{e}$ – вектор ошибок, который наложился на сообщение в процессе передачи $\overline{c}$ в канале с шумами. Поскольку $H\,\overline{c}^T = \overline{0}$, то $S(\overline{x}) = S(\overline{e})$ – зависит только от вектора-ошибки $\overline{e}$. Традиционно, координаты вектора $\overline{e}$ весом 2 находятся решением системы алгебраических уравнений:

$$\begin{cases} x + y = s_1; \\ x^3 + y^3 = s_2. \end{cases}$$

Данная система несложно преобразуется к квадратному уравнению. К сожалению, над полями Галуа характеристики 2 не существует эффективных алгоритмов решения алгебраических уравнений, а имеющиеся весьма вязки в реализации (см. [3], п. 9.2; [5], п. 2.9; [6], гл. 5).

Еще в 70-х годах XX века эксперты говорили об эффективности применения для коррекции ошибок автоморфизмов кодов. Правда, предполагалось весьма специфическое их применение – для сдвига имеющихся ошибочных разрядов в проверочное поле, где их просто можно отбросить (см. [4], п. 16.9, стр. 496–497). Внешне прозрачная идея остается нереализованной и по сей день. Тем не менее, автоморфизмы кодов нашли свое применение в помехоустойчивом кодировании, прямое и весьма успешное.

Г-орбиты ошибок, их спектры и нормы синдромов.

Группа Г состоит из степеней циклической подстановки σ, действующей на каждый вектор $\overline{x} = (x_1, x_2, ..., x_n)$ по правилу:

$$\sigma(\overline{x}) = (x_n, x_1, x_2, ..., x_{n-1}). \qquad (2)$$

Таким образом, группа Г является коммутативной циклической группой порядка n. По определению, она принадлежит группе автоморфизмов любого циклического кода длиной n, в частности, БЧХ-кодов с проверочной матрицей (1).

Для всякой вектор-ошибки $\overline{e} = (e_1, e_2, ..., e_n)$ ее Г-орбита

$$<\overline{e}>_\Gamma = <\overline{e}> = \left\{\overline{e}, \sigma(\overline{e}), ..., \sigma^{\nu-1}(\overline{e})\right\}, \qquad (3)$$

где ν – наименьшее натуральное число с условием: $\sigma^\nu(\overline{e}) = \overline{e}$. При этом ν делит n или же $\nu = n$. Во втором случае Г-орбита $<\overline{e}>$ имеет максимально возможную мощность и потому называется полной. Очевидно, в любом циклическом коде длиной $n > 1$ одиночные ошибки в количестве $C_n^1 = n$ составляют одну полную Г-орбиту. Двойные ошибки в количестве $C_n^2 = n(n-1)/2$ в циклических кодах с нечетной длиной $n = 2\mu + 1$ распределяются по $(n-1)/2 = \mu$ полным Г-орбитам $<\overline{e}_{1,2}>, <\overline{e}_{1,3}>, ..., <\overline{e}_{1,\mu+1}>$. Здесь $\overline{e}_{1,i}$ – вектор-ошибка весом 2 с единицами на первой и i-й позициях, $2 \le i \le \mu + 1$, и с нулевыми остальными координатами (детали см. в [1–3]).

Действие σ на вектор $\bar{e}$ по формуле (2) в БЧХ-коде C с проверочной матрицей (1) синхронно сопровождается столь же четким изменением синдрома: если $S(\bar{e}) = H\bar{e}^T = (s_1, s_2)^T$, то (см. [1–3])

$$S(\sigma(\bar{e})) = H\sigma(\bar{e})^T = (\alpha s_1, \alpha^3 s_2)^T. \quad (4)$$

Неравенство $s_1 \neq 0$ у синдромов ошибок весом 1, 2 влечет тот факт, что спектр синдромов каждой Г-орбиты названных векторов-ошибок имеет ту же мощность, что и сама Г-орбита, а циклическая структура этого спектра, определяемая формулой (4), адекватно соответствует циклической, «кольцевой» структуре самой Г-орбиты (формула (3)).

Равенство (4) послужило основой для определения нормы синдрома в данном коде формулой:

$$N(S(\bar{e})) = s_2 / s_1^3. \quad (5)$$

Главное достоинство этой формулы – ее постоянство на всех векторах каждой отдельно взятой Г-орбиты векторов-ошибок. Таким образом, вычисленная норма становится инвариантом, называемым нормой самой Г-орбиты.

Стройная система свойств норм синдромов (см. [3], п. 5.2), в частности, теорема 5.2 о попарном различии норм Г-орбит ошибок весом 1, 2, теорема о том, что в примитивном БЧХ-коде из равенства норм двух Г-орбит ошибок следует совпадение их спектров синдромов, послужили основой перестановочных норменных методов коррекции ошибок в рассматриваемых и более широких классах БЧХ-кодах. Основная их особенность в том, что вместо поиска ошибки с вычисленным синдромом во множестве всех исправляемых ошибок проводится поиск вычисленной нормы в списке норм декодируемых Г-орбит ошибок. Таким образом, поисковые процедуры в норменном декодере сокращаются в *n* раз быстрее по сравнению с классическими синдромными методами.

Увеличение *m* на единицу практически удваивает *n* и остальные параметры кода, включая и количество декодируемых Г-орбит ошибок. Через несколько подобных итераций это приводит к невероятному росту всех данных в прямой аналогии со знаменитой притчей о вознаграждении изобретателю шахмат. Выход – в разумном ограничении длин применяемых кодов и в применении для процедур декодирования более крупных орбит – G-орбит ошибок.

G-орбиты ошибок и их полиномиальные инварианты. Группа *G* некоммутативна, имеет порядок *mn*, получается присоединением к группе Г циклотомической подстановки φ, переставляющей координаты векторов *n*-мерного (*n* нечетно) пространства по правилу:

$$\varphi(i) = \begin{cases} 2i-1, & 2i-1 \le n, \\ 2i-1-n, & 2i-1 > n. \end{cases}$$

При этом подстановка φ имеет порядок *m*, $\varphi\sigma = \sigma^2\varphi$, всякую Г-орбиту $<\bar{e}>$ подстановка φ преобразует в новую Г-орбиту, поэтому для каждого вектора-ошибки $\bar{e}$ БЧХ-кода C ее G-орбита имеет вид:

$$<\bar{e}>_G = \left\{<\bar{e}>_\Gamma, \varphi(<\bar{e}>_\Gamma), ..., \varphi^{\mu-1}(<\bar{e}>_\Gamma)\right\}, \quad (6)$$

где μ – наименьшее натуральное число с условием: $\varphi^\mu(<\bar{e}>_\Gamma) = <\bar{e}>_\Gamma$. При этом μ делит *m* или же $\mu = m$. Во втором случае *G*-орбита $<\bar{e}>_G$ называется полной при условии, что и Г-орбита $<\bar{e}>_\Gamma$ – полная. Циклотомическая подстановка замечательна следующим свойством: если синдром $S(\bar{e}) = H\bar{e}^T = (s_1, s_2)^T$, а норма синдрома $N(S(\bar{e})) = s_2/s_1^3 = N$, то $S(\varphi(\bar{e})) = (s_1^2, s_2^2)^T$, $N(S(\varphi(\bar{e}))) = N^2$ (детали см. в [2], гл. 3, 4 или же в [3], гл. 4, 5). Повторное применение подстановки φ к вектору-ошибке приведет к повторному возведению в квадрат ее синдрома и нормы синдрома. Таким образом, вся *G*-орбита $<\bar{e}>_G$, построенная по формуле (6) как цикл, «круг» переходящих друг в друга Г-орбит, имеет синхронный и адекватный образ в спектре норм этих Г-орбит в виде 2-примарной последовательности норм:

$$\{N, N^2, ..., N^{2^{\mu-1}}\}, \text{ где } N^{2^\mu} = N. \quad (7)$$

Теорема 1. *Между циклом Г-орбит, составляющих G-орбиту* $<\bar{e}>_G$ *по формуле (6), и циклом их норм, составленном по формуле (7), существует взаимно однозначное соответствие. G-орбита* $<\bar{e}>_G$ *является неполной и состоит из* $\mu < m$ *Г-орбит тогда и только тогда, когда* $GF(2^\mu)$ *– наименьшее подполе поля* $GF(2^m)$, μ *делит m, содержащее норму N.*

