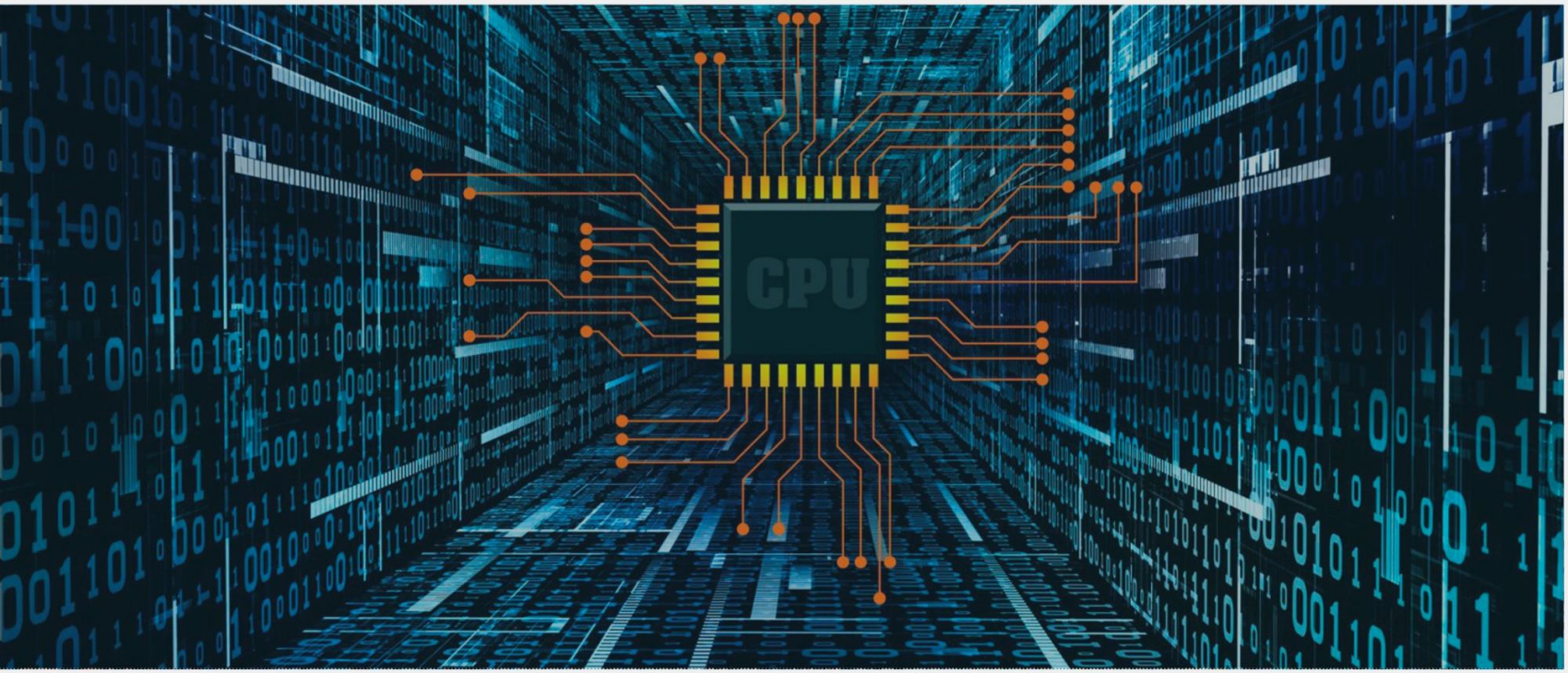
Материалы научно-технического семинара МИНСК

ЦИФРОВАЯ ОБРАБОТКА СИГНАЛОВ И ТЕОРИЯ КОДИРОВАНИЯ

26 АПРЕЛЯ
2018



ISBN 978-985-488-834-7

Научно-технический семинар
«Цифровая обработка сигналов
и теория кодирования»
приурочен к 80-летию со дня рождения
основателя белорусской школы
цифровой обработки сигналов и теории кодирования
доктора технических наук, профессора В. В. Лосева.

ЛОСЕВ ВЛАДИСЛАВ ВАЛЕНТИНОВИЧ

(28.04.1938–18.11.1990)

Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

ЦИФРОВАЯ ОБРАБОТКА СИГНАЛОВ И ТЕОРИЯ КОДИРОВАНИЯ

МАТЕРИАЛЫ НАУЧНО-ТЕХНИЧЕСКОГО СЕМИНАРА
(Минск, 26 апреля 2018 года)

DIGITAL SIGNAL PROCESSING AND THEORY OF CODING

MATERIALS OF SCIENTIFIC AND TECHNICAL SEMINAR
(Minsk, April 26, 2018)

Минск БГУИР 2018

УДК 621.391
ББК 32.811
Ц75

Ц75 **Цифровая** обработка сигналов и теория кодирования = Digital Signal Processing and Theory of Coding : материалы науч.-техн. семинара (Минск, 26 апреля 2018 года) / редкол. : В. К. Конопелько, В. Ю. Цветков, Л. А. Шичко. – Минск : БГУИР, 2018. – 88 с.

ISBN 978-985-543-428-4.

Сборник содержит статьи, в которых рассмотрен процесс становления в МРТИ в 70–80-х гг. XX века научной школы по цифровой обработке сигналов и теории кодирования. Предназначен для научных сотрудников в области ЦОС и ТК, аспирантов, магистрантов и студентов технических вузов.

Научное издание

Ответственный за выпуск *В. К. Конопелько*
Корректор *О. В. Бойправ*
Компьютерный дизайн и верстка *Е. Г. Макейчик*

Подписано в печать 26.06.2018. Формат 60×84 ⅛. Бумага офисная. Гарнитура «Таймс».
Печать цифровая. Усл. печ. л. 10,7. Уч.-изд. л. 7,6. Тираж 30 экз. Заказ 156.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
ЛП №02330/264 от 14.04.2014.
220013, Минск, П. Бровки, 6

ISBN 978-985-543-428-4

СОДЕРЖАНИЕ

CONTENTS

УДК 512 (075.8)

ПОДГОТОВКА РАДИОИНЖЕНЕРОВ ПО ЦИФРОВОЙ ОБРАБОТКЕ СИГНАЛОВ И ТЕОРИИ КОДИРОВАНИЯ В МИНСКОМ РАДИОТЕХНИЧЕСКОМ ИНСТИТУТЕ В 1968–1990 ГГ.

В.К. КОНОПЕЛЬКО, И.И. АСТРОВСКИЙ

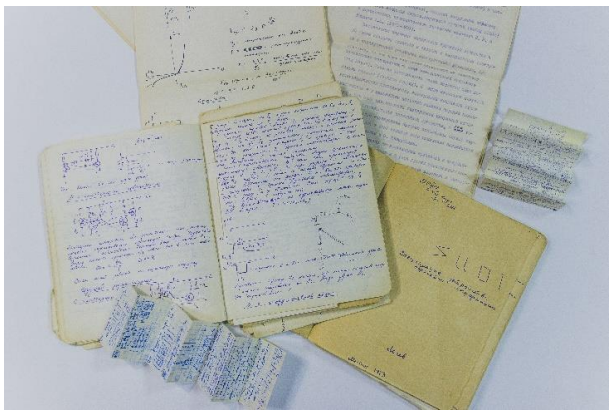
Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Представлены краткий обзор и наполнение учебных дисциплин по цифровой обработке сигналов и теории кодирования на кафедре радиопередающих устройств и радиотехнических систем Минского радиотехнического института.

Ключевые слова: теория кодирования, цифровая обработка сигналов.

Обучаясь в 1964–1967 гг. в аспирантуре кафедры радиотехнических систем Ленинградского электротехнического института им. В.И. Ульянова (Ленина), Лосев В.В. осознал необходимость изучения цифровой обработки сигналов и помехоустойчивого кодирования для эффективной борьбы с помехами. Работая с 1968 г. в МРТИ на кафедре радиопередающих устройств и радиотехнических систем (РПдУ и РТС), он прошел путь от ассистента до профессора кафедры, читал дисциплины «Импульсные устройства», «Цифровые и микропроцессорные устройства», в которых много внимания уделял применению цифровых алгоритмов для обработки радиосигналов (выполнение арифметических операций, изучение функций алгебры логики, синтез комбинационных устройств на основе микросхем малой и средней интеграции, мультиплексоров, программируемых логических матриц), абстрактному и структурному синтезу цифровых и микропрограммных автоматов [1]. Непрерывно совершенствовал эти дисциплины, дополнял, обновлял лабораторный практикум.

Наряду с преподаванием дисциплин по цифровой технике, начиная с 1973 г., разрабатывал и читал ряд спецкурсов: «Специальные устройства обработки информации», «Методы и устройства обработки информации», «Прикладная теория кодирования» (ПТК), «Цифровая обработка сигналов» (ЦОС), готовил и издавал соответствующие методические разработки и пособия [2, 3].



Поскольку основную роль при цифровой обработке сигналов играют алгоритмы, то в программу дисциплин им были заложены эффективные алгоритмы выполнения базовых арифметических и логических операций (сложения, вычитания, умножения, деления, возведения в степень), как для действительных, так и для комплексных чисел, а также операции с полиномами и векторно-матричные операции. Основные разделы программы посвящались обработке сигналов с помощью дискретных ортогональных преобразований. Подробно рассматривались различные виды быстрых алгоритмов дискретных преобразований Фурье, Уолша, Хаара.

Рассмотрение теоретико-числовых преобразований потребовало изучения основных положений высшей алгебры, операций над абстрактными элементами множеств, операций

с кольцами и полями Галуа. Изучение материала было направлено на решение насущных задач цифровой обработки сигналов в наземных и космических радиотехнических системах, радиолокации, радионавигации и связи. Особое внимание уделялось быстрым методам вычисления спектров, корреляционных функций и сверток, без расчета которых невозможно представить обработку сложных широкополосных сигналов.

Рассмотрение быстрых методов вычисления линейных, циклических и диадных корреляционных функций и сверток потребовало изучения основ модульной арифметики, операций с полиномами над полем, китайской теоремы об остатках, алгоритма Евклида, алгоритмов Винограда преобразований Фурье. Рассматривались структуры и реализации алгоритмов, в том числе с применением быстрых спектральных преобразований. При рассмотрении любого алгоритма выполнялись оценка вычислительной сложности и сравнительный анализ.

В дисциплине ПТК, как и в дисциплине ЦОС, большое внимание уделялось базовым алгоритмам кодирования и декодирования широко используемых помехоустойчивых кодов при последовательной и параллельной их обработке. Много внимания уделялось алгебраическим основам теории кодирования (вопросам построения конечных полей, группам, матрицам), изучению важнейших линейных кодов (Хэмминга, Рида-Маллера, Рида-Соломона, Адамара, БЧХ, низкоплотных, сверточных и других), методам их обработки (кодированию и декодированию в различных каналах передачи и хранения информации), позволяющим обнаруживать и исправлять случайные зависимые ошибки (модули, пакеты) и дефекты, проводить синтез цифровых кодеков на основе использования теории линейных автоматов и современной цифровой элементной базы.

Хорошо владея предметом и заглядывая далеко вперед, Лосев В.В. заложил в дисциплины ЦОС и ПТК классические базовые операции, без знания которых нельзя ни понять известные алгоритмы, ни освоить новые и, естественно, правильно их использовать при разработке разнообразных цифровых систем.

PREPARATION OF RADIOENGINEERS ON DIGITAL PROCESSING OF SIGNALS AND CODING THEORY IN MINSK RADIOTECHNICAL INSTITUTE IN 1968-1990

V.K. KONOPELKO, I.I. ASTROVSKY

A brief overview and content of educational disciplines on digital signal processing and coding theory at the department of radiotransmission devices and radioengineering systems of the Minsk radiotechnical institute are presented.

Keywords: coding theory, digital signal processing.

Список литературы

1. *Лосев В.В.* Цифровые методы формирования импульсных сигналов. Учебное пособие. Минск: МРТИ, 1979.
2. *Лосев В.В.* Помехоустойчивое кодирование в РТС ПИ. Циклические коды. Минск: МРТИ, 1984.
3. *Лосев В.В.* Микропроцессорные устройства обработки информации. Алгоритмы цифровой обработки. Учебное пособие с грифом Министерства народного образования БССР. Минск: «Вышэйшая школа», 1990.

УДК 004.9

ИССЛЕДОВАТЕЛЬСКАЯ ДЕЯТЕЛЬНОСТЬ ПРОФЕССОРА ЛОСЕВА В.В. В 1968–1990 ГГ. В ОБЛАСТИ СОЗДАНИЯ ЦИФРОВЫХ РАДИОСИСТЕМ

[1]В.К. КОНОПЕЛЬКО, [2]А.И. МИТЮХИН

[1]*Белорусский государственный университет информатики и радиоэлектроники П. Бровки, 6, Минск, 220013, Беларусь*

[2]*Институт информационных технологий Белорусского государственного университета информатики и радиоэлектроники, Козлова, 28, Минск, 220037, Беларусь*

Представлены результаты практического воплощения разработанных под руководством Лосева В.В. и его учеников алгоритмов цифровой обработки сигналов и теории кодирования в радиосистемах различного назначения.

Ключевые слова: радиосистема, помехоустойчивое кодирование, цифровая обработка, обнаружение, низкоскоростной код, изображение, разрешение.

Владислав Валентинович Лосев – известный советский ученый в области теории кодирования (ТК), цифровой обработки сигналов (ЦОС) и их использования в радиосистемах и системах связи различного назначения. Одним из первых он увидел в этих научных направлениях будущее развитие информационных технологий. Его имя отражено в исследованиях и множестве публикаций, посвященных проблемам поиска, полихотомическим методам синхронизации и обработки оптимальных кодовых конструкций методами максимального правдоподобия, мажоритарного и перестановочного декодирования, позволяющими эффективно осуществлять цифровую реализацию алгоритмов [1–11]. Его работы актуальны и значимы в исследованиях по разработке спектральных методов ЦОС в радиосистемах и в большой степени определялись практической необходимостью разработки новых алгоритмов в ЦОС и ТК для решения задач обнаружения и различения сигналов в каналах с шумами. Ниже представлены некоторые примеры практического воплощения научных результатов Лосева В.В. и его учеников.

Еще в конце 70-х гг. прошлого столетия в научных лабораториях Минского радиотехнического института (МРТИ) проводилась разработка системы энергетически скрытной связи с ортогональной модуляцией. В системе каждому уровню квантования речевого сигнала соответствовало кодовое слово низкоскоростного кода. Это была первая система подобного типа в СССР, продемонстрированная и одобренная к производству Министерством обороны (МО) СССР. Аналогом этой системы являлась американская система с кодовым разделением каналов «Диджилок». Развитием этой технологии передачи сигналов с разделением по коду для гражданских и военных пользователей являются в настоящее время широко применяемые технологии мобильной сотовой связи CDMA, беспроводной радиосвязи Wi-Fi, Bluetooth и др.

Научные и технические результаты, полученные в этой работе, использовались в 80-х гг. прошлого столетия при создании аппаратуры, в программе «Вега» для исследования дальнего космоса, где головным разработчиком являлось Особое конструкторское бюро Московского энергетического института (ОКБ МЭИ). Программа включала в себя ряд научно-исследовательских работ (НИР), связанных с разработкой аппаратуры для искусственных спутников и комплекса радиолокационного зондирования (картографирования) поверхности планеты Венера. Два комплекса находились на бортах космических станций «Венера-15» и «Венера-16». Техническим заданием на разработку радиолинии дальней космической связи задавалась необходимость осуществить радиосвязь на расстоянии 105–260 млн. км.

В МРТИ разрабатывалась аппаратура для обработки телеметрических сигналов многоканальной совмещенной системы связи, где применялись помехоустойчивые низкоскоростные коды разной длины для решения задач передачи эксплуатационных данных о работе спутниковой бортовой аппаратуры, а также исследовательских данных. В качестве переносчика информации использовались *M*-последовательности длиной 511 и 32767 двоичных символов. Применением кодированных сигналов обеспечивалось совместное измерение скорости движения и дальности космического аппарата. При измерении дальности осуществлялось измерение задержки между излученным и принятым сигналами: $\tau = 2D(t)/c,$ где $D(t)$ – дальность до объекта измерений, c – скорость света.

При измерении скорости оценивалось допплеровское приращение частоты: $\Delta f = 2\dot{D}(t) f / c,$ где $\dot{D}(t)$ – скорость движения объекта; f –несущая частота.

Периодическая 127-элементная *M*-последовательность использовалась для фазовой манипуляции сигналов радара с синтезированной апертурой. Кроме обеспечения связи с космическим аппаратом, информационная система должна была выполнять следующие задачи:

– передавать командную и телеметрическую информацию на борт космического аппарата с Земли;

– передавать технические и научные данные с космического аппарата на Землю;

– обеспечивать автоматическое слежение за частотой Доплера, а также слежение по угловым координатам.

Техническая реализация бортовой аппаратуры программы «Вега» и стыковка разработанных блоков, устройств и элементов космических станций осуществлялась в ОКБ МЭИ. На рис. 1 показана автоматическая межпланетная станция «Венера-16».

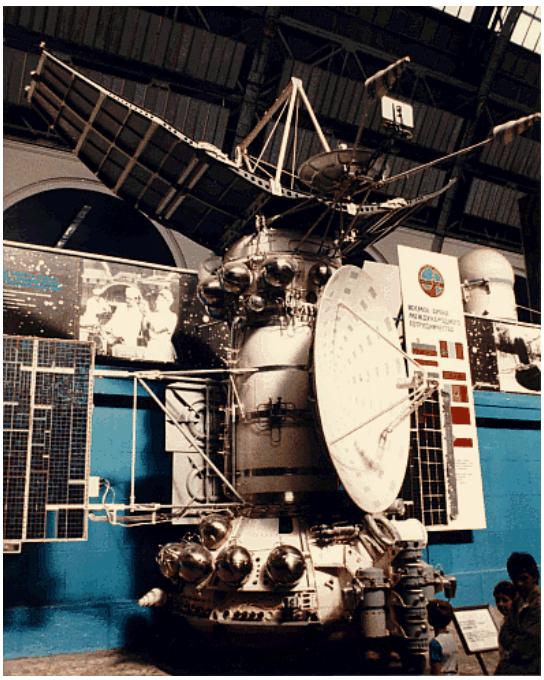


Рис. 1. Автоматическая космическая межпланетная станция «Венера-16»

Следует отметить, что на то время разрешение радиолокационных изображений планеты Венеры (рис. 2) составляло 1–2 км. В похожей американской программе разрешение изображений составляло примерно 20 км. В настоящее время качественные характеристики таких изображений достигают разрешения 200–300 м. Немного позднее модифицированные результаты предыдущих исследований и разработок использовались в проекте «Венера-Галлея» при создании аппарата «Вега». Две автоматические межпланетные станции «Вега-1» и «Вега-2» этого проекта осуществляли комплексное исследование кометы Галлея (рис. 3) и космического пространства с попутным облетом и изучением планеты Венера.

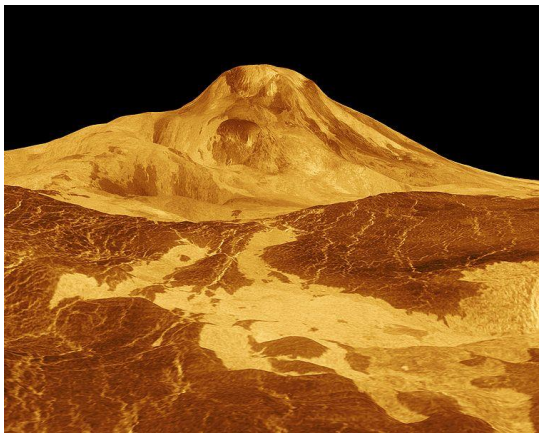


Рис. 2. Радиолокационное изображение поверхности Венеры

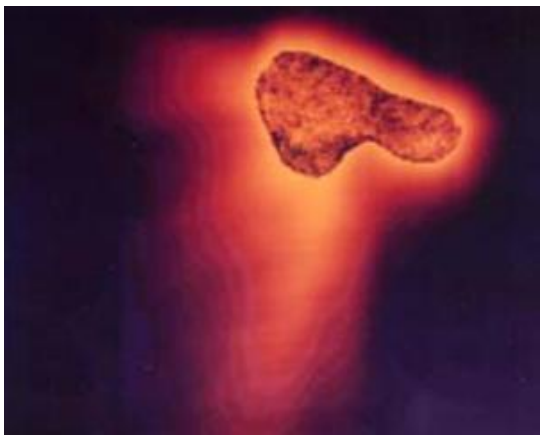


Рис. 3. Снимок ядра кометы Галлея

Под научным руководством профессора Лосева В.В. также был выполнен ряд специальных НИР по разработке систем скрытной кодированной передачи информации. Особое внимание было уделено исследованию новых алгоритмов синхронизации низкоскоростных кодов большой значности (десятки тысяч двоичных символов) по начальной фазе, тактовой и несущей частотам. Исследовалось влияние индустриальных и преднамеренных помех на систему обработки сложных кодированных сигналов. В результате на одном из предприятий СССР был осуществлен выпуск партии разработанной аппаратуры специального и народнохозяйственного назначения. Аппаратура показала свою эффективность и надежность. Постановлением № 315 Правительства СССР исполнители НИР дважды были отмечены премиями за высокое качество выполненных и внедренных научных результатов работы в разовой партии приборов, создание головного образца специального изделия для МО СССР.

Одновременно с разработкой аппаратуры проводились исследования, связанные с формированием и изучением свойств новых конструкций кодированных сигналов, предназначенных для использования в радионавигационных спутниковых системах. Разрабатывались новые цифровые алгоритмы слежения за задержкой кодированных сигналов аппаратуры пользователей радионавигационных спутниковых систем с надежной синхронизацией такой аппаратуры.

В настоящее время в БГУИР продолжаются исследования его учеников. Кроме научных направлений, в которых успешно работал профессор Лосев В.В., разрабатываются новые области применения ЦОС и ТК, решаются новые технические задачи современных информационных технологий. В частности, значительные исследования ориентированы на цифровую обработку пространственных данных для специальных применений. Решаются теоретические и практические задачи, связанные с обнаружением, эффективным описанием или поиском определенных объектов на изображениях, их распознаванием или идентификацией [12–18].

RESEARCH ACTIVITIES OF PROFESSOR LOSEV V.V. IN THE CREATION OF DIGITAL RADIOSYSTEMS IN 1968–1990

V.K. KONOPELKO, A.I. MITSIUKHIN

Abstract

The results of the practical implementation of algorithms for digital signal processing and coding theory in radiosystems for various purposes developed under the leadership of Losev V.V. and his students are presented.

Keywords: radiosystem, interference-free coding, digital processing, detection, slow code, image, resolution.

Список литературы

1. *Лосев В.В., Бродская Е.Б., Коржик В.И.* Поиск и декодирование сложных дискретных сигналов. М.: Радио и связь, 1988.
2. *Лосев В.В.* Верхняя граница сложности умножения вектора на бинарную матрицу // Радиотехника и электроника. 1980. Т. 25, № 11. С. 2465–2467.
3. *Лосев В.В., Дворников В.Д.* Определение фазы псевдослучайной последовательности по отрезку при помощи быстрых преобразований // Радиотехника и электроника. 1981. Т. 26, № 8. С. 1661–1671.
4. *Лосев В.В., Дворников В.Д.* Распознавание адресных последовательностей при помощи быстрых преобразований // Радиотехника и электроника. 1983. Т. 28, № 8. С. 1541–1547.
5. *Лосев В.В.* Декодирование мажоритарно-уплотненных сигналов при помощи диадной свертки // Радиотехника и электроника. 1980. Т. 25, № 9. С. 1999–2001.
6. *Лосев В.В.* Диадно-групповая структура последовательностей быстрого поиска // Радиотехника и электроника. 1980. Т. 25, № 2. С. 27–28.
7. *Лосев В.В.* Обнаружение последовательностей Голда при помощи быстрых преобразований // Радиотехника и электроника. 1981. Т. 26, № 8. С. 1660–1665.
8. *Лосев В.В.* Определение фазы длинных псевдослучайных *M*-последовательностей при помощи коротких преобразований Адамара // Радиотехника и электроника. 1983. Т. 28, № 3. С. 620–622.
9. *Лосев В.В.* Определение фазы псевдослучайной последовательности // Изв. вузов СССР. Радиоэлектроника. 1980. Т. 23, № 12. С. 81–82.
10. *Лосев В.В*. Применение теоретико-числовых преобразований для синхронизации и декодирования сигналов // Радиотехника и электроника. 1980. Т. 25, №7. С. 1468–1476.
11. *Лосев В.В., Якутик К.В.* Последовательности быстрого поиска для совмещенных систем // Изв. вузов СССР. Радиоэлектроника. 1983. Т. 26, №11. С. 17–21.
12. *Mitsiukhin A.* Application of hartley descriptors // Proc. Of 55th International Scientific Colloquium. Ilmenau, 13–17 September 2010. P. 836–841.
13. *Mitsiukhin A.* Segmentation of dynamical images by means of discrete Hartley transform // Proc. of 56 International Scientific Colloquium. Ilmenau, 12–16 September 2011. URN: urn:nbn:de:gbv:ilm1-2011iwk-011:5, id 1100.
14. *Міцюхін А.І.* Нелінейная канструкцыя карэкціруючага кода на аснове функцыі Мёбіуса // Матер. 15-й Междунар. науч. конф. им. акад. М. Кравчука, Киев, 15–17 мая, 2014. Т. 2. С. 137.
15. *Mitsiukhin A.* Extraction of the motion indications in the sequence of images // Proc. of 58th International Scientific Colloquium. Ilmenau, 8–12 September 2014. URN: urn:nbn:de:gbv:ilm1-2014iwk-0,75:0, id 2066.
16. *Митюхин А.И., Якубенко П.Н.* Корреляционные спектры и кодовые расстояния мажоритарных последовательностей // Докл. БГУИР. 2015. № 4 (90). С. 5–9.
17. *Mitsiukhin A.* Efficient description of the boundary of the object under observation // Proc. of 59th Ilmenau Scientific Colloquium. Ilmenau, 11–15 September 2017 [Электронный ресурс]. URL: http://db-thueringen.de/rsc/viewer/dbt_derivate_00039296/ilm1-2017iwk-018.pdf?page=6 (дата обращения: 20.04.2018).
18. *Міцюхін А.І.* Павышэнне надзейнасці біяметрычнай сістэмы // Proc. of 18th International scientific conf. named after M. Kravchuk. Kiev, October 7–10, 2017. Vol. 2. P. 124–126.

УДК 512 (075.8)

СТАНОВЛЕНИЕ БЕЛОРУССКОЙ ШКОЛЫ ЦИФРОВОЙ ОБРАБОТКИ СИГНАЛОВ И ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

[1]В.А. ЛИПНИЦКИЙ, [2]В.К. КОНОПЕЛЬКО

[1]*Военная академия Республики Беларусь*
Минск-57, 220057, Беларусь

[2]*Белорусский государственный университет информатики и радиоэлектроники*
П. Бровки, 6, Минск, 220013, Беларусь

Исследуется процесс становления научной школы цифровой обработки сигналов и помехоустойчивого кодирования в МРТИ–БГУИР за четыре прошедших десятилетия.

Ключевые слова: помехоустойчивое кодирование, цифровая обработка сигналов.

Доктор технических наук, профессор Лосев В.В. (1938–1990) – один из ведущих специалистов в области радиотехники в Минском радиотехническом институте (МРТИ) последней четверти XX века. Представитель Ленинградской научной школы, он решил посвятить свои знания, опыт и разносторонние таланты белорусскому народу.

Следует сказать, что на тот момент МРТИ был знаменит на весь Советский Союз не только своей командой по баскетболу, а прежде всего, своим мощным научным потенциалом и считался первым из четырех радиотехнических вузов СССР. Факультет радиоэлектроники был основополагающим в МРТИ. Кафедры радиотехнических систем, приемо-передающих устройств, антенн, микроэлектроники возглавляли выдающиеся ученые СССР. Они создавали творческую атмосферу и высокий уровень научных исследований в вузе и в Беларуси в целом (тема отдельного и большого разговора).