Доказательство. Первая часть утверждения обоснована выше. Собственно, циклотомическая подстановка так и определяется, чтобы ее действие на вектор ошибок сопровождался возведением ее синдрома в квадрат. Как известно, отображение $f: x \to x^2$ в любом поле Галуа $GF(2^m)$ характеристики 2 есть не что иное, как автоморфизм Фробениуса в этом поле – образу-

ющая группы Галуа поля $GF(2^m)$ над своим подполем $Z/2Z$. Поэтому множество $N, N^2, ..., N^{2^{\mu-1}}$ при наименьшем натуральном μ с условием $N^{2^\mu} = N$ является полной системой элементов, сопряженных с N. Тогда полином $p_\mu(N, x) = p(x) = (x - N)(x - N^2)...(x - N^{2^{\mu-1}})$ имеет коэффициенты, определяемые теоремой Виета и, следовательно, инвариантные относительно действия автоморфизма Фробениуса, а потому принадлежащие минимальному подполю $Z/2Z$. Минимальное подполе поля $GF(2^m)$, содержащее N, по теории расширений Галуа [7], должно быть расширением $Z/2Z$ степени μ; в противном случае элемент N должен был бы иметь менее μ сопряженных. Теорема 1 полностью доказана.

Методом от противного доказывается, что $p_\mu(N, x)$ является неприводимым над $Z/2Z$ полиномом. Следовательно, это единственный полином степени μ, содержащий все корни множества (7). Полином $p_\mu(N, x)$ называют неприводимым полиномом любого из своих корней, потому его иногда обозначают через $Irr(N^{2^i}, x)$ [7, гл. 4, 8]. В [5] этот полином авторы назвали полиномиальным инвариантом G-орбиты (6). Теорема 1 и отмеченные свойства полинома $p_\mu(N, x)$ служат полным оправданием и обоснованием такого названия.

Наиболее характерные G-орбиты ошибок и их параметры. 1. В БЧХ-коде C любой длины Г-орбита J ошибок весом 1 имеет норму $N = 1$. G-орбита одиночных ошибок совпадает с J. Поэтому полиномиальный инвариант этой G-орбиты совпадает с полиномом $x+1$.

2. Пусть у БЧХ-кода C величина $m = 2s$ – четная. Тогда $2^m - 1 = 2^{2s} - 1 = (2^s - 1)(2^s + 1)$ – делится на три: $n = 3\nu$. Вектор-ошибка весом $2\ \overline{e}_{1,\nu+1} = (1, \nu+1)$ с единицами на 1-й и ν+1-й позициях и с нулями на остальных позициях имеет компоненты синдрома: $s_1 = 1 + \alpha^\nu \neq 0$; $s_2 = 1 + (\alpha^\nu)^3 = 1 + 1 = 0$. Следовательно, $N = N(S(1, \nu + 1)) = 0$. Поскольку $\varphi((1, \nu+1)) = (1, 2\nu+1) = \sigma^{2\nu}(1, \nu+1) \in <(1, \nu+1)>$, то G-орбита $<(1, \nu+1)>_G = <(1, \nu+1)>_J$. Поэтому полиномиальный инвариант этой G-орбиты совпадает с x.

Пусть $m = 2s+1$ – нечетное. В этом случае отсутствуют Г-орбиты двойных ошибок с нулевой нормой. Действительно, согласно лемме 3.2 [2] в этом случае $n = 2^{2s+1} - 1$ не делится на 3 и поэтому возведение в куб является автоморфизмом мультипликативной группы $GF(2^{2s+1})^*$. (детали см. в п. 2.12 [7]). Отсюда следует, что столбцы подматрицы (α^{3i}) проверочной матрицы $H = (\alpha^i, \alpha^{3i})^T$ БЧХ-кода C над рассматриваемым полем попарно различны и в целом составляют в этой подматрице перестановку столбцов подматрицы (α^i). Это означает, что для всех двойных ошибок $\overline{e}$ вторая компонента их синдрома $S(\overline{e})$ в рассматриваемом БЧХ-коде $s_2 \neq 0$ и $N(S(\overline{e})) \neq 0$.

3. Пусть $m = p$ – простое, $p > 2$. Тогда поле $Z / 2Z = GF(2)$ является единственным подполем поля $GF(2^p)$. Здесь G-орбита ошибок весом 1 – единственная G-орбита ошибок весом 1, 2, совпадающая со своей Г-орбитой и с полиномиальным инвариантом $x+1$. Согласно предыдущему примеру здесь отсутствуют Г-орбиты двойных ошибок с нулевой нормой. Значит, здесь любая Г-орбита двойных ошибок J имеет норму N, отличную от нуля и от 1. Тогда норма N должна порождать поле $GF(2^p)$, а полином $Irr(N, x)$ должен иметь степень p. А это означает, что G-орбита $< J >_G$ должна быть полной. Согласно малой теореме Ферма $2^{p-1} \equiv 1 (\mathrm{mod}\ p)$, то есть $2^{p-1} - 1 = p\eta$ для подходящего целого η. Следовательно, в БЧХ-коде C над полем $GF(2^p)$ все множество из $(n - 1)/2 = (2^p - 1 - 1)/2 = 2^{p-1} - 1 = p\eta$ полных Г-орбит двойных ошибок делится на η полных G-орбит ошибок.

4. Пусть у БЧХ-кода C вновь величина $m = 2s$ – четная. Тогда поле Галуа $GF(2^m)$ содержит подполе $GF(2^2)$; в силу примера 2 величина n делится на 3; для $\nu = n/3$ и примитивного элемента $\alpha \in GF(2^m)$ степени α^ν и $\alpha^{2\nu}$ являются кубическими корнями из 1 и потому принадлежат подполю $GF(2^2)$. Если у БЧХ-кода C найдется двойная ошибка $\overline{e} = (1, i)$ с нормой синдрома $N(S(\overline{e})) = \alpha^\nu$, то тогда G-орбита $<\overline{e}>_G = \{<\overline{e}>_\Gamma, <\phi(\overline{e})>_\Gamma\}$ – состоит из двух Г-орбит со спектром норм $\{\alpha^\nu, \alpha^{2\nu}\}$. Причем такая G-орбита – единственная! Ее полиномиальным инвариантом является единственный неприводимый над $Z/2Z$ полином $x^2 + x + 1$.

Нормы Г-орбит двойных ошибок в каждом коде занимают $(n-1)/2$ значений из $n + 1$ всех возможных. Поэтому априори можно утверждать, что примерно в половине БЧХ-кодов с четным $m = 2s$ имеется одна единственная Г-орбита двойных ошибок с нормой синдрома $N(S(\overline{e})) = \alpha^\nu$, а во второй половине БЧХ-кодов таких двойных ошибок не имеется.

Непосредственные расчеты подтверждают данное предположение. При $m = 4$ и $n = 15$ такой является Г-орбита $<\overline{e}>_{\Gamma} = <(1, 7)>_{\Gamma}$. В БЧХ-коде над полем $GF(2^4)$ с примитивным элементом α-корнем полинома $x^4 + x + 1$ норма данной Г-орбиты равна $\alpha^5 = \alpha^{n/3}$. При $m = 8$ и $n = 255$ таковой является Г-орбита $<\overline{e}>_{\Gamma} = <(1, 52)>_{\Gamma}$. В БЧХ-коде над полем $GF(2^8)$ с примитивным элементом α-корнем полинома $p(x) = x^8 + x^4 + x^3 + x + 1$ норма данной Г-орбиты равна $\alpha^{85} = \alpha^{n/3}$. При $m = 12$ и $n = 4095$ таковой является Г-орбита $<\overline{e}>_{\Gamma} = <(1, 820)>_{\Gamma}$. В БЧХ-коде над полем $GF(2^{12})$ с примитивным элементом α-корнем полинома $p(x) = x^{12} + x^7 + x^4 + x^3 + 1$ норма данной Г-орбиты равна $\alpha^{1365} = \alpha^{n/3}$. При $n = 6$ и $n = 10$ таких Г-орбит не имеется.