Как ученый-исследователь, Лосев В.В. прозорливо ощутил, что на смену аналоговым системам передачи и обработки информации неизбежно должны прийти цифровые. И в сторону последних он решительно повернул свои научные интересы и исследования. Обладая большой эрудицией, неподражаемым интеллектом, дружелюбным характером и личным обаянием, он увлек в то же русло научные интересы своих друзей, коллег и учеников: Конопелько В.К., Будько А.А., Дворникова В.Д., Карякина Ю.Д., Саломатина С.Б., Урбановича П.П., Астровского И.И., Юрцевича М.М., Митюхина А.И., Тарасова А.С., Мальцева С.В. и многих других. О широких творческих и научных связях Лосева В.В. и за пределами Беларуси свидетельствует монография, посвященная спектральным методам обработки радиосигналов [1]. Об его активной научной деятельности говорят многочисленные публикации, подготовленные как единолично, так и в соавторстве. Отметим хотя бы одну из первых больших работ в мире по проблемам надежного хранения информации – монографию [2], выполненную совместно с Конопелько В.К., а также работы [3, 4] и работы, опубликованные в известных журналах СССР.

Лосев В.В. был инициатором изменений и в учебном процессе в сторону более углубленного изучения цифровых систем обработки (ЦОС), математических основ кодирования и декодирования при хранении и передаче информации – теории кодирования (ТК). Естественно, литература в данной, новой области науки и ее приложений, существовала лишь в форме научных статей и свежих научных монографий. Поэтому учебную литературу для студентов и аспирантов приходилось создавать с чистого листа. И достаточно успешно. Об этом свидетельствуют ряд учебных пособий Лосева В.В. для студентов-радиотехников, к примеру, пособие [5], а также учебное пособие с грифом Минобразования

БССР [6], остающееся актуальным и популярным и в наши дни. Ее оцифрованный вариант давно доступен для просмотра и скачивания в русскоязычном сегменте сети Интернет. Творческая энергия и организаторский талант Лосева В.В. позволили ему впервые в Беларуси создать из круга соратников и учеников действенную, активную и работающую школу по ЦОС и ТК (рис. 1).

Рис. 1. Школа по ЦОС и ТК в МРТИ-БГУИР

После преждевременной кончины Лосева В.В. руководство школой перешло к его наиболее яркому и талантливому ученику – доктору технических наук, профессору Конопелько В.К., который продолжил и развил исследования по всем основным направлениям ЦОС и ТК, защиты информации. Им подготовлен ряд методических пособий под общим названием «Помехоустойчивое кодирование в РТС ПИ» (см., к примеру [7], написанные как иллюстрация и развитие определенных тем дисциплины «Теория кодирования»). Пособия в концентрированной форме содержат богатые идеи и темы для самостоятельной научно-исследовательской работы студентов старших курсов и аспирантов. К примеру, радиоинженер Власова Г.А. – одна из первых женщин, защитивших кандидатскую диссертацию на кафедре РПдУ и РТС. Ее работа была посвящена синдромным идентификаторам классов эквивалентности ошибок в линейных кодах [8], получившим впоследствии название «нормы синдромов». Проведенные в дальнейшем исследования по теории норм синдромов оказались весьма плодотворными [9]. На работы, в которых представлены результаты этих исследований, до сих пор есть ссылки в сети Интернет.

Новый виток научной и педагогической деятельности школа ЦОС и ТК приобрела в 1998 г. с приходом Конопелько В.К. на должность заведующего кафедрой сетей и устройств телекоммуникаций (СиУТ). Прежде всего им был реализован давний замысел – организовать межфакультетский коллектив для создания первого в Беларуси, уникального по тематике, полноте и широте материала двухтомного учебника по «Теории прикладного кодирования», предназначенного для студентов, магистров, аспирантов, обучающихся по специальностям, связанным с инфокоммуникационными технологиями. Впоследствии этот учебник получил гриф Министерства образования Республики Беларусь [10].

Второй замысел Конопелько В.К. состоял в широком использовании ЦОС и ТК практически в всем научно-исследовательских направлениях кафедры. Благодаря позитивной и конструктивной энергии Конопелько В.К. и его учеников, опубликован широкий спектр монографий по ЦОС, ТК и защите информации ([11–15] – лишь небольшая их выборка). Тем самым, прежде всего, систематизировались и аккумулировались новые научные знания, фрагментарно разбросанные и терявшиеся по многочисленным публикациям в журналах, сборниках материалов и тезисов конференций, депонированных изданиях. Кроме того, авторы монографий получали интегрированный взгляд на свои исследования. Некоторые из них начинали задумываться о написании собственных кандидатских и докторских диссертаций. Это позволило укрепить ППС кафедры высококвалифицированными специалистами. Каждый новый

доктор наук читал на кафедре собственный курс. В 2004–2017 гг. на кафедре защитили докторские диссертации Бобов Михаил Никитич (по проблемам безопасности), Липницкий Валерий Антонович (по теории норм синдромов), Рылов Александр Сергеевич (по проблемам распознавания речи), Борискевич Анатолий Антонович (по проблемам защиты информации), Цветков Виктор Юрьевич (по вопросам обработки и передачи изображений). За последние два десятилетия на кафедре защищено более двух десятков кандидатских диссертаций как гражданами Республики Беларусь, так и представителями стран Азии, Африки и Латинской Америки.

В настоящее время Белорусская школа по ЦОС и ТК представляет собой живой, действующий организм, способный на конструктивную научную и учебную работу в области инфокоммуникаций.

FORMATION OF BELARUSIAN SCHOOL OF DIGITAL SIGNAL PROCESSING AND NOISE-IMMUNE CODING

V.A. LIPNITSKI, V.K. KONOPELKO

Abstract

The development of the scientific school of digital signal processing and noise-immune coding in the MRTI–BSUIR for the past four decades has been studied.

Keywords: noise-immune coding, digital signal processing.

Список литературы

1. *Лосев В.В., Бродская Е.Б., Коржик В.И.* Поиск и декодирование сложных дискретных сигналов. М.: Радио и связь, 1988.
2. *Конопелько В.К., Лосев В.В.* Надежное хранение информации в полупроводниковых запоминающих устройствах. М.: Радио и Связь, 1986.
3. *Лосев В.В.* Определение фазы псевдослучайной последовательности // Изв. вузов. Радиотехника. 1980. Т. 22, № 12. С. 81–82.
4. *Лосев В.В., Дворников В.Д.* Декодирование кода максимальной длины при помощи быстрого преобразования Уолша // Радиотехника и электроника. Т. 24, № 3. С.630–632.
5. *Лосев В.В.* Учебное пособие по спецкурсу «Цифровые методы формирования импульсных сигналов». М.: МРТИ, 1979.
6. *Лосев В.В.* Микропроцессорные устройства обработки информации. Алгоритмы цифровой обработки. Минск: Вышэйшая школа. 1990.
7. *Конопелько В.К.* Помехоустойчивое кодирование в радиотехнических системах передачи информации: Однородные коды. Минск: Ротапринт МРТИ, 1993.
8. *Власова Г.А., Конопелько В.К.* Идентификация ошибок при передаче информации с корректирующими кодами // Матер. Междунар. НТК «Современные системы связи». Нарочь, май 1995 г. С. 36.
9. *Конопелько В.К., Липницкий В.А.* Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. Издание второе. М.: УРСС, 2004.
10. Теория прикладного кодирования в 2 т. Учебное пособие с грифом Мин. образования / Под ред. Конопелько В.К. Минск: БГУИР, 2004.
11. *Дворников В.Д., Конопелько В.К., Липницкий В.А.* Теория и практика низкоскоростных кодов. Минск: БГУИР, 2002.
12. *Бобов М.Н., Конопелько В.К.* Обеспечение безопасности в телекоммуникационных системах. Минск: БГУИР, 2002.
13. *Липницкий В.А., Конопелько В.К.* Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск: Издат. центр БГУ, 2007.
14. *Королёв А.И., Саид Ахмед Аль-алем, Конопелько В.К.* Помехоустойчивое кодирование информации. Минск: Бестпринт, 2013.
15. *Цветков В.Ю., Конопелько В.К., Липницкий В.А.* Предсказание, распознавание и формирование образов многоракурсных изображений с подвижных объектов. Минск: Издат. центр БГУ, 2014.

УДК 512 (075.8)

АНАЛИЗ БЫСТРЫХ МЕТОДОВ ЦИФРОВОЙ ОБРАБОТКИ СЛОЖНЫХ СИГНАЛОВ И ДЕКОДИРОВАНИЯ НИЗКОСКОРОСТНЫХ КОДОВ

В.Д. ДВОРНИКОВ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Представлены синтез и анализ методов цифровой обработки сигналов, а также подходы к декодированию низкоскоростных кодов в радиотехнических системах.

Ключевые слова: декодирование, цифровая обработка, радиотехническая система.

Семидесятые годы прошлого столетия характеризуются стремительным ростом интереса к новым методам формирования и обработки сигналов в радиотехнических системах (РТС) различного назначения. Наиболее перспективным оказался подход, в котором используются сложные сигналы в совокупности с цифровыми алгоритмами их формирования и обработки. Это позволяло повышать такие технические характеристики как помехоустойчивость, надежность, дальность действия, скрытность, точность измерения параметров, быстродействие систем и устройств.

Наиболее изученными в тот период времени были сигналы, формируемые на основе двоичных *M*-последовательностей (кодов максимальной длины). Они легко генерируются, имеют достаточно большие ансамбли и обладают идеальными корреляционными свойствами. Поэтому именно они чаще всего становились основой для построения систем передачи информации, синхронизации, локации, и навигации. Для их обработки, в основном, использовались согласованные фильтры, многоканальные корреляторы и сигнальные процессоры на основе алгоритмов преобразования Фурье. Уровень развития производства элементной базы того периода времени не позволял создавать быстродействующую и простую аппаратуру обработки сигналов. В особенности если речь шла о применении длинных, порядка нескольких тысяч символов, сигналов.

В конце 1974 г., в научном коллективе, который возглавлял Лосев В.В., был разработан алгоритм обработки сигналов на основе бинарных *M*-последовательностей при помощи быстрого преобразования Уолша (БПУ). Не уступая в помехоустойчивости известным корреляционным алгоритмам, он был значительно проще в реализации и выигрывал у них по быстродействию.

Результаты исследований были защищены авторским свидетельством и опубликованы в СССР в декабре 1976 г. в журнале «Известия ВУЗов. Радиоэлектроника» [1]. В январе 1977 г. появилась публикация [2] американских авторов практически одинакового с [1] содержания, но с частным решением. Выходные данные публикаций говорят о неоспоримом приоритете СССР в данном научном достижении. К сожалению, перевод русскоязычной публикации на английский язык появился только через несколько лет, поэтому в научном мире закрепилось представление об американском приоритете.

В дальнейшем, в работах Лосева В.В. и его учеников данный подход и его модификации были использованы для разработки быстрых алгоритмов обработки целого ряда сигналов, которые формируются на базе *M*-последовательности (последовательностей Голда, Гордона–Миллса–Велча, Кассами, Мак-Элис) [3, 4]. Продуктивным данный подход оказался и для обработки очень длинных сигналов по отрезку [5].

На основе полученных научных результатов разработан ряд технических решений, которые защищены авторскими свидетельствами СССР [6, 7] и реализованы в реальных устройствах в ходе выполнения нескольких НИР.

Еще одним применением процессоров БПУ явилось использование их для декодирования низкоскоростных кодов, таких как код максимальной длины [8] и код Рида–Маллера [9]. При этом реализуется корреляционный алгоритм декодирования, позволяющий получить максимальную помехоустойчивость. Кроме этого, за счет упрощения декодера он легко реализуется как аппаратно, так и программно. Что касается кода Рида–Маллера, то впервые было показано и доказано, что коэффициент сложности корреляционного декодера при увеличении порядка кода и его длины, асимптотически стремится к нулю. Это оказалось возможным при его представлении в виде каскадной конструкции из q-ичного полного кода и кода Рида–Маллера первого порядка.

Многие результаты исследований Лосева В.В. были новаторскими. Так, он существенно развил теорию дихотомического и полихотомического поиска последовательностей Стифлера, нашел способы ввода в синхросигналы информации и ее выделения, в которых используются свойства диадного сдвига [4]. Еще одним плодотворным направлением в обработке сигналов было использование секционирования – разбиения составных последовательностей на компоненты, имеющие особые свойства, позволяющие выполнять быструю обработку. Такой подход реализован в алгоритме поиска последовательностей Гордона–Милса–Велча [9].

Многие подходы и методы исследований Лосева В.В. применялись его учениками в их дальнейшей самостоятельной научной деятельности. Так, получили развитие методы обработки M-последовательностей и последовательностей Гордон–Милса–Велча, использующие их двумерное представление в виде матрицы, имеющей в своей структуре блок, образованный диадным сдвигом [9–11]. Это позволило использовать вычисление диадной свертки. По структуре цифровая обработка отличается от ранее упомянутого метода вычисления корреляции для M-последовательности, но имеет равную величину вычислительной сложности.

Полученные результаты интересны еще и тем, что последовательности Гордон–Милса–Велча имеют бóльшую структурную сложность, чем M-последовательность и позволяют существенно повысить защищенность сигнала. При этом сохраняется возможность быстро и надежно выполнять его поиск и синхронизацию.

Еще одним примером использования диадного сдвига является метод формирования и декодирования низкоскоростных кодов на базе бент-последовательностей [12]. Бент-последовательности получаются из бент-функций, которые являются частью класса максимально-нелинейных функций. Они интенсивно исследуются и широко применяются в криптографических системах. Их основные достоинства заключаются в высокой структурной сложности и большом размере множества. Это позволяет легко формировать необходимое количество ансамблей сигналов для создания больших сетей помехоустойчивой и защищенной передачи информации. При этом их обработка не сложнее, чем вычисление БПУ.

Бент-последовательности структурно связаны с матрицей БПУ, которая образует ядро алгоритма их формирования. Если в качестве ядра использовать матрицу преобразования Фурье, то получаются комплексные ортогональные последовательности, называемые последовательностями Фрэнка [13]. Сигналы Фрэнка имеют в прямом смысле идеальную периодическую автокорреляционную функцию и широко исследуются в настоящее время.

В [12] описан алгоритм обработки последовательностей Фрэнка, в основу которого положено преобразование последовательности в двумерную матрицу. При этом алгоритм вычисления корреляции свертки при помощи двукратного преобразования Фурье исходной последовательности заменяется комбинацией вычисления нескольких более коротких преобразований Фурье и прямого вычисления корреляции или свертки. Вычислительная сложность алгоритма не превышает вычислительной сложности одного преобразования Фурье размерности исходной последовательности.

Приведенные примеры не исчерпывают всех возможностей применения описанных подходов к цифровой обработке других классов сложных сигналов и низкоскоростных кодов.

ANALYSIS OF FAST METHODS OF DIGITAL PROCESSING OF COMPLEX SIGNALS AND LOW-SPEED CODES DECODING

V.D. DVORNIKOV

Abstract

Synthesis and analysis of digital signal processing methods, as well as approaches to decoding of low-speed codes in radiotechnical systems are presented.

Keywords: decoding, digital processing, radiotechnical system.

Список литературы

1. *Лосев В.В. Дворников В.Д.* Способ многоканальной обработки симплексных кодов // Изв. ВУЗов. Радиоэлектроника. 1976. № 12. С. 89.
2. *Kohn M., Lempel A.* On fast *M*-sequence transforms // IEEE Transactions on Information Theory. January, 1977. P. 135.
3. *Лосев В.В., Дворников В.Д.* Распознавание адресных последовательностей при помощи быстрых преобразований // Радиотехника и электроника. 1983. № 8. С. 1540–1547.
4. *Лосев В.В., Бродская Е.Б., Коржик В.И.* Поиск и декодирование сложных дискретных сигналов. М.: Радио и связь, 1988.
5. *Лосев В.В., Дворников В.Д.* Определение фазы ПСП по отрезку с помощью БПУ // Радиотехника и электроника. 1981. № 8. С. 1666–1671.
6. *Дворников В.Д., Лосев В.В., Будько А.А.* Устройство определения фазы *M*-последовательности / Авторское свидетельство СССР № 625314.
7. *Дворников В.Д., Лосев В.В.* Устройство декодирования *M*-последовательности / Авторское свидетельство СССР № 773948.
8. *Лосев В.В., Дворников В.Д.* Декодирование кода максимальной длины при помощи БПУ // Радиотехника и электроника. 1979, № 3. С. 1233–1239.
9. *Дворников В.Д., Конопелько В.К., Липницкий В.А.* Теория и практика низкоскоростных кодов. Минск: БГУИР. 2002.
10. *Дворников В.Д., Макаров А.И.* Декодирование негрупповых кодов при помощи быстрого преобразования Уолша-Адамара // Сб. докл. 1-й междунар. конф. «Цифровая обработка сигналов и ее применение – DSPA'98». Москва, 1998. Т. 2. С. 63–66.
11. *Дворников В.Д.* Сравнительный анализ быстрых алгоритмов обработки *M*-последовательности // Матери. второй науч.-практ. конф. «Гидроакустическая связь и средства аварийно-спасательного назначения». Волгоград, 2003. С. 33–39.
12. *Дворников В.Д.* Ортогональные коды на основе бент-последовательностей // Докл. БГУИР. 2003. № 1. С. 110–113.
13. *Дворников В.Д.* Многофазные последовательности с идеальными корреляционными свойствами // Докл. БГУИР. 2003. № 1. С. 111–114.

УДК 621.391

ПРИМЕНЕНИЕ ОРТОГОНАЛЬНОГО БАЗИСА УОЛША В ЦИФРОВОЙ ОБРАБОТКЕ СИГНАЛОВ

А.А. БУДЬКО

Белорусский государственный университет информатики и радиоэлектроники, П. Бровки, 6, Минск, 220013, Беларусь

Анализируются особенности применения ортогонального базиса Уолша в цифровой обработке сигналов при создании быстродействующих специализированных процессоров.

Ключевые слова: функция Уолша, быстрое спектральное преобразование, мгновенный спектр, быстрое декодирование.

Известно достаточно большое количество систем ортогональных функций. Однако применение той или иной системы ортогональных функций в радиотехнике и в других отраслях науки и техники зависит от ряда причин и, в первую очередь, от имеющейся элементной базы. Так, синусоидальные и косинусоидальные функции и понятия гармонического анализа, введенные Фурье в 1822 г., стали широко использоваться с появлением ламп, индуктивностей и конденсаторов. Появление интегральных схем явилось стимулом и обязательным условием использования системы ортогональных функций Уолша, которая была введена американским математиком Дж. Уолшем в 1923 г., хотя была известна и использовалась еще в конце XIX века [1–3]. В начале 70-х гг. прошлого века, когда еще шли жаркие дискуссии о возможности применения систем ортогональных функций Уолша, Лосеву В.В. понадобились определенные смелость и научная интуиция, чтобы предложить заниматься исследованиями в этой области [4]. Кроме элементной базы, обеспечивающей практическое применение определенной системы ортогональных функций, необходимыми условиями являлось также и то, чтобы эти функции обладали определенными структурными и другими свойствами, а также обеспечивали возможную простоту генерирования и спектральных преобразований. На решение этих вопросов, в первую очередь, и были направлены проводимые исследования. Были установлены взаимосвязи между одномерными и многомерными функциями Уолша, между одномерными и двумерными, одномерными и многомерными преобразованиями в базисе функций Уолша [5, 6], что представляло и представляет практический интерес при обработке изображений [7].

При разработке генераторов функций Уолша возникают такие противоречивые требования, как простота реализации и быстродействие. Для построения генераторов функций можно использовать определение функций Уолша через функции Радемахера, которые легко генерируются двоичными счетчиками. Однако, поскольку функции не могут генерироваться быстрее, чем счетчик получает приращение, то минимальный интервал аргумента ограничен. В более быстрых схемах генераторов функций Уолша используются регистры сдвига. Такие генераторы полностью основаны на быстродействии интегральных схем. Однако плата за повышение быстродействия стала чрезмерна высока, поскольку для формирования любой функции $W(k, x)$, $0 < x \le 2^n - 1$ предлагалось использовать 2^n-разрядный регистр. Используя свойства симметрии функций Уолша и взаимосвязь между одномерными и многомерными функциями, можно построить программированные и параллельные генераторы, требующие значительно меньших аппаратурных затрат [8, 9] не в ущерб быстродействию.

Интересной особенностью функций Уолша является то, что они имеют в настоящее время четыре системы упорядочения. Практически изначально использовались три системы: Уолша–Адамара, Уолша–Пэли и Уолша–Качмажа. В [10] при рассмотрении возможных систем

упорядочения функций Уолша было обращено внимание на еще одну матрицу функций Уолша, которая также была симметричной и впоследствии была названа матрицей Уолша–Трахтмана. Для этой системы упорядочения были получены формула для определения элементов матрицы в показательной форме, рекуррентная формула и мнемоническое правило построения матрицы, и построены алгоритмы БПУ типа «бабочка» [11, 12].

Одной из основных операций при обработке информации в базисе функций Уолша является вычисление коэффициентов преобразования. Оно осуществляется с помощью алгоритмов БПУ с использованием вычислительных машин или специализированных процессоров БПУ. К настоящему времени известно большое количество алгоритмов БПУ. Все эти алгоритмы требуют одно и то же количество операций, а именно $N \cdot \log_2 N$. Особое место занимают так называемые «замечательные» алгоритмы: алгоритмы типа «бабочка», позволяющие осуществлять вычисления на местах, экономя память; алгоритмы, имеющие одинаковый вид на каждой итерации и др. Выбор того или иного алгоритма зависит от решаемой задачи, а также от возможностей практической реализации.

Процессоры БПУ делятся на три типа: параллельные, у которых входные значения сигнала поступают в параллельном виде и значения выходных коэффициентов преобразования также получаются в параллельном виде; последовательные, у которых входные значения сигнала поступают в последовательном виде и значения выходных коэффициентов преобразования также получаются в последовательном виде; последовательно-параллельные, у которых входные значения сигнала поступают в последовательном виде, а значения выходных коэффициентов преобразования получаются в параллельном виде. Для построения процессоров параллельного типа используются алгоритмы БПУ, которые позволяют проводить вычисления «на местах», чтобы сократить аппаратурные затраты – однако и в этом случае затраты велики. Существенно меньшие аппаратные затраты при реализации процессоров БПУ последовательного типа [13, 14]. Однако в этом случае коэффициенты преобразования на выходе процессора получаются в последовательном виде.

В теории спектральных преобразований Уолша установились следующие понятия спектров. Спектр по Уолшу – это коэффициенты преобразования в той или иной системе упорядочения в зависимости от последовательности входного сигнала. При этом преобразования осуществляются со значениями входного сигнала $0 \div N-1$, $N \div 2N-1$, $2N \div 3N-1$ и т.д., то есть на составных интервалах. Другое понятие спектра – спектр мощности, третье – спектр мощности, инвариантный к циклическому сдвигу. Во многих практических приложениях необходимо осуществлять вычисление коэффициентов преобразования от последовательностей, составленных из N значений входного сигнала, после каждого нового значения входного сигнала, т.е. спектра, отражающего свойства процесса в данный момент времени. По аналогии с гармоническим спектром [15] такой спектр назван мгновенным спектром по Уолшу. Исследуя итерационную структуру вычисления спектральных коэффициентов от векторов входного сигнала $\overline{f_i}, \overline{f_{i+1}}, \ldots$, можно заметить, что в вычислениях имеются общие промежуточные результаты, что, в принципе, позволяет сократить до $2(N-1)$ число операций для каждой новой оценки спектра, вместо обычных $N \cdot \log_2 N$. Сокращение количества операций эквивалентно сокращению аппаратных затрат при реализации процессоров для вычисления мгновенного спектра. Были разработаны процессоры БПУ последовательно-параллельного типа [16, 17], в которых используются общие результаты промежуточных вычислений при оценке мгновенного спектра по Уолшу.

В процессе исследования M-последовательности и функции Уолша была обнаружена взаимосвязь между ними [17], что позволило реализовать быстрое декодирование кодов максимальной длины.

Выводы

Результаты, полученные при исследовании функций Уолша, внедрялись в научно-технические проекты и в учебный процесс [18]. Уже в 80-х гг. прошлого века студенты МРТИ–БГУИР изучали и исследовали функции Уолша, БПУ и процессоры, реализующие БПУ, а также быстрое декодирование кодов максимальной длины в курсе по цифровой обработке сигналов.

APPLICATION OF ORTHOGONAL WALSH FUNCTION IN DIGITAL HANDLING OF INFORMATION

A.A. BUDZKO

Abstract

The main purpose of this paper to show why orthogonal Walsh functions and Walsh transforms have became a very important instrument in digital processing of information. This paper also describes necessary condition for widely using any system of orthogonal functions in science and technique.

Keywords: Walsh function, fast spectral transformation, instantaneous spectrum, fast decoding.

Список литературы

1. *Henning F.H.* Transmission of Information by Orthogonal Functions. Berlin, Heidelberg, New York, 1970.
2. *Henning F.H.* Sequency Theory.Fundations and application. New York, San Francisco, London: Academic Press, 1977.
3. *Henning F.H.* Nonsinusoidal Waves for Radar and Radio Communication. New York, London, Toronto, Sydney, San Francisco, 1981.
4. *Лосев В.В.* Микропроцессорные устройства обработки информации. Алгоритмы цифровой обработки. Минск: Вышэйшая школа, 1990.
5. *Будько А.А., Дворников В.Д.* Взаимосвязь одномерного и многомерного преобразований Уолша-Адамара // Радиотехника и электроника. 1977. Вып. 7. С. 33–37.
6. *Будько А.А., Лосев В.В.* Взаимосвязь одномерного и многомерного преобразований Уолша. Методы и средства преобразований сигналов. Рига, 1976.
7. *Лосев В.В, Будько А.А., Дворников В.Д.* Устройство преобразования двумерных дискретных фигур методом Уолша-Адамара / Авторское свидетельство № 562816.
8. *Будько А.А., Дворников В.Д., Лосев В.В.* Генератор функций Уолша / Авторское свидетельство № 637805.
9. *Будько А.А.* Генератор функций Уолша / Авторское свидетельство № 1091145.
10. *Трахтман А.М., Трахтман В.А.* Основы теории дискретных сигналов на конечных интервалах. М.: Сов. радио, 1975.
11. *Budko A.A., Hu Zhengming.* Trahtman System of Walsh Function and the Permutation of Column Order // J. of China Institute of Communication. 1986. № 3. P. 27–34.
12. *Будько А.А.* Новая система упорядочения функций Уолша // Радиотехника и электроника. 1985. № 3. С. 75–81.
13. *Лосев В.В, Будько А.А., Дворников В.Д.* Устройство для вычисления коэффициентов преобразования по Уолшу / Авторское свидетельство №744555.
14. *Лосев В.В, Будько А.А., Дворников В.Д.* Устройство для ортогонального преобразования цифровых сигналов по Уолшу-Адамару / Авторское свидетельство № 555404.
15. *Харкевич А.А.* Спектры и анализ. Физмат, М., 1962.
16. *Будько А.А., Лосев В.В, Дворников В.Д.* Устройство ортогонального преобразования по Уолшу / Авторское свидетельство № 620974.
17. *Дворников В.Д., Лосев В.В., Корякин Ю.Д., Будько А.А.* Устройство определения фазы *М*-последовательности / Авторское свидетельство № 625314.
18. *Будько А.А.* Методические указания к лабораторной работе «Быстрое декодирование кодов максимальной длины» по курсу «Специализированные устройства обработки информации». Минск, 1982.

УДК 512 (075.8)

МНОГОЭТАПНЫЙ ПОИСК ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

[1]И.И. АСТРОВСКИЙ, [2]А.И. МИТЮХИН

[1]*Белорусский государственный университет информатики и радиоэлектроники П. Бровки, 6, Минск, 220013, Беларусь*

[2]*Институт информационных технологий Белорусского государственного университета информатики и радиоэлектроники, Козлова, 28, Минск, 220037, Беларусь*

Проводится анализ методов поиска сигналов на основе псевдослучайных последовательностей (низкоскоростных кодов, корректирующих многократные ошибки).

Ключевые слова: многократные ошибки, низкоскоростной код, псевдослучайная последовательность.

Расцвет творческой научной деятельности Лосева В.В. пришелся на годы стремительного прорыва СССР в космос. В те годы наряду с решением насущных проблем космонавтики необходимо было срочно решать сложнейшие вопросы улучшения тактико-технических характеристик устройств радиолокации, радионавигации и связи [1]. Стало очевидным, что решения могут быть найдены путем внедрения цифровых методов обработки сигналов, что позволит реализовать быстродействующие системы обработки сигналов. Причем не простых, а с использованием сложных сигналов с большой базой (низкоскоростных кодов).