5. В БЧХ-кодах C над полями $GF(2^m)$ с $m = 3\mu$ – делящимся на 3 и содержащими подполе $GF(2^3)$, которое определяется одним из двух неприводимых полиномов третьей степени: $x^3 + x + 1$ и $x^3 + x^2 + 1$, могут существовать одна, две или ни одной G-орбиты ошибок весом 2, состоящие в точности из трех Г-орбит. Так, при $m = 3$ и $n = 7$ все двойные ошибки укладываются в одну полную G-орбиту из трех Г-орбит; при $m = 6$ и $n = 63$ имеются в точности две G-орбиты двойных ошибок, содержащие по три Г-орбиты ошибок: $<(1, 8)>_{\Gamma}$ и $<(1, 10)>_{\Gamma}$; при $m = 9$ и $n = 511$ существует одна G-орбита, содержащая три Г-орбиты: $<(1, 74)>_{\Gamma}$; при $m = 12$ и $n = 4095$ таких G-орбит не имеется.

Заключение

Установлено взаимно-однозначное соответствие между строением G-орбит как строго фиксированного цикла Г-орбит и структурой спектра норм этих составляющих Г-орбит. Это соответствие усиливается синхронностью действия циклотомической подстановки на Г-орбиты и автоморфизма Фробениуса на нормы этих Г-орбит. Первая часть утверждения обоснована выше. Большинство G-орбит двойных ошибок являются полными, то есть содержат максимально возможное количество полных Г-орбит ошибок. Неполные G-орбиты двойных ошибок возможны только над полями Галуа $GF(2^m)$ с составным показателем m. В G-орбите может содержаться $\mu < m$ Г-орбит, только при μ делящем m, количество таких G-орбит не превосходит числа неприводимых над минимальным подполем полиномов степени μ. Наличие небольшого числа неполных G-орбит ошибок не сильно осложняет работу перестановочных декодеров на основе полиномиальных инвариантов.

ЛИТЕРАТУРА

1. **Конопелько В. К., Липницкий В. А.** Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. Монография. – Мн.: БГУИР, 2000. – 242 с. Изд. 2-е. – М.: Едиториал, УРСС 2004. – 176 с.

2. **Липницкий В. А., Конопелько В. К.** Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. – Мн.: Издательский центр БГУ, 2007. – 240 с.

3. **Липницкий В. А.** Теория норм синдромов. – Мн.: БГУИР, 2011. – 96 с.

4. **Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.** Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.

5. **Липницкий, В. А.** Полиномиальные инварианты G-орбит ошибок БЧХ-кодов и их применение. / В. А. Липницкий, Е. В. Середа // Доклады БГУИР. – 2017. – № 5(107) – С. 62 – 69.

6. **Муттер В. М.** Основы помехоустойчивой телепередачи информации – Л.: Энергоатомиздат, 1990. – 286 с.

7. **Липницкий, В. А.** Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа. – Мн.: БГУИР, 2006. – 88 с.

8. **Лиддл Р., Ниддеррайтер Г.** Конечные поля. Т.1, 2. – М.: Мир, 1988. – 882 с.

REFERENCES

1. **Konopel'ko V. K., Lipnickij V. A.** Teorija norm sindromov i perestanovochnoe dekodirovanie pomehoustojchivyh kodov. Monografija. – Mn.: BGUIR, 2000. – 242 s. Izd. 2-e. – M.: Editorial, URSS 2004. – 176 s.

2. **Lipnickij V. A., Konopel'ko V. K.** Normennoe dekodirovanie pomehoustojchivyh kodov i algebraicheskie uravnenija. – Mn.: Izdatel'skij centr BGU, 2007. – 240 s.

3. **Lipnickij V. A.** Teorija norm sindromov. – Mn.: BGUIR, 2011. – 96 s.

4. **Mak-Vil'jams F. Dzh., Slojen N. Dzh. A.** Teorija kodov, ispravljajushhih oshibki. – M.: Svjaz', 1979. – 744 s.

5. **Lipnickij, V. A.** Polinomial invariants of errors' G-orbit of BCH codes and its application / V. A. Lipnickij, E. V. Sereda // Doklady BGUIR. – 2017. – № 5(107) – S. 62–69.

6. **Mutter V. M.** Osnovy pomehoustojchivoj teleperedachi informacii – L.: Jenergoatomizdat, 1990. – 286 s.

7. **Lipnickij, V. A.** Sovremennaja prikladnaja algebra. Matematicheskie osnovy zashhity informacii ot pomeh i nesankcionirovannogo dostupa. – Mn.: BGUIR, 2006. – 88 s.

8. **Liddl R., Nidderrajter G.** Konechnye polja. T.1, 2. – M.: Mir, 1988. – 882 s.

Поступила *16.01.2018*
После доработки *10.03.2018*
Принята к печати *01.06.2018*

Lipnickij V.[1], Serada A.[2]

PROPERTIES OF GROUPS G OF DOUBLE ERRORS AND ITS INVARIANTS IN BCH CODES

[1] Military Academy of the Republic of Belarus
[2] Belarusian State University of Mathematics and Radioelectronics

The goal of the work is the further extending the scope of application of code automorthism in methods and algorithms of error correction by these codes. The effectiveness of such approach was demonstrated by norm of syndrome theory that was developed by Belarusian school of noiseless coding at the turn of the XX and XXI century. The group Γ of the cyclical shift of vector component lies at the core of the theory. Under its action The error vectors are divided into disjoint Γ-orbits with definite spectrum of syndromes. This allowed to introduce norms of syndrome of a family of BCH codes that are invariant over action of group Γ. Norms of syndrome are unique characteristic of error orbit Γ of any decoding set, hence it is the basis of permutation norm methods of error decoding. Looking over the Γ-orbits of errors not the errors these methods are faster than classic syndrome methods of error decoding, are avoided from the complex process of solving the algebraic equation in Galois field, are simply implemented.

A detailed theory for automorphism group G of BCH codes obtained by adding cyclotomic substitution to the group Γ develops in the article. The authors held a detailed study of structure of G-orbit of errors as union of orbits Γ of error vectors; one-to-one mapping of this structure on the norm structure of group Γ. These norms being interconnected by Frobenius automorphism in the Galois field – field of BCH code constitute the complete set of roots of the only irreducible polynomial. It is a polynomial invariant of its orbit G. The main focus of the work is on the description of properties and specific features of groups G of double errors and its polynomial invariants.

Keywords: *BCH code, norm of syndrome theory, BCH code automorphism, norm of syndrome, syndrome, polynomial invariants of norm of syndrome.*

Липницкий Валерий Антонович – кандидат физико-математических наук (1980), доктор технических наук (2003), профессор по кафедре математики (2004), заведующий кафедрой высшей математики УО «Военная академия Республики Беларусь». Ученик академика В. П. Платонова и профессора В. К. Конопелько. Совместно с последним разработал теорию норм синдромов – новое направление в теории и практике помехоустойчивого кодирования, развивающее эффективное применение автоморфизмов кодов для коррекции ими ошибок в телекоммуникационных системах. Автор более 300 научных работ, четырёх монографий, ряда патентов на изобретения. Область научных интересов – алгебра и ее приложения, защита информации от помех и несанкционированного доступа.

Lipnitski Valery – PhD of Physico-Mathematical Sciences (1980), Grand PhD of Engineering Sciences (2003), Full Professor (2004), Head of the Department of Higher Mathematics of the Military Academy of the Republic of Belarus, the apprentice of academician V. P. Platonov and professor V. K. Konopelko. Together with the latter was developed norm of syndrome theory – a new direction in the theory and practice of noise-immune coding, which develops an effective application of code automorphisms for correcting errors in telecommunication systems. The author of more than 300 scientific works, four monographs, a number of patents for inventions. The field of scientific interests is algebra and its applications, information security from interference and unauthorized access. valipnitski@yandex.ru

Середа Елена Владимировна – магистр технических наук (2013), аспирант кафедры защиты информации УО «Белорусский государственный университет информатики и радиоэлектроники». Область научных интересов – исследование групп автоморфизмов линейных кодов и применение автоморфизмов кодов к разработке перестановочный алгоритмов декодирования этих кодов.