Применение сложных сигналов обеспечивает построение скрытных, трудноуязвимых радиолокационных систем с разнесенными передатчиками и приемниками, создание помехоустойчивых разностно-дальномерных навигационных систем, в том числе систем космической связи, навигации и исследования небесных тел радиолокационными методами [1].

Выбор сигналов играет важную роль. Для обеспечения скрытности они должны обладать свойствами шумоподобности и в то же время обеспечивать надежную работу при малых отношениях сигнал/помеха. Формирование и обработка сигналов должны иметь простые схемные решения и не требовать больших объемов памяти и времени на обработку. Сигналы должны обладать хорошими авто- и взаимно-корреляционными свойствами и в то же время специальными свойствами, позволяющими ускорить их обработку. Необходимо было найти методы и быстрые алгоритмы как формирования, так и обработки, включая поиск и синхронизацию в частотно-временном пространстве при приеме этих сигналов в условиях малых отношений сигнал / помеха.

Использование известных методов простого перебора (последовательный поиск, метод слепого поиска), осуществляемых примерно за $N/2$ попыток, является неприемлемым при больших длинах последовательностей, состоящих из N дискретов. Проведенные исследования показали, что время поиска можно сократить вплоть до значений, близких к $\log_2 N$ попыток, что обеспечивает существенный выигрыш [2, 3].

Применение так называемых «пилот-сигналов», позволяющих обеспечить синхронный прием, по многим причинам, в том числе по проблемам скрытности, не всегда является приемлемым. Решение виделось в применении многоэтапных методов поиска с добавлением к передаваемому сигналу синхронизирующих псевдослучайных последовательностей, не коррелирующих с передаваемыми сигналами сообщений [4].

Заманчивым оказался поиск с использованием гребенчатых функций зависимости выходного сигнала от временного сдвига принимаемой и опорной последовательностей. В простейшем случае опорный сигнал может быть образован аддитивной смесью сдвинутых

во времени нескольких синхронизирующих сигналов, которыми могут быть любые псевдослучайные сигналы, в том числе и коды максимальной длины. Таким образом, пространство неопределенности делится на число частей, пропорциональных числу суммируемых сигналов, и находится одна из точек гребенчатой функции. На следующем этапе опорный сигнал образуется путем исключения из суммы определенных сдвигов опорного сигнала, например, четных. Гребенчатая функция прореживается и вновь ищется очередная точка. Если все пространство неопределенности каждый раз делится пополам, получается классический дихотомический поиск [1, 2, 5].

Существенным недостатком такого метода поиска является большая вычислительная сложность обработки, поскольку опорный сигнал является многоуровневым. Исследования показали, что опорные сигналы можно упростить путем их бинарного квантования. Выходные функции при этом также имеют гребенчатый вид. Надежность такой обработки несколько снижается, но, как правило, остается приемлемой.

Практические запросы, в частности, требование скрытности работы радиосистем, ставят задачу применения разнообразных по форме сигналов. Поэтому наличие даже достаточно эффективных методов поиска для отдельных видов сигналов не решает проблемы поиска в целом. В [6] предложен способ синтеза последовательностей, быстро входящих в синхронизм, основанный на двоичных решениях. В этом методе синтезируемая последовательность образуется как сумма взаимно ортогональных подпоследовательностей, периоды повторения которых удваиваются. Благодаря этому, оказывается возможным организовать быстрый многоэтапный (дихотомический) поиск. Идея этого способа была положена в основу оригинального способа, предложенного Лосевым В.В. [3] – ускоренного поиска *M*-последовательностей.

Заслуживающей внимания оказалась и идея построения троичных последовательностей для передачи информации и синхронизации, предложенная Лосевым В.В. [2, 7]. В этом методе используется смесь последовательностей быстрого поиска, предложенных Стифлером [8] и последовательностей максимальной длины, поскольку они компенсируют недостатки и дополняют достоинства друг друга. Последовательности Стиффлера, обладая хорошими синхронизирующими свойствами, не предназначены для передачи информации. Последовательности максимальной длины при инверсной манипуляции обладают высокой помехоустойчивостью, близкой к потенциальной, однако не являются оптимальными для синхронизации при ограничениях на сложность аппаратуры поиска.

Нельзя не отметить, что наряду с Лосевым В.В. проблемами поиска сложных сигналов занимались и другие исследователи. Так, целый ряд полезных результатов был получен Клюевым Л.Л. и его учениками, которые одновременно сотрудничали и с Лосевым В.В. Наиболее важные результаты были получены при исследовании синхронизирующих свойств двоичных последовательностей Велти [9]. Основными достоинствами этих последовательностей являются большой ансамбль, хорошие корреляционные свойства, простота генерирования и специфический алгоритм построения, позволяющий организовывать быстрые методы ускоренного поиска этих последовательностей.

Особого внимания заслуживает многоэтапный поиск с использованием вычислителя суммы модулей, описанный в работах [10]. В этом методе входной сигнал коррелируется с подпоследовательностями (отрезками) ожидаемого сигнала, полученные значения взаимокорреляционных функций складываются по модулю в течение длительности ожидаемого сигнала. От этапа к этапу длительность подпоследовательностей удваивается. В результате полученные функции суммы модулей имеют гребенчатый вид, расстояния между максимумами которых удваиваются от этапа к этапу, что позволяет организовать дихотомический поиск. Алгоритм поиска пригоден для любой последовательности ансамбля. Поэтому помимо синхронизирующих свойств последовательности Велти способны передавать и низкоскоростную информацию.

Помимо разработки ускоренных методов поиска сигналов были получены оценки среднего времени поиска и его дисперсии [4], разработаны программы моделирования и произведены расчеты на ЭВМ. Полученные результаты были весьма интересными в 70–80 гг. 20-го века и не теряют своей актуальности и по сей день.

MULTISTAGE SEARCH OF PSEUDORANDOM SEQUENCES

I.I. ASTROVSKY, A.I. MITSIUKHIN

Abstract

An analysis of methods for searching signals on the basis of pseudorandom sequences (low-speed codes correcting multiple errors) is carried out.

Keywords: multiple errors, low-speed code, pseudo-random sequence.

Список литературы

1. Поиск, обнаружение и измерение параметров сигналов в радионавигационных системах / Под ред. Ю.М. Казаринова. М.: Сов. радио, 1975.
2. *Лосев В.В., Бродская Е.Б., Коржик В.И.* // Поиск и декодирование сложных дискретных сигналов. М.: Радио и связь, 1988.
3. *Астровский И.И., Лосев В.В.* Об одном подходе к сокращению времени вхождения в синхронизм // Радиотехника и электроника». 1975. Вып. 4. С. 24–28.
4. *Астровский И.И., Клюев Л.Л.* Расчет статистических характеристик времени слепого сканирующего поиска с использованием теории марковских процессов // Изв. АН БССР, сер. физ.-техн. наук. 1975. № 4. С. 111–112.
5. *Астровский И.И., Клюев Л.Л.* Устройство синхронизации псевдошумовых сигналов по задержке / Авторское свидетельство № 520716.
6. *Стиффлер Дж.Дж.* Теория синхронной связи. М.: Связь, 1975.
7. *Астровский И.И., Лосев В.В.* Троичные последовательности для передачи информации и синхронизации // Изв. АН БССР, сер. физ.-техн. наук. 1975. № 1. С. 117.
8. *Stiffler J.J.* Rapid Acquisition Sequences // IEEE Trans on Inform Theory. 1968. Vol. IT-14, № 2. P. 221–225.
9. *Велти.* Четверичные коды для импульсного радиолокатора // Зарубежная радиоэлектроника. 1961. № 4. С. 3–19.
10. *Клюев Л.Л., Астровский И.И.* Синхронизация приемных устройств по задержке при приеме Д-последовательности // Радиотехника и электроника. 1975. Т. 20, № 1. С. 178–181.

УДК 004.56 (043.2)

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

М.Н. БОБОВ

ОАО «АГАТ-системы управления» – управляющая компания холдинга
«Геоинформационные системы управления»
Минск, 220114, Беларусь

Рассматриваются проблемы обеспечения кибербезопасности в современных инфокоммуникационных технологиях.

Ключевые слова: информационный ресурс, защита информации, кибербезопасность.

В настоящее время инфокоммуникационные технологии (ИКТ) стремительно развиваются, усиливая свое влияние на все ключевые сферы деятельности личности, организаций и государств. Внедрение ИКТ в процессы государственного управления является основой построения эффективного и социально ответственного демократического государства в XXI веке. В то же время, вместе со значительным ростом возможностей, проникновение ИКТ во все сферы жизни вызывает возникновение ряда новых и развитие уже существующих угроз личности, обществу и государству. Трансграничный характер ИКТ, их зависимость от сложных информационных технологий, активное использование площадок и сервисов ИКТ широкими группами граждан и организаций различных государств, обеспечивая новые возможности, создают и развивают новые угрозы для нанесения урона правам, интересам и жизнедеятельности личности, организации, государственных органов. К таким угрозам можно отнести:

– проведение кибератак против защищаемых информационных ресурсов со стороны киберпреступников и кибертеррористов;

– использование кибероружия в рамках специальных операций и кибервойн, в том числе сопровождающих традиционные боевые действия.

В настоящее время специалистами по защите информации выявлено целое множество кибератак, которые используют следующие известные инструменты: фишинг, троян, DDoS-атака, ботнет, backdoor, черви, классические файловые вирусы, вирус-вымогатель (шифровальщик), вредоносная программа (зловред), руткит, фрод, флуд (flood) [1]. Все многообразие инструментов кибератак используется для достижения их основной цели – проникновение в защищаемую инфокоммуникационную среду и установление над ней контроля. Как показывает исследование компании Fortinet [2], проводником преобладающей части успешных атак, с которыми довелось столкнуться организациям, стала широкомасштабная инфраструктура «Киберпреступление как услуга», которая обусловлена следующими факторами:

– готовность инструментов атак к применению в любое время и в любом месте;

– ускоренное распространение вредоносного программного обеспечения (ПО) за счет взаимопроникновения инфраструктур;

– снижение эффективности отслеживания состояния безопасности гибких распределенных инфраструктур.

Вместе с тем, в настоящее время создан и широко используется ряд сервисов и технологий, которые, с одной стороны, обуславливают эффективность функционирования современной инфокоммуникационной среды, а с другой стороны, являются легальным каналом проникновения в защищаемую инфокоммуникационную среду и установления над ней контроля. К таким сервисам и технологиям можно отнести:

– распространение программного обеспечения;
– обновление программного обеспечения;
– аппаратная виртуализация.

На рынке программного обеспечения действуют следующие основные способы распространения продуктов: продажа лицензий, сдача в аренду, распространение условно бесплатного программного обеспечения, распространение некоммерческого программного обеспечения, продажа или распространение программного обеспечения как услуги (Software as a Service, SaaS) и его разновидностей облачных вычислений и грид-вычислений. Производителями программного обеспечения также регулярно выпускаются обновления и патчи, которые, в основном, необходимы для достижения следующих целей:

– исправление имеющихся ошибок в программе;
– устранение обнаруженных уязвимостей или дыр безопасности;
– расширение функциональных возможностей программы.

Поэтому своевременное обновление ПО является таким же массовым и приоритетным сервисом, как и его распространение. Очевидно, что при массовом использовании ИТ-устройств требуются инструменты централизованного и удаленного управления и контроля. Поэтому на рынке предлагаются специальные утилиты, которые автоматически могут отслеживать обновления программ и устанавливать их.

Сложившаяся в настоящее время технология массового распространения и обновления ПО обуславливает необходимость тотального контроля его безопасности, т.к. поставляемое и обновляемое ПО может содержать программные закладки и недекларированные возможности (НДВ). Основная опасность программных закладок заключается в том, что, являясь частью защищенной системы, они способны принимать активные меры по маскировке своего присутствия в системе. Если программная закладка написана грамотно, то после того, как она внедрена в систему, обнаружить ее стандартными средствами администрирования очень трудно, поэтому она может функционировать неограниченно долгое время, и на протяжении всего этого времени внедривший ее злоумышленник имеет практически неограниченный доступ к системным ресурсам. Закладки могут наносить ущерб как отдельным пользователям и компаниям, так и целым государствам, например, ставя под угрозу обороноспособность страны. Опасность получить закладку зависит от надежности и порядочности разработчиков ПО, а также интереса со стороны спецслужб. Во многих случаях при разработке ПО программисты используют чужие библиотеки и открытое программное обеспечение (Open source), в котором могут быть как скрытые уязвимости, так и НДВ. Интерес для спецслужб представляют широко распространенные, используемые миллионами пользователей программы, а также государственные предприятия, производители военной техники и предприятия стратегически важных отраслей.

Основными мерами противодействия программным закладкам в настоящее время являются:

– проведение проверок ПО на наличие НДВ;
– использование «песочниц».

Проверки ПО на НДВ проводятся в специализированных лабораториях как вид сертификационных испытаний и состоят из следующих основных этапов: статический анализ, динамический анализ и ручной анализ исходного кода. Процесс сертификации ПО происходит по принципу тестирования исходного кода и сопоставления результатов данных проверок с описанием, содержащимся в специальных документах, предоставляемых вместе с ПО. В крупных компаниях поиск ошибок в программах и их тестирование – это отдельный этап, построенный по строго отлаженным методикам и проводимый большим количеством сотрудников. Сертификация на НДВ – еще одна дополнительная проверка, требующая длительного периода времени и больших финансовых затрат, что существенно поднимает стоимость конечного продукта. Вместе с тем, испытательные лаборатории, осуществляющие сертификацию на отсутствие НДВ, не обладают ни людскими, ни техническими ресурсами, позволяющими в массовом порядке на должном уровне и в кратчайшие сроки проводить процедуру проверки сложного ПО. Еще одной проблемой является то, что обновление ПО и установка исправлений являются нарушениями условий действия выданного сертификата

и требуют повторной процедуры проверки. Похожая ситуация возникает, если срок действия сертификата истек.