Serada Alena – Master of Engineering sciences (2013), PhD student at the Department of Information Security of the Belarusian State University of Informatics and Radioelectronics. The field of scientific interests is the investigation of automorphism groups of linear codes and the application of automorphisms of codes to the development of permutational algorithms for decoding these codes. elen.vt@gmail.com

УДК 510.644

А. В. СОКОЛОВ[1], О. Н. ЖДАНОВ[2]

КЛАСС СОВЕРШЕННЫХ ТРОИЧНЫХ РЕШЕТОК

1Одесский национальный политехнический университет, Одесса, Украина
2Сибирский государственный университет науки и технологий им. академика М. Ф. Решетнева

В настоящее время совершенные алгебраические конструкции успешно применяются для синтеза систем сигналов, конструирования блочных и поточных криптоалгоритмов, для создания генераторов псевдослучайных ключевых последовательностей. Среди совершенных алгебраических конструкций значительное место занимают бент-последовательности и связанный с ними класс совершенных двоичных решеток. Бент-последовательности применяются для построения современных криптографических примитивов, а также для построения кодов постоянной амплитуды (С-кодов), используемых в технологии кодового разделения каналов. В свою очередь, совершенные двоичные решетки используются для построения корректирующих кодов, систем бифазных фазоманипулированных сигналов и многоуровневых криптографических систем. Развитие методов многозначной логики в современных информационных и коммуникационных системах привлекло внимание исследователей к усовершенствованию методов синтеза многозначных бент-последовательностей для задач криптографии и передачи информации. Новые результаты, полученные в области синтеза троичных бент-последовательностей, делают актуальной задачу изучения класса совершенных троичных решеток. В настоящей статье результаты для совершенных двоичных решеток распространяются на трехзначный случай. На основе понятия разбаланса троичной функции введено определение совершенной троичной решетки. Полный класс совершенных троичных решеток третьего порядка получен регулярным методом, минуя перебор. Так, установлено, что класс совершенных троичных решеток является объединением четырех подклассов, в каждом из которых определены соответствующие методы размножения. В работе установлена взаимосвязь между классом троичных бент-последовательностей и классом совершенных троичных решеток. Полученные результаты являются основой для внедрения совершенных троичных решеток в современные криптографические и телекоммуникационные алгоритмы.

Ключевые слова: *многозначная логика, совершенная троичная решетка, бент-последовательность.*

Введение

Развитие методов многозначной логики, происходящее в настоящее время, обуславливает появление новых подходов к криптографической защите информации. Методы многозначной логики представляют интерес и для перспективных квантовых криптоалгоритмов. Так, в работах [1, 2] предложены эффективные алгоритмы генерации псевдослучайных ключевых последовательностей на основе функций многозначной логики. К настоящему времени уже созданы такие криптографические примитивы, как S-блоки подстановки на основе функций многозначной логики, а также работоспособный блочный симметричный криптоалгоритм на их основе [3], в то время как в работе [4] предложен эффективный поточный шифр на основе недвоичных кодов Рида-Соломона.

Дальнейшее развитие криптографических методов, основанных на использовании принципов многозначной логики во многом сопряжено с исследованием совершенных алгебраических конструкций, например, таких как максимально нелинейные бент-последовательности. Теория двоичных бент-последовательностей является достаточно развитой, построению методов синтеза таких последовательностей посвящено немало работ, например, [5–7]. В двоичном случае бент-последовательности являются основой для построения алгоритмов поточного шифрования, а также блоков замен. Еще одним важным классом алгебраических конструкций являются совершенные двоичные решетки (СДР) [8]. В настоящее время они

получили распространение для построения систем бинарных фазоманипулированных сигналов для CDMA технологии и композиционных матричных криптоалгоритмов.

Как нам представляется, для дальнейшего развития криптографических методов будет полезным исследование многозначных, в первую очередь, трехзначных аналогов совершенных алгебраических конструкций.

Исследования [9] позволили установить связь между классом совершенных двоичных решеток четвертого порядка и классом бент-последовательностей практически ценной длины $N = 16$. Так, полный класс совершенных двоичных решеток (СДР) является подмножеством полного класса бент-последовательностей длины $N = 16$, в то время как для больших длин, СДР являются обособленными совершенными алгебраическими конструкциями и их связь с бент-последовательностями на сегодняшний день не установлена.

Определение 1 [10]. Совершенной двоичной решеткой называют двумерную последовательность-матрицу

$$H(N) = \left\| h_{i,j} \right\|, \quad i, j = \overline{0, N-1}, \quad h_{i,j} \in \{-1, 1\}, \quad (1)$$

имеющую двумерную периодическую автокорреляционную функцию – ДПАКФ (Цwo-dimensional periodic autocorrelation function – 2D PACF), элементы которой определяются следующим соотношением

$$R(m,n) = PACF(m,n) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} h_{i,j} h_{i+m,j+n} = \begin{cases} N^2, \text{ при } m = n = 0, \\ 0, \text{ при других } m \text{ и } n, \end{cases} \quad (2)$$

где $m, n = \overline{0, N-1}$.

Например, легко видеть, что СДР

$$H(4) = \begin{bmatrix} + & + & + & - \\ + & + & + & - \\ + & + & + & - \\ - & - & - & + \end{bmatrix}$$

имеет

$$\left\| R(m,n) \right\| = \begin{bmatrix} 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad (3)$$

где элементы $H(4)$ представлены в знаковой форме: $-1 \Rightarrow -$, $+1 \Rightarrow +$.

Практическая ценность совершенных двоичных решеток и их связь с повсеместно используемыми бент-последовательностями делают актуальной задачу обобщения данных алгебраических конструкций на многозначный случай.

Целью настоящей статьи является построение метода синтеза полного класса совершенных троичных решеток (СТР) третьего порядка.

Разбаланс функций 3-логики

Решение задачи построения СТР связано с обобщением определения СДР на случай троичной логики. Напомним основные факты для двоичного случая.

Рассмотрим последовательность $B(t)$, $t = 0, 1, ..., N-1$ из N элементов над алфавитом ± 1. Умножая последовательность $B(t)$, $t = 0, 1, ..., N-1$ на матрицу Адамара H порядка N получаем вектор $S(\omega)$, $\omega = 0, 1, ..., N-1$, который называется вектором коэффициентов преобразования Уолша-Адамара

$$S(\omega) = B(t)H, \quad (4)$$

где матрица Адамара формируется по хорошо известному рекуррентному правилу

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}, \; H_1 = [1]. \quad (5)$$

Приведем полезный для дальнейшего изложения пример. Пусть задан исходный двоичный вектор $B(t) = \{+--\}$ длины $N = 4$. Соответственно, для нахождения $S(\omega)$ мы должны использовать матрицу Адамара порядка $N = 4$

$$H = \begin{bmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{bmatrix}. \quad (6)$$

Коэффициенты преобразования Уолша-Адамара находятся умножением исходного вектора $B(t)$ на матрицу Уолша-Адамара (все вычисления проводятся над Z_2):

$$W(1) = (+1)(+1) + (-1)(+1) + (-1)(+1) + (-1)(+1) = +1 - 1 - 1 - 1;$$

$$W(2) = (+1)(+1) + (-1)(-1) + (-1)(+1) + (-1)(-1) = +1 + 1 - 1 + 1;$$

$$W(3) = (+1)(+1) + (-1)(+1) + (-1)(-1) + (-1)(-1) = +1 - 1 + 1 + 1;$$

$$W(4) = (+1)(+1) + (-1)(-1) + (-1)(-1) + (-1)(+1) = +1+1+1-1. \quad (7)$$

В результате получаем новый бинарный вектор, для которого находим сумму элементов. Эта сумма является знаковым представлением такой общепринятой [10] в теории совершенных двоичных решеток величины, как *разбаланс*

$$\Delta_{sign} = K^{(+)} - K^{(-)}, \quad (8)$$

где $K^{(+)}$ – количество элементов «+ 1», а $K^{(-)}$ – количество элементов «–1».

Аналогом преобразования Уолша-Адамара для функций многозначной логики является преобразование Виленкина-Крестенсона [11]. Пусть, например, нам задан троичный вектор $t = [z_0 \ \ z_1 \ \ z_2]$, где $z_0 = e^{j0}$, $z_1 = e^{j2\pi/3}$, $z_2 = e^{j4\pi/3}$.

Коэффициенты преобразования Виленкина-Крестенсона могут быть найдены для вектора t по следующей формуле

$$\Omega = tV', \quad (9)$$

где V – матрица Виленкина-Крестенсона порядка N, равного длине вектора t, штрих означает транспонирование.

Правило рекуррентного построения матриц Виленкина-Крестенсона любого порядка $\mu = 3^L$, $L \in N$ представлено в работах [12, 13]

$$V_{3^L} = \begin{bmatrix} V_{3^{L-1}} & V_{3^{L-1}} & V_{3^{L-1}} \\ V_{3^{L-1}} & \left(V_{3^{L-1}}+1\right) \bmod 3 & \left(V_{3^{L-1}}+2\right) \bmod 3 \\ V_{3^{L-1}} & \left(V_{3^{L-1}}+2\right) \bmod 3 & \left(V_{3^{L-1}}+1\right) \bmod 3 \end{bmatrix}. \quad (10)$$

В нашем случае матрица Виленкина-Крестенсона и матрица, комплексно-сопряженная к ней, имеют следующий вид:

$$V_3 = \begin{bmatrix} z_0 & z_0 & z_0 \\ z_0 & z_1 & z_2 \\ z_0 & z_2 & z_1 \end{bmatrix}, \ V_3' = \begin{bmatrix} z_0 & z_0 & z_0 \\ z_0 & z_2 & z_1 \\ z_0 & z_1 & z_2 \end{bmatrix}. \quad (11)$$

Рассмотрим процесс вычисления коэффициентов преобразования Виленкина-Крестенсона

$$\begin{aligned} \Omega(1) &= z_0 z_0 + z_0 z_1 + z_0 z_1; \\ \Omega(2) &= z_0 z_0 + z_1 z_1 + z_2 z_1; \\ \Omega(3) &= z_0 z_0 + z_2 z_1 + z_1 z_1. \end{aligned} \quad (12)$$

Заметим, что удобно от мультипликативной группы корней из единицы Γ_3 перейти к изоморфной ей аддитивной группе кольца Z_3 и наоборот.

Рассмотрим обобщение разбаланса на троичный случай. Пусть $|i|$ – количество элементов i.

Определение 2. Значением разбаланса Δ последовательности над алфавитом $\{0, 1, 2\} \leftrightarrow \{z_0, z_1, z_2\}$ назовем величину

$$\Delta(x) = \sqrt{\left(1 \cdot |0| - 0.5\left(|1| + |2|\right)\right)^2 + \left(\frac{\sqrt{3}}{2}|1| - \frac{\sqrt{3}}{2}|2|\right)^2}. \quad (13)$$

Запишем процедуру нахождения абсолютных значений преобразования Виленкина-Крестенсона в терминах наших определений

$$\left|\Omega_i\right| = \Delta(x \cdot vil_i) \quad (14)$$

где vil_i – i-я функция Виленкина-Крестенсона.

Продолжим рассмотрение нашего примера

$$\Omega(1) = \Delta(z_0 z_0, z_0 z_1, z_0 z_1) = \Delta(0,1,1) = \sqrt{(1 \cdot 1 - 0{,}5(2+0))^2 + \left(\frac{\sqrt{3}}{2}2 - \frac{\sqrt{3}}{2}0\right)^2} = \sqrt{3};$$

$$\Omega(2) = \Delta(z_0 z_0, z_1 z_1, z_2 z_1) = \Delta(0,2,0) = \sqrt{(1 \cdot 2 - 0{,}5(0+1))^2 + \left(\frac{\sqrt{3}}{2}0 - \frac{\sqrt{3}}{2}1\right)^2} = \sqrt{\frac{9}{4} + \frac{3}{4}} = \sqrt{3};$$

$$\Omega(3) = \Delta(z_0 z_0, z_2 z_1, z_1 z_1) = \Delta(0,0,2) = \sqrt{(1 \cdot 2 - 0{,}5(0+1))^2 + \left(\frac{\sqrt{3}}{2}0 - \frac{\sqrt{3}}{2}1\right)^2} = \sqrt{\frac{9}{4} + \frac{3}{4}} = \sqrt{3}. \quad (15)$$

Результат полностью совпадает с результатом прямого метода вычисления коэффициентов преобразования Виленкина-Крестенсона.

Аналогично определению ДПАКФ (2), введем следующее определение.

Определение 3. Периодической автокорреляционной p-функцией назовем следующую сумму

$$Kp(m,n) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} h_{i,j} h_{i+m,j+n} (\bmod p), \quad (16)$$

где $m, n = \overline{0, N-1}$.

При $p = 2$ получается классическая двумерная периодическая автокорреляционная функция.

Пример. Рассмотрим троичную бент-последовательность

$$\beta_1 = \{0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 2 \quad 0 \quad 2 \quad 1\}, \quad (17)$$

которую представим в виде матрицы третьего порядка

$$B_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix}. \quad (18)$$

Найдем для матрицы (18) соответствующие элементы матрицы $Kp(m,n)$ согласно (16)

$$Kp = \begin{bmatrix} 3 & 3 & 3 \\ 3 & 3 & 3 \\ 3 & 3 & 3 \end{bmatrix}. \quad (19)$$

Определение 4. Совершенной троичной решеткой (СТР) назовем матрицу, для которой функция $Kp(m,n)$ является постоянной $Kp(m,n) = \text{const}$ при любых значениях сдвига m и n.

В настоящей работе путем экспериментальных исследований установлено, что все существующие троичные бент-последовательности, количество которых равно $J_B = 486$ [14, 15], представленные в виде троичных матриц порядка $N = 3$, обладают равномерной матрицей $Kp(m,n)$, т.е. являются СТР.

Тем не менее существуют и другие СТР, которые не могут быть образованы из бент-последовательностей. Далее представим регулярные методы синтеза полного множества СТР порядка $N = 3$, опишем правила размножения для каждого из трех подмножеств (классов) и определим мощность множества СТР над алфавитом $\{0, 1, 2\} \leftrightarrow \{z_0, z_1, z_2\}$.

Класс 1.

СТР на основе матриц Виленкина-Крестенсона вида

$$PTA_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix}. \quad (20)$$

Правило размножения 1.1. СТР класса 1 допускают все возможные знаковые кодирования строк последовательностями длины $N = 3$.

Например, для матрицы (20) умножением каждой строки на соответствующий элемент последовательности $z = [011]$ получаем новую матрицу

$$PTA_1^{`} = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 0 & 2 \end{bmatrix}. \quad (21)$$

Всего возможных правил знакового кодирования существует $J_{11} = 3^3 = 27$.

Правило размножения 1.2. СТР класса 1 допускает все возможные перестановки строк, количество которых $J_{12} = 3! = 6$.

Таким образом, общее количестве СТР класса 1, которые могут быть построены с помощью разработанных двух правил размножения, составляет $J_1 = J_{11}J_{12} = 27 \cdot 6 = 162$.

Класс 2.

СТР вида

$$PTA_2 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 2 & 2 \end{bmatrix}. \quad (22)$$

Правило размножения 2.1. Представим исходную СТР (22) в обобщенном виде

$$PTA_2 = \begin{bmatrix} \alpha & \alpha & \beta \\ \alpha & \beta & \alpha \\ \alpha & \gamma & \gamma \end{bmatrix}, \quad (23)$$

где коэффициенты α, β, γ различны и принимают значения из множества $\{0, 1, 2\} \leftrightarrow \{z_0, z_1, z_2\}$, количество способов равно $J_{21} = 3! = 6$.