«Песочницы» используются для запуска непроверенного кода из небезопасных источников, как средство для обнаружения и анализа вредоносных программ. Она обычно представляет собой жестко контролируемый набор ресурсов для исполнения гостевой программы, например, место на диске или в памяти. Песочницы позволяют проводить автоматизированный статистический и динамический анализ подозрительных файлов в виртуализированной среде и при необходимости блокировать их. Это позволяет безопасно оценить «поведение» и последствия открытия подозрительного файла. Анализ файла проводится в автоматическом режиме в виртуальной среде, идентичной рабочей станции пользователя, и не требует от администратора системы специальных знаний в части анализа кода. Независимость от сигнатурных методов детектирования позволяет при использовании «песочницы» обнаружить вредоносный код «нулевого дня», специально разработанный (модифицированный) для проведения целевой атаки. Тем не менее, реализация описанных выше механизмов защиты требует значительных вычислительных ресурсов. Их реализация на уровне конечных рабочих станций невозможна либо неэффективна, поэтому производители предлагают специализированные программно-аппаратные комплексы, работающие на уровне сети. Повышенная безопасность исполнения кода в «песочнице» связана с большой нагрузкой на систему. Именно поэтому их используют только в случае выявления подозрительного кода.

Появление новых процессоров с поддержкой технологии аппаратной виртуализации расширило возможности, как для средств защиты информации, так и для средств, нарушающих информационную безопасность. Программное обеспечение, использующее технологию аппаратной виртуализации, работает в новом, более привилегированном, чем операционная система, режиме. С одной стороны, такое ПО, выполняющее функции монитора виртуальных машин (МВМ), повышает сервисные возможности электронной вычислительной машины (ЭВМ) и снижает стоимость ее эксплуатации. Но с другой стороны, появляется возможность для негласного внедрения программной закладки с бесконтрольными возможностями. В настоящее время подавляющее большинство процессоров Intel и AMD поддерживают технологию аппаратной виртуализации и поэтому потенциально все ЭВМ с такими процессорами подвержены угрозам нарушения информационной безопасности, поскольку становится возможной реализация тотального контроля компьютера. Основная задача состоит в захвате управления оборудованием виртуализации. Тот, кто первый захватил оборудование виртуализации, тот в состоянии создать для всех последующих желающих с ней поработать соответствующую программно-аппаратную среду. Для этой цели служит уже отработанная и реально существующая технология, основанная на использовании двух компонент, которые можно условно называть гипердрайвером и гиперагентом.

Гипердрайвер – программа, резидентно находящаяся в оперативной памяти и осуществляющая контроль над аппаратурой и программной средой вычислительной системы. Для ее работы используется аппаратная виртуализация центрального процессора, с помощью которой создается виртуальная среда, и в ней запускается операционная система. Основные функции гипердрайвера:

– обеспечивать работоспособности своего кода в любой программной среде;

– оставаться незамеченным для любых программных средств, загруженных на ЭВМ;

– осуществлять постоянный контроль выбранных аппаратных и программных объектов в вычислительной среде;

– обеспечивать связь с компонентами визуализации и управления его работой.

Гиперагент – программа, осуществляющая управление гипердрайвером и получение информации от гипердрайвера. Гиперагент организует интерфейс между гипердрайвером и пользователем системы. Эта программа функционирует на прикладном уровне и выполняет следующие функции:

– действует как редактор оперативной памяти, редактор памяти ввода / вывода (в адресном пространстве памяти), позволяет просматривать область БИОС;

– выполняет дампирование в файл заданных областей адресного пространства;

– оперативно выполняет сложные поисковые операции в памяти, используя для этого специально зарезервированный процессор в гипердрайвере;

– сохраняет в дампе события, связанные с выполнением команды CPUID (идентификация процессора);

– включает / выключает режим подстановок в блоках параметров, получаемых в результате выполнения команды CPUID.

При запуске гипердрайвер переводит процессоры в виртуальный режим, а последний из них изолирует от ЭВМ и использует исключительно для скоростного сканирования оперативной памяти. После развертывания гипердрайвера, уже находясь в виртуальном режиме, он осуществляет загрузку хостовой операционной системы.

Таким образом, гипердрайвер является средством оперативного и тотального контроля за любым аппаратным и программным ресурсом вычислительной системы. Это свойство определяет область его основного применения – регистрация интересующих программных и аппаратных событий, а также эмуляция несуществующего оборудования. С помощью гипердрайвера также могут подвергаться исследованию и контролю программные комплексы ядра гипервизоров, поскольку не представляет сложности пропустить гипервизор любой известной системы виртуализации под управлением ранее запущенного гипердрайвера. Размер кода гипердрайвера позволяет выполнить его безболезненное размещение в БИОС вместе с функциями из арсенала шпионских технологий. Универсальные способы размещения дополнительных программных модулей во флеш-памяти БИОС уже давно отработаны и используются даже в легальных коммерческих продуктах. Обнаружить в них программный код гипердрайвера, даже после выпаивания микросхемы флеш-памяти, абсолютно невозможно.

ACTUAL PROBLEMS OF CYBERSECURITY SUPPORT

M.N. BOBOU

Abstract

The problems of cybersecurity support in modern infocommunication technologies are considered.

Keywords: information resource, information security, cybersecurity.

Список литературы

1. ISO/IEC 27032 2012. «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности».
2. Tadviser [Электронный ресурс]. URL: https://www.tadviser.ru (дата обращения: 20.04.2018).

УДК 621.391 -047.58

АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ ФОРМИРОВАНИЯ И ОБРАБОТКИ СИГНАЛОВ

С.Б. САЛОМАТИН

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Рассматриваются методы и алгоритмы формирования и обработки сигналов с использованием конечных алгебраических структур в виде групп, колец и полей. Определяются преобразования, инвариантные к временным и пространственным сдвигам. Показывается эффективность алгоритмов обработки сигналов в спектральной области.

Ключевые слова: алгебраическая система, группа, кольцо, поле, смежный класс, дискретное преобразование Фурье.

Введение

Алгебраические системы, структурные теоремы алгебры и теории чисел лежат в основе большинства цифровых алгоритмов формирования и обработки сигналов. Основой таких алгоритмов является специальная организация массивов данных в виде конечных алгебраических структур (групп, колец, полей) [1–6].

Модели преобразования сигналов

Алгебра. **C**-алгебра A определяется как кольцо в **C**-векторном пространстве, для которого операции сложения в кольце и векторном пространстве совпадают [3–5]. Дополнительно для $\alpha \in C,\ g,\ h \in \mathrm{A}$, должно выполняться условие $\alpha(gh) = (\alpha g)h = g(\alpha h)$.

Модуль. Пусть A будет **C**-алгебра. Левый A-модуль определяется как **C**-векторное пространство M, в котором разрешены операции $\mathrm{A} \times \mathrm{M} \to \mathrm{M},\ (a,m) \to a \cdot m,$ причем, для $a,b,1 \in \mathrm{A}$ и $m,n \in \mathrm{M},\ a(m+n) = am + an,\ (a+b)m = am + bm,\ (ab)m = a(bm),\ 1 \cdot m = m.$

Модуль – абелева группа с кольцом операторов. Модуль является обобщением векторного (линейного) пространства над полем *K* для случая, когда *K* заменяется некоторым кольцом.

Примеры модулей.

1. Любая абелева группа M является модулем над кольцом целых чисел *Z*. Для $a \in Z$ и $m \in Z$ произведение *am* определяется как результат сложения *m a* раз.

2. В случае, когда A – поле, понятие унитарного A-модуля в точности эквивалентно понятию линейного векторного пространства над A.

Матрично-векторная модель. Многие алгоритмы цифровой обработки сигналов основываются на линейном преобразовании дискретного сигнала. Математически такое преобразование может быть записано с помощью матрично-векторного произведения $\mathbf{X} = \mathbf{M}\mathbf{x},$ где $x \in F^N$ – вектор дискретного сигнала; $\mathrm{M} \in F^{N \times N}$ – матрица преобразования над полем *F*; **X** – спектр сигнала.

Полиномиальная модель. В качестве моделей сигналов и фильтров преобразований можно использовать полиномы $S(z^{-1})$ и $H(z^{-1})$ степени *N*–1, а саму операцию фильтрации рассматривать как результат произведения полиномов. В таком представлении результат линейной фильтрации имеет более высокую степень полинома, чем полиномы сигналов

и фильтров, и фильтрация как алгебраическая форма не является замкнутой. Пространство сигналов можно замкнуть, используя операцию умножения по модулю $\left(z^{-N}-1\right)$ $H\left(z^{-1}\right)S\left(z^{-1}\right)\mathrm{mod}\left(z^{-N}-1\right)$.

В этом случае сигналы и фильтры располагаются в пространстве полиномов в z^{-1} по модулю $z^{-N}-1$, которое обозначается $\mathbf{C}\left[z^{-1}\right]/\left(z^{-N}-1\right)$ и называется полиномиальной алгеброй.

Модели сигналов и операторы сдвига

Модель сигнала определяется через тройку операторов (*A,* Ф*, M*), где *A* – алгебра фильтров, *M* – модуль сигналов, Ф – обобщенное биективное линейное отображение из векторного пространства (т.е. отсчетов сигнала) в модуль *M* [3, 4, 5].

Ключевую роль в алгебраической модели играет оператор сдвига. Вид сдвига тесно связан с моделью сигнала. В моделях конечных и бесконечных интервалов используются разные операторы сдвига. Другие операторы сдвига ведут к новым моделям сигналов и новым спектральным преобразованиям.

Модель временного сдвига. Модель временного сдвига (рис. 1, *а*) можно определить как $q\langle\rangle t_n = t_{n+1}$, где q – оператор сдвига; $\langle\rangle$ – операция сдвига; t_n – точка дискретного времени.

Модель ассоциируется с бесконечным или конечным *Z*-преобразованиями.

Модель пространственного сдвига. Пространственный сдвиг (рис. 1, *б*, *в*) в операторной форме можно записать как $q\langle\rangle t_n = \frac{1}{2}\left(t_{n-1}+t_{n+1}\right)$. С такой моделью ассоциируется дискретное косинусное преобразование (ДКП) [5, 6].

Покажем, что оператор *k*-го пространственного сдвига q_k может быть задан полиномом Чебышева $T_k(q)$: $q_k = T_k(a)$.

Действительно, можно записать следующие соотношения

$$q_{k+1}\langle\ \rangle t_n = \left(t_{n+k+1}-t_{n-k-1}\right)/2\ = \left(t_{n+k+1}+t_{n+k-1}+t_{n-k+1}+t_{n-k-1}\right)/2-\left(t_{n+k-1}+t_{n-k+1}\right)/2 =$$

$$= 2q\langle\ \rangle\left(t_{n+k}+t_{n-k}\right)/2-\left(t_{n+k-1}+t_{n-k+1}\right)/2 = \left(2qq_k-q_{k-1}\right)\langle\ \rangle t_n.$$

Напомним, что последовательность полиномов $T=\left(T_n \mid n\in Z\right)$, удовлетворяющая рекуррентному соотношению $T_{n+1}(v)=2vT_n(v)-T_{n-1}(v)$, называется последовательностью полиномов Чебышева [5, 6].

Используя рекуррентное свойство полиномов Чебышева, можно получить: $q_{k+1}=T_{k+1}(q)$.

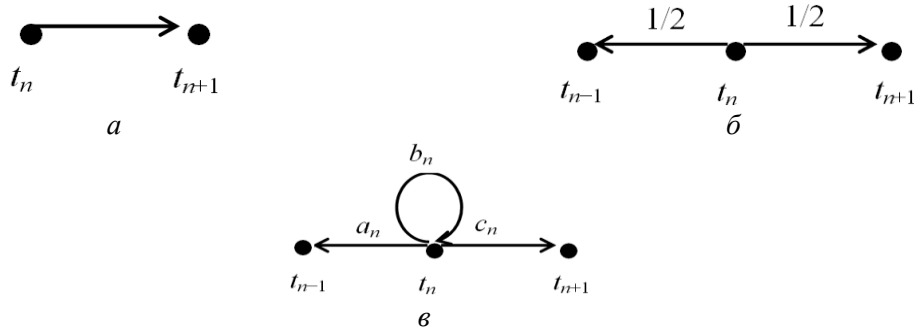


Рис. 1. Примеры возможных сдвигов в алгебраической модели: *а* – временной; *б* – пространственный; *в* – цепь сдвиговых состояний

Инвариантность к сдвигу. Инвариантность к сдвигу является ключевой концепцией обработки сигналов. В алгебраической теории это свойство имеет простую форму представления. А именно, если q оператор сдвига, а h – фильтр, то h обладает свойством инвариантности к сдвигу, если для всех сигналов s, $h(qs) = q(hs)$, что эквивалентно $hq = qh$.

Требование инвариантности к сдвигу для всех фильтров запишется как $q \cdot h = h \cdot q$, для всех $h \in A$.

Так как сдвиг q формируется A, то необходимо, чтобы A была коммутативна. Обратно, если A представляет собой коммутативную алгебру, то все фильтры $h \in A$ обладают свойством инвариантности к сдвигу.

Алгебры, инвариантные к сдвигу. В случае одного сдвига алгебра образуется одним элементом v. В бесконечномерном случае получаются алгебры ряда переменной v или полиномов произвольной степени от v. Если обработка ведется на конечных интервалах, то получаются алгебры полиномов вида $A = \mathbf{C}[v] / p(v)$, где p – полином степени n; $\mathbf{C}[v] / p(v)$ – множество всех полиномов степени меньшей, чем n, с операциями сложения и умножения по модулю $p(v)$. Векторное пространство алгебры A имеет размерность n.

Пример. Обозначим через C_N множество комплекснозначных N-периодических функций целочисленного аргумента $x = x(j),\ j \in Z$. Элементы этого множества можно условно называть сигналами. В C_N обычным способом вводятся операции умножения на комплексное число, сложения и умножения сигналов. А именно $y = cx \Leftrightarrow y(j) = cx(j),\ j \in \mathbf{Z}$; $y = x_1 + x_2 \Leftrightarrow y(j) = x_1(j) + x_2(j),\ j \in \mathbf{Z}$, $y = x_1 x_2 \Leftrightarrow y(j) = x_1(j) x_2(j),\ j \in \mathbf{Z}$.

В результате C_N становится коммутативной алгеброй с единицей. Единицей является сигнал **1**.

Обратный к x сигнал x^{-1} определяется из условия $x \cdot x^{-1} = 1$. Очевидно, что сигнал x обратим тогда и только тогда, когда все его отсчеты $x(j)$ отличны от нуля. В этом случае $x^{-1}(j) = \left[x(j)\right]^{-1},\ j \in Z$.

Модель сигнала на конечном интервале может быть построена с помощью алгебры $A = M = \mathbf{C}[v] / (v^N - 1)$, где $v = z^{-1}$, и отображения $\Phi : \mathbf{s} \to \sum_{0 \le n < N} s_n v^n \in M$, где сигнал $\mathbf{s} = (s_0, ..., s_{N-1}) \in V = \mathbf{C}^n$ допускает комплексные значения.

Пространственная модель сигнала может быть построена с помощью полиномиальной алгебры вида $A = M = \mathbf{C}[v] / T_N(v)$ и отображения $\Phi : \mathbf{s} \to \sum_{0 \le n < N} s_n T_n(v) \in M$, где T_n – полиномы Чебышева первого рода. Соответствующее Фурье-преобразование для этой модели носит название дискретного косинусного преобразования.

Модели дискретных спектральных преобразований

Рассмотрим алгоритм дискретного преобразования Фурье F [4]. Действие алгоритма F эквивалентно декомпозиции сигнального модуля в неприводимые компоненты, с помощью которых формируется спектр сигнала. Это созвучно декомпозиции векторного пространства в инвариантные подпространства с соответствующим линейным отображением. Алгебраическая структура дискретного преобразования Фурье (ДПФ), которая имеет декомпозицию матрицы для групповой алгебры $C[Z]$ циклической группы Z_N, состоящей из N элементов, запишется как $F_N : C[Z_N] \to C \oplus ... \oplus C$, где $\oplus$ – оператор прямой суммы.

В случае полиномиальной алгебры и сигнальной модели $A = M = \mathbf{C}[v] / p(v)$, и такая декомпозиция может быть описана с помощью китайской теоремы об остатках следующим образом: $F : \mathbf{C}[v] / p(v) \to \mathbf{C}[v] / (v - \alpha_0) \oplus ... \oplus \mathbf{C}[v] / (v - \alpha_{N-1})$. Здесь $H(z^{-1})$ и $\{\alpha_n\}$ – нули полинома p (предположительно различные). Предполагается, что $\mathbf{C}[v] / p(v)$ представляет собой полную декомпозицию. Если $p(v) = q(r(v))$, то возможна двухэтапная декомпозиция:

$\mathbf{C}[v] / p(v) \to \mathbf{C}[v] / (r(v) - \beta_0) \oplus ... \oplus \mathbf{C}[v] / (r(v) - \beta_{K-1})$

$\to \mathbf{C}[v] / (v - \alpha_0) \oplus ... \oplus \mathbf{C}[v] / (v - \alpha_{N-1})$,

где β_k – нули $q(v)$, $\deg(q) = K$.

Если $N = KM$, то получается алгоритм преобразования Фурье Кули–Тьюки, с помощью которого проводятся вычисления по модулю $p(v) = v^N - 1 = (v^M)^K$.

Такая структура позволяет обобщить понятие спектрального преобразования на другие классы сигналов.

Свойство декомпозиции ДПФ может быть распространено на произвольную конечную группу $G \neq Z_N$. Такой подход приводит к Фурье-анализу на группах. Использование $\mathbf{C}[G]$-модулей позволяет строить матрицы преобразований, обладающие свойствами симметрии, что удобно для дискретных преобразований, инвариантных к определенным классам сдвигам. Примером таких преобразований служит дискретное тригонометрическое преобразование.

Второе обобщение связано с выбором произвольного полинома $p(v) \neq v^N - 1$ и произвольного базиса $\mathbf{C}[v]/p(v)$. Такой подход приводит к полиномиальным преобразованиям. Так, если выбрать произвольный p и базис вида $\left(1, v, ..., v^N\right)$, то приходим к матричным структурам Вандермонда, имеющим большое значение для пространственно-временных преобразований.

Фурье-анализ на группах

Пусть G будет конечной группой. Построим из элементов группы базис следующего векторного пространства: $\mathbf{C}[G] = \{\sum_{g \in G} a_g g \mid a_g \in \mathbf{C}\}$.

Очевидно, что $\mathbf{C}[G]$ является векторным пространством, натянутым на элементы группы. Можно определить стандартный вид операции умножения в $\mathbf{C}[G]$, используя дистрибутивный закон и умножение элементов группы. Следовательно, $\mathbf{C}[G]$ представляет собой алгебру. С другой точки зрения, $\mathbf{C}[G]$ можно рассматривать как множество комплексных функций $g \to a_g$ на группе G. Регулярный модуль $M = A = \mathbf{C}[G]$ определяет сигнальную модель следующим образом. Если G состоит из n элементов, то получается множество $M = A = \mathbf{C}[G]$ и отображение $\Phi : \mathbf{C}^n \to \mathbf{C}[G]$, $\mathrm{s} \to \sum_{g \in G} s_g g$.

В данном случае сигнал и фильтры являются элементами алгебры групп. Операторами сдвига в группе G являются элементы, выбранные как образующие множества элементов группы. Если группа нециклическая, то G, а следовательно, и $\mathbf{C}[G]$ требуют, как минимум, двух образующих – генераторов или сдвигов. Если G некоммутативная группа, тогда не коммутативны и пары генераторов группы. Следовательно, определенная выше модель становится зависимой от сдвига.

Полиномиальные и групповые алгебры. Полиномиальные алгебры всегда коммутативны и ясно, что некоммутативная группа, ассоциированная с групповой алгеброй, не может быть полиномиальной алгеброй. С другой стороны, известно, что каждая групповая алгебра для коммутативной группы является полиномиальной алгеброй с очень специфической структурой.

Рассмотрим пример, когда коммутативная группа G представлена в виде прямого произведения циклических групп $G = \mathbf{Z}_{n_1} \times ... \times \mathbf{Z}_{n_m}$, где $\mathbf{Z}_{n_i}$ имеет размерность n_i, а образующим элементом является x_i. Тогда можно записать следующим образом:

$\mathbf{C}[G] = \mathbf{C}[x_1, ..., x_m] / < \{x_i^{n_i} - 1 \mid 1 \le i \le m\} >$.

В случае одной переменной (одномерный сигнал), G должна быть циклической, $G = Z_n$. В итоге получается следующее: $\mathbf{C}[\mathbf{Z}_n] = \mathbf{C}[v]/(v^n - 1)$.

Полученная алгебра ассоциирована с дискретным преобразованием Фурье размера n. Тот факт, что ДПФ ассоциировано с $C\left[Z_n\right]$, породил значительные усилия по развитию Фурье-анализа для других, некоммутативных групп, и по поиску алгоритмов быстрых вычислений. С другой стороны, понимание того, что некоммутативные группы создают зависимые от сдвига модели, сдерживает применение таких групп при обработке сигналов.

На рис. 2 показана схема пересечения областей существования алгебр.

Рис. 2. Структурное расположение алгебр и коммутативной группы

Модели на основе полиномиальной алгебры одной переменной

Пусть $p(v)$ – полином степени $\deg\{p\} = n$. Тогда класс вычетов по модулю p $A = \mathbf{C}[v]/\,p(v) = \{h(v) \,|\, \deg\{h\} < n\}$ является алгеброй со сложением полиномов и умножением полиномов по модулю p. Назовем такую алгебру полиномиальной алгеброй одной переменной. Полиномиальная алгебра всегда циклическая, т.е. формируется одним подходящим для этого элементом. Обычно это v, который является и оператором сдвига. Это означает, что все элементы в A получены путем последовательного возведения v в степени, суммирования и умножения на скаляр. Другими словами, элементы алгебры это полиномы переменной v.

Пример. Предположим, что $p(v) = (v-1)(v+1) = v^2 - 1$. Умножая два элемента v, $v+1 \in A$, можно получить $v(x+1) = v^2 + v \equiv v+1 \mod(v^2-1)$. Выражение читается следующим образом: $v^2 + v$ конгруэнтно (или равно) $v+1$ по модулю $v^2 - 1$. Таким образом, определяется равенство двух полиномом по модулю третьего полинома.

Модель сигналов. Выберем векторное пространство $V = C^n$, полиномиальную алгебру $A = \mathbf{C}[v]/\,p(v)$, $\deg\{p\} = n$ и модуль M = A. Далее выберем базис $\mathbf{b} = (\mathbf{p}_0, ..., \mathbf{p}_{n-1})$. Этот выбор позволяет определить конечную n-мерную сигнальную модель (A, M, Ф). Биективное линейное отображение Ф при этом будет иметь вид: $\Phi : \mathbf{C}^n \to M$, $\mathbf{s} \to \sum_{0 \le l < n} s_l p_l$, где $\mathbf{s} = (s_0, ..., s_{n-1})^T \in C^n$ – сигнальный вектор.

Заметим, что Ф играет роль Z-преобразования и зависит от выбора базиса b. Базисный элемент p_i образует в модуле M единичный импульс, т.е. в векторе $\mathbf{s}$ компонента $s_i = 1$, а остальные компоненты $s_l = 0$ для $l \ne i$.

Пример. Для рассмотренного выше примера зададим базис $\mathbf{b} = \{1, v\}$ в алгебре $M = A = \mathbf{C}[v]/(v^2 - 1)$. Сигнальная модель для векторного пространства $\mathbf{C}^2$ определится следующим образом: $\Phi : \mathbf{C}^2 \to M$, $(s_0, s_1) \to s_0 + s_1 v$.

Фильтрация. Сигнальная модель определяет фильтрацию на сигнальном пространстве M как операцию A на M. Алгебра A описывает пространство фильтров, а A-модуль – M-пространство сигналов. Заметим, что даже если множества A и M равны, их алгебраические структуры не равны. Например, A воздействует на M, но не наоборот, фильтры (элементы A) могут каскадироваться, т.е. умножаться, в то время как сигналы (элементы M) не могут.

Определим сигнал $s = \Phi(\mathbf{s}) = \sum_{0 \le l < n} s_l p_l \in M$ и фильтр $h \in A$. Тогда фильтрация сигнала s с помощью фильтра h запишется как $h \cdot s \in M$, т.е. произведение полиномов h и s по модулю p. Заметим, что так как результат принадлежит M, его тоже можно рассматривать как сигнал. Операция фильтрации или умножении на h – это линейного отображение, которое имеет матричное представление в базисе b $\varphi(h) \cdot \mathbf{s} \in \mathbf{C}^N$.

Пример. Пусть $h = h_0 + h_1 v \in A = \mathbf{C}[v]/(v^2 - 1)$ – произвольный фильтр. Вычислим матрицу $\varphi(h)$ его преобразования в базисе $\mathbf{b} = (1, v)$. Столбцы матрицы представляют собой отклики фильтра на воздействия базисных компонентов:
$h \cdot 1 = h_0 + h_1 v \in M$, $h \cdot v = h_0 v + h_1 v^2 \equiv h_1 + h_0 v \mod(v^2 - 1)$.

Следовательно, $\varphi(h)=\begin{bmatrix} h_0 & h_1 \\ h_1 & h_0 \end{bmatrix}$ и $h\cdot s \Leftrightarrow \varphi(h)\cdot \mathbf{s}$.

Спектры и Фурье-преобразование

Предположим, что $p(v)$ сепарабельный полином вида $p(v)=\prod_{k=0}^{N-1}(v-\alpha_k),\ \alpha_k\neq\alpha_l$, для $k\neq l$.

Преобразование Фурье сигнала s можно записать в виде отображения или регулярного модуля M: $\Delta:\mathbf{C}[v]/p(v)\to\mathbf{C}[v]/(v-\alpha_0)\oplus\ldots\oplus\mathbf{C}[v]/(v-\alpha_{N-1}),\quad s=s(v)\to(s(\alpha_0),\ldots,s(\alpha_{N-1}))$. Компонента регулярного модуля $M_k=\mathbf{C}[v]/(v-\alpha_k)$ имеет размерность 1. Следовательно, элементы (векторы) $\mathbf{C}[v]/(v-\alpha_k)$ являются полиномами степени 0 или скалярами $c\in\mathbf{C}$. Далее M_k представляет собой A-модуль, т.к. $h=h\in A, c\in M_k$ и $h(v)c\equiv h(\alpha_k)c \mod(v-\alpha_k)\in M_k$. Спектральное преобразование можно рассматривать как проекцию сигнала $s\in\mathbf{C}[v]/p(v)$ на модуль $\mathbf{C}[v]/(v-\alpha_k)$: $s(v)\equiv s(\alpha_k) \mod(v-\alpha_k)$.

Множество одномерных, неприводимых подмодулей $M_k=\mathbf{C}[v]/(v-\alpha_k)$ составляют спектр сигнального пространства M. Каждый подмодуль M_k одновременно формирует собственное пространство всех фильтров (или линейных систем) в A.

Спектр сигнала $s\in M$ можно рассматривать как вектор $\Delta(s)=(s(\alpha_0),\ldots,s(\alpha_{N-1}))$, а скаляр $s(\alpha_k)$ – как его компоненту.

Пример. Найдем спектр Фурье сигнала $s(v)=1+3v$. Запишем преобразование Фурье в полиномиальной форме: $\Delta:\mathbf{C}[v]/(v^2-1)\to\mathbf{C}[v]/(v-1)\oplus\mathbf{C}[v]/(v+1)$. Корни полинома $p(v)$ равны $\alpha_0=1;\ \alpha_1=-1$. Спектр сигнала $s=s(v)\to S=(s(1),s(-1))=(4,-2)$.

Матричная форма преобразования Фурье. Преобразование Фурье – это линейное отображение, которое имеет матрицу преобразования **F**, соответствующую выбранному базису $\mathbf{b}=(\mathbf{p}_0,\ldots,\mathbf{p}_{N-1})$ Столбцы матрицы **F** определяются как коэффициенты полинома $p_l(v)\equiv p_l(\alpha_k) \mod(v-\alpha_k)$. Соответственно, l-й столбец матрицы равен вектору $[p_l(\alpha_0),\ldots,p_l(\alpha_{N-1})]^T$.

Диагонализирующие свойства преобразования Фурье. Пусть F будет Фурье преобразование для регулярного A-модуля $C[v]/p(v)$ в базисе **b** и соответствующая матрица преобразования φ. Тогда преобразование $\mathbf{FAF}^{-1}=diag(a_0,\ldots,a_{N-1})$ диагонализирует матрицу **A**, если $\mathbf{A}=\varphi(h)$, где фильтр $h\in A$.