Правило размножения 2.2. Конструкция (23) СТР класса 2 допускает все возможные перестановки строк, которых существует $J_{22} = 3! = 6$.

Правило размножения 2.3. Конструкция СТР класса 2 допускает все возможные циклические сдвиги столбцов, количество сдвигов равно $J_{23} = N = 3$.

Итого, общее количество СТР, которые могут быть построены на основе правил размножения 2.1–2.3, составляет $J_2 = J_{21}J_{22}J_{23} = 6 \cdot 6 \cdot 3 = 108$.

Класс 3.

СТР вида

$$PTA_3 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 2 & 2 & 0 \end{bmatrix}. \quad (24)$$

Правило размножения 3.1. Представим исходную СТР (24) в обобщенном виде

$$PTA_3 = \begin{bmatrix} \alpha & \alpha & \beta \\ \alpha & \alpha & \beta \\ \gamma & \gamma & \alpha \end{bmatrix}, \quad (25)$$

где коэффициенты α, β, γ могут принимать значения из множества $\{0, 1, 2\} \leftrightarrow \{z_0, z_1, z_2\}$, соответственно, $J_{31} = 3! = 6$ различными способами.

Правило размножения 3.2. Для СТР третьего класса вида (24) допустимы перестановки строк и столбцов из полного множества перестановок, тем не менее, только перестановки вида

$$P = \begin{cases} 1 & 2 & 3; \\ 1 & 3 & 2; \\ 3 & 1 & 2, \end{cases} \qquad (26)$$

не приводят к появлению повторяющихся структур.

Таким образом, общее количество перестановок строк и столбцов равно $J_{32} = 3 \cdot 3 = 9$.

Итого, применяя к СТР третьего класса правила размножения 3.1, 3.2, можно получить $J_3 = J_{31} J_{32} = 6 \cdot 9 = 54$ различных СТР.

Класс 4.

Решетки, состоящие из 4 символов α, 4-х символов β и одного символа γ, где $\alpha, \beta, \gamma \in \{0, 1, 2\}$. Например,

$$PTA_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 2 \end{bmatrix}. \qquad (27)$$

Синтез данных решеток происходит следующим образом.

Шаг 1. Рассмотрим матрицу 3-го порядка, заполненную элементами α.

$$\begin{bmatrix} \alpha & \alpha & \alpha \\ \alpha & \alpha & \alpha \\ \alpha & \alpha & \alpha \end{bmatrix}. \qquad (28)$$

Шаг 2. Один элемент γ мы можем разместить в ней $C_9^1 = 9$ различными способами. Данный шаг позволяет создать 9 различных матриц.

Шаг 3. Четыре элемента β могут быть размещены $C_8^4 = 70$ различными способами. Данный шаг позволяет создать 70 различных матриц.

Шаг 4. К полученным решеткам прибавить значения из множества $\{0, 1, 2\}$ по mod 3. Данный шаг позволяет создать 3 различные матрицы из одной.

Итого, предложенный метод позволяет сгенерировать $J_4 = 9 \cdot 70 \cdot 3 = 1890$ СТР.

Таким образом, на основе описанных четырех классов СТР может быть построен полный класс мощности $J_{PTA} = J_1 + J_2 + J_3 + J_4 = 162 + 108 + 54 + 1890 = 2214$.

Выводы

Отметим основные результаты проведенных исследований:

1. Введено определение совершенных троичных решеток, которое является обобщением совершенных двоичных решеток на случай троичной логики.

2. Полный класс совершенных троичных решеток третьего порядка построен регулярными методами. Проведена классификация полного множества совершенных троичных решеток на четыре класса и описаны правила размножения для каждого из них.

3. Введено определение разбаланса троичной последовательности, которое может быть использовано как основа дальнейших исследований совершенных алгебраических конструкций многозначной логики.

Отметим, что полученные результаты ставят новые актуальные задачи, среди которых особо выделим следующие:

– нахождение порядков матриц над алфавитом $\{0, 1, 2\} \leftrightarrow \{z_0, z_1, z_2\}$, для которых существуют совершенные троичные решетки;

– разработка рекуррентных методов синтеза совершенных троичных решеток;

– установление связи между классами бент-последовательностей длин L больше 9 и совершенных троичных решеток;

– разработка методов синтеза матриц Виленкина-Крестенсона на основе совершенных троичных решеток;

– разработка методов синтеза сигнальных и криптографических конструкций на основе совершенных троичных решеток.

ЛИТЕРАТУРА

1. **Гнатюк, С. О.** Метод оцінювання якості тритових псевдовипадкових послідовностей для криптографічних застосувань / С. О. Гнатюк, Т. О. Жмурко, В. М. Кінзерявий, Н. А. Сейлова. – Information Technology and Security, 2015. – Т. 3. – № 2(5). – С. 108–116.

2. **Соколов, А. В.** Генератор псевдослучайных ключевых последовательностей на основе тройственных наборов бент-функций / А. В. Соколов, О. Н. Жданов, Н. А. Барабанов. – Проблемы физики, математики и техники, 2016. – № 1(26). – С. 85–91.

3. **Zhdanov, O. N.** Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic / O. N. Zhdanov, A. V. Sokolov. – Far East Journal of Electronics and Communications, 2016. – Vol. 16, No. 3. – P. 573–589.

4. **Tao, Wu.** Stream cipher by reed-solomon code / Wu Tao, Wang Ruomei. – Information and Communication Technology Convergence (ICTC), 2017. – P. 422–427.

5. **Токарева, Н. Н.** Бент-функции: результаты и приложения. Обзор работ / Н. Н. Токарева // Приклад. дискрет. математика. – Томск, 2009. – Сер. № 1(3). – С. 15–37.

6. **Mesnager, S.** Several New Infinite Families of Bent Functions and Their Duals / S. Mesnager.— IEEE Transactions on Information Theory, 2014. – Vol. 60. – No. 7. – P. 4397–4407.

7. **Qingshu, Meng.** A novel algorithm enumerating bent functions / Qingshu Meng, Min Yang, Huanguo Zhang, Jingsong Cui. – Discrete Mathematics, 2008. – Vol. 308. – Issue 23. – P. 5576–5584.

8. **Kopilovich, L. E.** On perfect binary arrays / L. E. Kopilovich. – Electronics Letters, 1988. —Vol. 24. – No. 9. – P. 566–567.

9. **Мазурков, М. И.** Регулярные привила построения полного класса бент-последовательностей длины 16 / М. И. Мазурков, А. В. Соколов. – Труды ОНПУ. – 2013. – № 2(41). – С. 231–237.

10. **Wild P.** Infinite families of perfect binary arrays / P. Wild. – Electron. Lett, 1988. – Vol. 24. – No. 14. – P. 845–847.

11. **Трахтман, А. М.** Основы теории дискретных сигналов на конечных интервалах / А. М. Трахтман, В. А. Трахтман. – М.: Сов.радио, 1975. – 208 с.

12. **Stankovic, R. S.** Representation of Multiple-Valued Logic Functions / R. S. Stankovic, J. T. Astola, C. Moraga. – Morgan & Claypool Publishers, Synthesis lectures on digital circuits and systems, 2012. – p. 170.

13. **Соколов, А. В.** Методы синтеза алгебраической нормальной формы функций многозначной логики / А. В. Соколов, О. Н. Жданов, А. О. Айвазян. – Системный анализ и прикладная информатика, 2016. – № 1. – С. 69–76.

14. **Мазурков, М.** Метод синтеза бент-последовательностей в базисе Виленкина-Крестенсона / М. И. Мазурков, А. В. Соколов, Н. А. Барабанов // Известия высших учебных заведений. Радиоэлектроника. – 2016. – Т. 59, N 11. – С. 47–55.

15. **Sokolov, A. V.** Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties / A. V. Sokolov, O. N. Zhdanov. – Journal of Telecommunication, Electronic and Computer Engineering. – Vol. 8. – No. 9. – P. 39–43.

REFERENCES

1. **Hnatiuk, S. O.** Method for quality evaluation of trit pseudorandom sequence to cryptographic applications / S. O. Hnatiuk, T. O. Zhmurko, V. N. Kinzeriavyi, N. A. Seilova. – Information Technology and Security, 2015. – Vol. 3. – No. 2(5). – C. 108–116.

2. **Sokolov, A. V.** Pseudo-random key sequence generator based on triple sets of bent-functions / A. V. Sokolov, O. N. Zhdanov, N. A. Barabanov. – Problems of physics, mathematics and technics, 2016. – No. 1(26). – P. 85–91.

3. **Zhdanov, O. N.** Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic / O. N. Zhdanov, A. V. Sokolov. – Far East Journal of Electronics and Communications, 2016. – Vol. 16, No. 3. – P. 573–589.

4. **Tao, Wu.** Stream cipher by reed-solomon code / Wu Tao, Wang Ruomei. – Information and Communication Technology Convergence (ICTC), 2017. – P. 422–427.

5. **Tokareva, N. N.** Bent functions: results and applications. Survey of works / N. N. Tokareva. – Applied Discrete Mathematics. – Tomsk, 2009. – Ser. № 1(3). – P. 15–37.

6. **Mesnager, S.** Several New Infinite Families of Bent Functions and Their Duals / S. Mesnager.— IEEE Transactions on Information Theory, 2014. – Vol. 60. – No. 7. – P. 4397–4407.

7. **Qingshu, Meng.** A novel algorithm enumerating bent functions / Qingshu Meng, Min Yang, Huanguo Zhang, Jingsong Cui. – Discrete Mathematics, 2008. – Vol. 308. – Issue 23. – P. 5576–5584.

8. **Kopilovich, L. E.** On perfect binary arrays / L. E. Kopilovich. – Electronics Letters, 1988. —Vol. 24. – No. 9. – P. 566–567.

9. **Mazurkov, M. I.** The regular rules of constructing the complete class of bent-sequences of length 16 / M. I. Mazurkov, A. V. Sokolov. – Proceedings of ONPU, 2013. – No. 2(41). – P.231–237.

10. **Wild P.** Infinite families of perfect binary arrays / P. Wild. – Electron. Lett, 1988. – Vol. 24. – No. 14. – P. 845–847.

11. **Trakhtman, A. M.** Fundamentals of the theory of discrete signals on finite intervals / A. M. Trakhtman, V. A. Trachtman. – Moscow: Sov. radio, 1975. – p. 208.

12. **Stankovic, R. S.** Representation of Multiple-Valued Logic Functions / R. S. Stankovic, J. T. Astola, C. Moraga. – Morgan & Claypool Publishers, Synthesis lectures on digital circuits and systems, 2012. – p. 170.

13. **Sokolov, A. V.** Synthesis methods of algebraic normal form of many-valued logic functions / A. V. Sokolov, O. N. Zhdanov, A. O. Ayvazyan. – System analysis and applied information science, 2016. – No. 1. – P. 69–76.

14. **Mazurkov, M. I.** Synthesis method for bent sequences in the Vilenkin-Chrestenson basis / M. I. Mazurkov, A. V. Sokolov, N. A. Barabanov. – Radioelectronics and Communications Systems, 2016. – Vol. 59. – No. 11. – P. 510–517.

15. **Sokolov, A. V.** Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties / A. V. Sokolov, O. N. Zhdanov. – Journal of Telecommunication, Electronic and Computer Engineering. – Vol. 8. – No. 9. – P. 39–43.

Поступила	*После доработки*	*Принята к печати*
20.11.2017	23.02.2018	01.06.2018

Sokolov A. V., Zhdanov O. N.
radiosquid@gmail.com

THE CLASS OF PERFECT TERNARY ARRAYS

In recent decades, perfect algebraic constructions are successfully being use to signal systems synthesis, to construct block and stream cryptographic algorithms, to create pseudo-random sequence generators as well as in many other fields of science and technology. Among perfect algebraic constructions a significant place is occupied by bent-sequences and the class of perfect binary arrays associated with them. Bent-sequences are used for development of modern cryptographic primitives, as well as for constructing constant amplitude codes (C-codes) used in code division multiple access technology. In turn, per-fect binary arrays are used for constructing correction codes, systems of biphase phase-shifted signals and multi-level cryp-tographic systems. The development of methods of many-valued logic in modern information and communication systems has attracted the attention of researchers to the improvement of methods for synthesizing many-valued bent-sequences for cryptog-raphy and information transmission tasks. The new results obtained in the field of the synthesis of ternary bent-sequences, make actual the problem of researching the class of perfect ternary arrays. In this paper we consider the problem of extending the definition of perfect binary arrays to three-valued logic case, as a result of which the definition of a perfect ternary array was introduced on the basis of the determination of the unbalance of the ternary function. A complete class of perfect ternary arrays of the third order is obtained by a regular method, bypassing the search. Thus, it is established that the class of perfect ternary arrays is a union of four subclasses, in each of which the corresponding methods of reproduction are determined. The paper establishes the relationship between the class of ternary bent-sequences and the class of perfect ternary arrays. The obtained results are the basis for the introduction of perfect ternary arrays into modern cryptographic and telecommunication algorithms.

Keywords: *many-valued logic, perfect ternary array, bent-sequence.*

Соколов Артем, кандидат технических наук, старший преподаватель кафедры Информатики и управления защитой информационных систем Одесского национального политехнического университета. Является автором монографии и более 80 научных публикаций. Научные интересы включают в себя методы защиты информации на основе совершенных алгебраических конструкций, методы синтеза алгоритмов шифрования данных и нелинейных S-блоков.

Artem V. Sokolov was born in Odessa, USSR, in 1990. He received a Bachelor (Hons) degree in systems of technical data protection in 2011, Master (Hons) degree in systems of technical data protection and automation of it's processing in 2013 and Ph. D. degree in data protection systems in 2014 from Odessa National Polytechnic University, Odessa, Ukraine.

From 2012 to 2014 he was a Junior Researcher of the Data Security department in Odessa National Polytechnic University. From 2014 to 2017 he was a Senior Lecturer of the Data Security department in Odessa National Polytechnic University. Since 2017 he is a Senior Lecturer of the department of Informatics and control of information systems protection in Odessa National Polytechnic University. He is the author of a book and more than 80 articles. His research interests include data protection methods based on perfect algebraic constructions, nonlinear S-box synthesis methods, and stream encryption algorithms.

A. V. Sokolov awards and honors include: Gold Medal for high achievements in education, Hons Diploma of Winner in Master Competition, 2013; winner of «Information and communication networks» Ukrainian competition of research papers, 2012; Diploma for excellent academic and research activities, 2010.

Жданов Олег Николаевич, доцент кафедры безопасности информационных технологий Сибирского государственного университета науки и технологий им. академика М. Ф. Решетнева. Общее количество публикаций 75.

Сфера научных интересов: системы дифференциальных уравнений в частных производных, являющиеся моделями процессов в механике сплошных сред, защита информации.

Zhdanov Oleg Nikolaevich was born on April 16, 1964. He graduated from Krasnoyarsk State University in 1986. The Ph. D. thesis in mathematical analysis

was defended in 1994. At the moment O. N. Zhdanov is Associate Professor of Informational Technologies subdepartment of Siberian State University of Science and Technology named after Academician M. F. Reshetnev and associate professor of Algebra and mathematical logic department of Siberian Federal university.

O. N. Zhdanov gives the following lecture courses: «Cryptographic methods of information security» (there is a certificate of Institute of Cryptography, Communication and Information Sciences of the corresponding advanced training), «Number-theoretic algorithms of cryptography», «Reliability theory».

The total number of his publications is 75. Eight of them are study guides.

Together with pupils, he developed a key information choice method for realization of block encryption algorithms. Together with Chalkin T. A. he received the copyright certificate on the program complex realizing the choice of key information for data encryption according to the current standard of Russia.

O. N. Zhanov was awarded by a letter of thanks from Legislative Assembly of Krasnoyarsk Krai, a breastplate of the Ministry of Education and Science of the Russian Federation «For development of students research activity».

Уважаемые авторы,

Общими критериями для публикации статей в журнале являются актуальность, новизна материала и его ценность в теоретическом и/или прикладном аспектах.

С целью приведения элементов данных, содержащихся в журнале, в соответствие международным требованиям зарубежных аналитических информационных систем (индексов цитирования), используемых для оценки деятельности учреждений образования при расчете показателей в международных рейтингах университетов, редколлегия журнала предлагает руководствоваться Правилами в приведенной ниже редакции приближения к унифицированной системе цитирования научных публикаций SCOPUS,

С 2016 г. Редколлегия журнала предлагает руководствоваться Правилами в приведенной ниже редакции.

Правила для авторов

1. Общие требования

Материалы статей представляются на бумажном носителе (в двух экз.) по адресу: 220013, Минск, ул. Ф. Скорины, 25/3, корп. 20, каб. 508 (Петренко Юрий Николаевич) и в электронном виде e-mail: CA_PI@bntu.by. Телефон для справок: (017) 266 26 58.

Статья, представляемая на бумажном носителе, должна быть подписана всеми авторами. К статье прилагаются сведения об авторах: фамилия, имя, отчество полностью, почтовый адрес, телефоны, адрес электронной почты, место работы, ученая степень и звание, должность. При наличии нескольких авторов должен быть указан автор, ответственный за переписку.

Статьи, поступившие в редакцию журнала, регистрируются в установленном порядке. Статьи, оформленные с нарушением приведенных правил, к рассмотрению редакцией не принимаются. Принятые статьи рецензируются.

При положительной рецензии статья предлагается к опубликованию.

Редакция не принимает статьи, опубликованные ранее в других журналах или научных изданиях.

Гонорар автору за публикацию статьи не выплачивается. Материалы, присланные в редакцию, авторам не возвращаются.

2. Правила оформления статей

2.1. Объем статей (с иллюстрациями) не должен превышать:

• для оригинальной статьи – 7 страниц (не более 8 иллюстраций);

• для краткого сообщения – 3 страниц (не более 2 иллюстраций).

Статья должна быть набрана с помощью текстового редактора Microsoft Word 2007.

Параметры страницы: формат А4 (высота 29,7 см., ширина – 21 см.); отступ для левого поля и поля сверху – 25 мм, правого и нижнего – 20 мм; нумерация страниц сверху в колонтитуле, со второй страницы, с выравниванием по правому краю.

Текст набирается шрифтом TimesNewRoman, 12 пт. Межстрочный интервал – полуторный. Абзацный отступ – 12 мм.

2.2. Индекс УДК набирается шрифтом TimesNewRoman, 12 пт, все прописные, выравнивание – по правому краю.

2.3. Фамилия и инициалы автора (авторов) в именительном падеже, должность, ученая степень и ученое звание печатаются шрифтом TimesNewRoman, 12 пт, курсив, выравнивание – по левому краю.

2.4. Название статьи набирается шрифтом Arial, 12 пт, жирный, все прописные, выравнивание – по центру.

2.5. Полное название организации (организаций), в которой работает (учится) автор (авторы) набирается шрифтом TimesNewRoman, 12 пт, выравнивается по центру, После названия организации пропускается две строки, далее следует адрес (адреса) электронной почты, пропускается две строки.

2.6. Аннотация и ключевые слова (объем 200–250 слов на русском (англ.) языке статьи набирается шрифтом TimesNewRoman, 10 пт, межстрочный интервал 1,15 пт, курсив, выравнивается по центру. Аннотация должна содержать (рекомендованная структура): цель и задачи работы, методы исследований, ре-

зультаты, выводы. Аннотация должна быть пригодна для опубликования отдельно от статьи. Английский вариант не должен быть механическим переводом русского текста, а обеспечивать понимание сути работы для иностранных читателей;

После аннотации пропускается одна строка.

2.7. Текст статьи (набирается шрифтом TimesNewRoman, 12 пт, с абзацем, выравнивание – по ширине) должен содержать следующие элементы:

1) *введение* (может содержать: краткий обзор литературы по проблеме исследования, перечисление нерешенных ранее вопросов, постановку проблемы, цель исследований). Слово «Введение» печатается шрифтом TimesNewRoman, 12 пт, жирный, выравнивание – по левому краю.

2) *основная часть исследования* (возможно деление на подразделы), включающая графики и другой иллюстративный материал (при их наличии), при этом таблицы и рисунки не должны дублировать друг друга. Название каждого подраздела статьи печатается шрифтом TimesNewRoman, 12 пт, жирный, выравнивание – по левому краю.

3) *Заключение* (формулируются основные полученные результаты с указанием их новизны, преимуществ по сравнению с аналогами). Слово «Заключение» печатается шрифтом TimesNewRoman, 12 пт, жирный, выравнивание – по левому краю.

2.8. *Литература*. Список литературы оформляется шрифтом TimesNewRoman, 12 пт в соответствии с Инструкцией по оформлению диссертации, автореферата и публикаций по теме диссертации, утвержденной постановлением президиума Государственного высшего аттестационного комитета Республики Беларусь 24.12.1997 № 178 (в редакции постановления ВАК Беларуси от 22.02.2006 № 2). www.edu.grsu.by/files/liter.doc.

Слово «Литература» печатается шрифтом TimesNewRoman, 12 пт, все прописные, выравнивание – по левому краю.

Источники должны располагаться в порядке цитирования в тексте. Порядковые номера ссылок в тексте должны быть написаны внутри квадратных скобок (например: [1], [2]).

В статьях на русском языке должно быть до 10 источников, включая статьи из международных журналов, а также ссылки на собственные исследования. В англоязычных статьях должно быть до 30 источников, включая статьи из международных журналов, а также ссылки на собственные исследования. Обзорные статьи должны включать до 50 ссылок, включая статьи из международных журналов, а также ссылки на собственные исследования.

Список источников должен оформляться на русском и английском языках.

С целью повышения цитирования авторов в журнале проводится транслитерация русскоязычных источников с использованием официальных кодировок в следующем порядке: имена авторов транслитерируются латиницей, название статьи – смысловой транслитерацией (перевод на английский язык), название источника, где опубликована работа, транслитерируется латиницей, если у источника (журнала) нет официального названия на английском языке).

Для удобства транслитерации возможно использование онлайн-сервисов: http://www.translit.ru.

Все русскоязычные источники литературы должны быть представлены в транслитерированном варианте. За правильность приведенных в списке литературы данных ответственность несут автор(ы). В списке должны иметь место ссылки на издания, включенные в международные базы цитирования Scopus и Web of Science).

2.9. *После списка литературы* на русском и английском языках в статье на русском (англ.) языке должно следовать название статьи, список авторов, сведения о них и аннотация на английском (русском) языке.

Далее указывается: грант, гос. программа, тема госбюджетной НИР (№ Гос. регистрации) или иной документ, в рамках которой выполнена работа (или инициативная).

2.10. *Резюме авторов* (шрифтом TimesNewRoman, 10 пт.,) сопровождается фотографией (3×4 см.), JPG.

2.11. *Оформление формул.* Только сложные формулы должны быть набраны с помощью встроенного в MS Word редактора формул Equation. Просто буквы с индексами могут быть набраны без использования формульного редактора с помощью средств оформления MS Word. Латинские символы должны быть набраны курсивом, как в формулах, так и на рисунках, и в тексте, а русские и греческие – обычным текстом.

В редакторе формул должен быть установлен следующий размер символов: обычный символ – 11 пт., крупный индекс – 7 пт., мелкий индекс – 5 пт., крупный символ – 17 пт., мелкий символ – 12 пт. Формулы выравниваются по центру страницы. При необходимости делать ссылки на формулы их следует нумеровать арабскими цифрами, помещенными в круглые скобки, в порядке упоминания. Номера формул выравниваются по правому краю страницы.