В частности, F диагонализирует матрицу сдвига $\varphi(v)$, поскольку оператор сдвига v имеет частотный отклик, равный $(\alpha_0,\ldots,\alpha_{N-1})$. Рассмотренное свойство позволяет найти механизм фильтрации в частотной области. Действительно, рассмотрим соотношение $\varphi(h)\mathbf{s}=\mathbf{F}^{-1}\mathbf{F}\varphi(h)\mathbf{F}^{-1}\mathbf{Fs}=\mathbf{F}^{-1}diag(h(\alpha_0),\ldots,h(\alpha_{N-1}))\mathbf{Fs}$, которое показывает, что умножение матрицы преобразования φ на вектор s во временной области равносилен умножению в частотной области его спектра **Fs** на диагональную матрицу $diag(h(\alpha_0),\ldots,h(\alpha_{N-1}))$.

Применение алгебраических спектральных преобразований

Смежно-групповое спектральное преобразование Фурье [7]. Пусть над полем комплексных чисел задан характер $\exp(\mp j2\pi/M)$ конечной циклической группы порядка M, тогда элементы $\exp(\mp j2\pi p\vartheta/M)$, $p,\vartheta=0,1,\ldots M-1,\ M=L\tilde{Q}$ удовлетворяют условию замкнутости относительно операции умножения и ассоциативности. Из группы выделим подгруппу $\Psi=\{\exp(-j2\pi lk/L),\ l,k=0,1,\ldots L-1\}$. Произведение подгруппы на элемент группы

$a(q)=\exp(-j2\pi ql/M)$, $l=0,\ldots,L-1$ образует смежный класс по подгруппе Ψ с параметром q, где $q=0,1,\ldots\tilde{Q}-1$. Подгруппу Ψ можно рассматривать как матрицу дискретно-экспоненциальных функций (ДЭФ) дискретного преобразования Фурье (ДПФ):
$\mathbf{W}\equiv\mathbf{W}(l,k)=\{\exp(-j2\pi lk/L),\ l.k=0,1,\ldots,L-1\}$,
тогда с учетом произведения $\mathbf{W}(l,k)\exp(-j2\pi qk/M)$ ядро смежно-группового преобразования Фурье будет иметь вид $\exp\left(-j2\pi l\left(q+k\tilde{Q}\right)/M\right)$.

Свойство вращения ядра преобразования Фурье. В ДПФ нулевой спектральный коэффициент определяется при угле $\theta=0$ рад радиус-вектора на Z-плоскости. С учетом смежных классов угол поворота радиус-вектора для нулевого спектрального коэффициента определяется из ядра преобразования при $l,q=1,\ k=0$ и равен $\vartheta=2\pi/M$ рад, что соответствует вращению ядра ДПФ.

Смежно-групповое спектральное (СГС) преобразование Фурье обладает свойством интерполяции спектра сигнала. Причем длина СГС-преобразования меньше длины преобразования ДПФ в количество смежных классов.

Матричное СГС-преобразование обладает свойствами циклического сдвига компонентов спектра сигнала. Величина сдвига определяется коэффициентом кратности значения смежного класса по отношению к количеству смежных классов.

Контраст спектральных коэффициентов и точность оценки частоты сигнала в матричном смежно-групповом спектральном преобразовании пропорционально зависят от числа смежных классов при фиксированной длине преобразования.

Алгоритм формирования частотно-манипулированного (ЧМ) и кодо-фазо-манипулированного (КФМ) сигналов. Алгоритмы управления матрицами циклического сдвига и матрицей образующего смежных классов в СГС-преобразовании могут быть использованы для формирования ансамблей кодовых сигналов с фазовой манипуляцией [7]. Причем углы скачков фазы и значения частот в формируемых сигналах контролируются числом смежных классов. На рис. 3 приведена схема формирования сигнала с динамически изменяемой структурой.

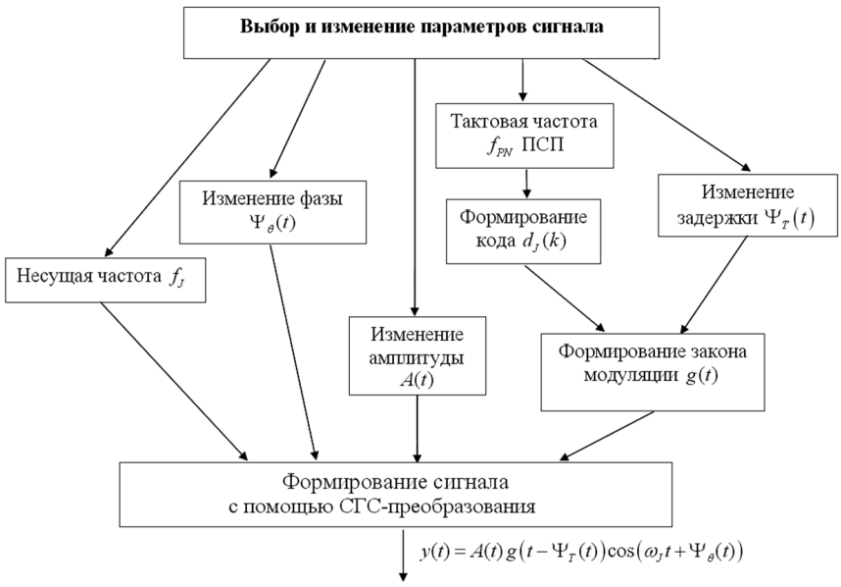


Рис. 3. Схема формирования сигнала с динамически изменяемой структурой

Алгоритмы оценки частоты и задержки сигнала

Пусть определен спектр $F^{0,0}\{E\}=\tilde{E}(k),k=0,1,\ L-1$ сигнала $E(l)$. Известно, что при циклическом сдвиге сигнала на величину m, его спектр будет иметь вид: $\tilde{E}_m(k)=\tilde{E}(k)\exp(j2\pi mk/L)$. Оценка задержки сводится к оценке параметра m. Таким образом,

задачи оценки частоты и задержки могут быть решены методами спектральных преобразований [7, 8]. Алгоритмы оценки позволяют построить процедуры быстрого последовательно-параллельного поиска сложного сигнала на основе многоканального смежно-группового спектрального преобразования с повышенной точностью оценки частоты (рис. 4).

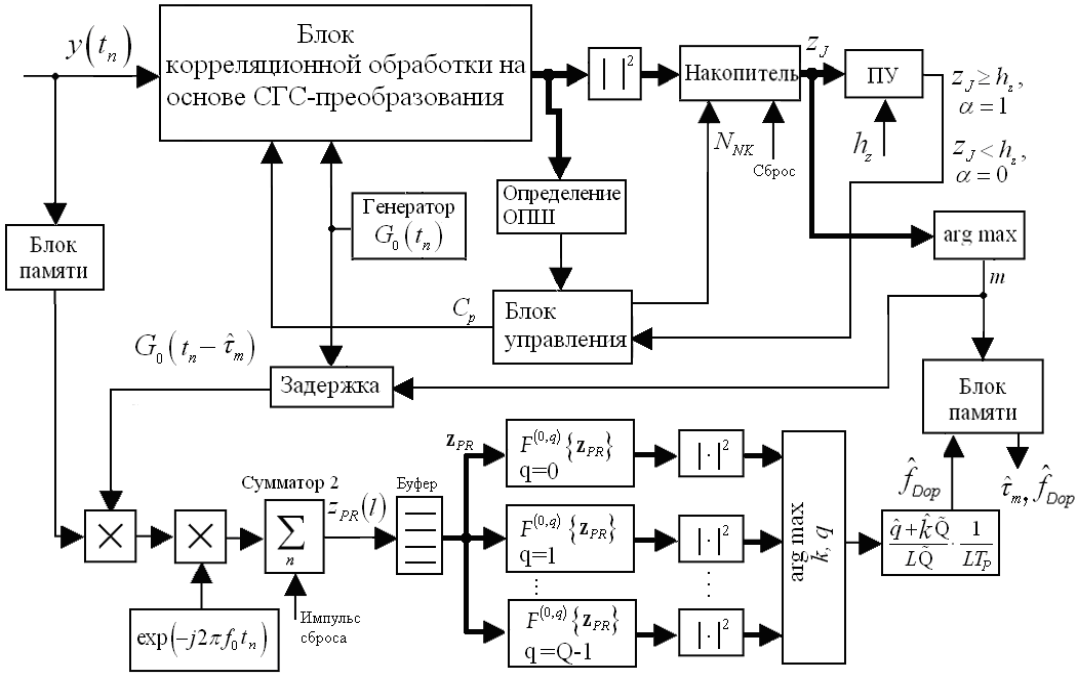


Рис. 4. Структура обнаружителя-измерителя сложного сигнала

При использовании алгоритма БПФ по основанию 2 вычислительная сложность Q-канального СГС-преобразования размерности L составляет $\tilde{Q}L\log_2 L$ операций сложения, $\tilde{Q}\left(0{,}5L\log_2(L)+L\right)$ операций комплексного умножения.

Заключение

Построены модели сигналов и их преобразований во временной и спектральной области с использованием механизмов теории групп, колец и полей. Определены свойства смежно-групповых преобразований, позволяющие разработать схемы формирования сигналов с динамически изменяющей структурой и разработать алгоритмы оценки частоты и задержки.

ALGEBRAIC SYSTEMS OF SIGNALS FORMATION AND PROCESSING

S.B. SALOMATIN

Abstract

Methods and algorithms of signal formation and processing using finite algebraic structures in the form of groups, rings and fields are considered. The transformations invariant to time and spatial shifts are determined. The efficiency of signal processing algorithms in the spectral region is shown.

Keywords: algebraic system, group, ring, field, adjacent class, discrete Fourier transform.

Список литературы

1. *Лосев В.В.* Микропроцессорные устройства обработки информации. Алгоритмы цифровой обработки: учебное пособие для вузов. Минск: Вышэйшая школа, 1990.
2. *Блейхут Р.* Быстрые алгоритмы цифровой обработки сигналов: Пер. с англ./Р. Блейхут. М.: Мир, 1989.
3. *Вариченко Л.В., Лабунец В.Г., Раков М.А.* Абстрактные алгебраические системы и цифровая обработка сигналов. Киев: Наукова думка, 1986.
4. *Саломатин С.Б.* Цифровая обработка сигналов в радиоэлектронных системах. Минск: БГУИР, 2002.
5. *Pueschel M., Moura J.M.F*. Algebraic Theory of Signal Processing [Electronic recourse]. URL: http:arxiv.org/abs/cs.IT/0612077 (date of access: 19.04.2018).
6. *Саломатин С.Б.* Моделирование алгоритмов быстрой обработки сигналов в инфокоммуникационных сетях: учеб.-метод. пособие. Минск: БГУИР, 2016.
7. *Ходыко Д.Л., Саломатин С.Б.* Смежно-групповые спектральные преобразования сложных сигналов // Докл. БГУИР. 2012. № 5 (67). С. 93–98.
8. *Ходыко Д.Л., Саломатин С.Б.* Многоканальный частотно-временной адаптивный фильтр на основе двойного смежно-группового преобразования // Докл. БГУИР. 2012. № 6 (68). С. 56–62.

УДК 621.391.037.372

АЛГЕБРАИЧЕСКИЕ ПРОСТРАНСТВЕННО-ВРЕМЕННЫЕ КОДЫ

С.Б. САЛОМАТИН

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Рассматриваются методы построения пространственно-временных кодов на основе теории решеток, алгебраических чисел и алгебраических систем с делением. Приводятся и анализируются основные алгоритмы декодирования пространственно-временных кодов на основе алгебраических моделей каналов и систем обработки сигналов.

Ключевые слова: алгебраическое число, теория решеток, пространственно-временной код, сигнал.

Введение

С математической точки зрения для построения кода для заданного целого n требуется определить кодовую книгу $C_G \subset \mathrm{M}_n(F)$, кодовые слова которой принадлежат n-мерному пространству M над полем F [1–6].

Кодовая книга имеет вид множества матриц, размером $n \times M$, над полем F. Кодовые матрицы должны удовлетворять условию полноты разнесения, т.е. свойству, согласно которому разность двух различных матричных элементов кода C имела отличный от нуля определитель. Желательно, чтобы код C_G обладал свойствами неисчезающей положительности определителя, реализовывал полную скорость информационного сигнала, имел удобную для реализации форму символов и равномерное распределение средней передаваемой мощности.

Алгебраические структуры

Решетка Λ определяется как дискретная, имеющая базис, абелева подгруппа действительных или комплексных n-мерных векторных пространств $\mathbf{V}$, т.е. $\mathbf{V} = R^n$

Пусть Λ формируется с помощью базиса $\{\boldsymbol{\beta}_1,...,\boldsymbol{\beta}_n\}$. Тогда решетку $\Lambda \subset \mathbf{V}$ можно записать следующим образом [3, 4, 7, 8]:

$$\Lambda = \left\{ \sum_{i=1}^{k} z_i \boldsymbol{\beta}_i \mid z_i \in Z \right\},$$

где $k \le n$ – ранг решетки. Решетка имеет полный ранг, если $k = n$.

Объем основного параллелепипеда решетки обозначается как $\mathrm{vol}(\Lambda)$ и определяется через гипермеру множества $\left\{ \sum_{i=1}^{k} x_i \beta_i \mid 0 \le x_i < 1 \right\}$.

Матричное представление полных решеток $\Lambda \subseteq \mathbf{V}$ задается порождающей матрицей $\mathbf{M}$, строками которой являются векторы базиса $\left\{ \boldsymbol{\beta}_i = (\beta_{i,1},...,\beta_{i,n}), i = 1,...,n \right\}$.

Объем решетки может быть вычислен через определитель порождающей матрицы $\mathrm{vol}(\Lambda) = \det(M) = \det\left(\left[\beta_{i,j} \right] \right)$.

Матрица Грамма решетки Λ имеет следующий вид: $\mathrm{Gram}(\Lambda) = MM^{\mathrm{T}}$ – для действительных чисел; $\mathrm{Gram}(\Lambda) = MM^{H}$ – для поля комплексных чисел, где T и H – операторы транспонирования и эрмитового сопряжения матриц.

Отсюда объем решетки запишется следующим образом: $\mathrm{vol}(\Lambda) = \sqrt{\det(Gram(\Lambda))}$.

Решетка называется ортогональной, если ее базисные векторы ортогональны друг другу. Матрица Грамма в этом случае имеет вид диагональной матрицы.

Примеры решеток представлены на рис. 1.

а *б*

Рис. 1. Примеры дискретных решеток: *а* – решетка гауссовских целых чисел, Z^2-эквивалентное множество – кольцо комплексных целых; $Z[i] = \{a + bj \mid a,b \in Z, j = \sqrt{-1}\}$; *б* – решетка гексагональной форме, построенная с помощью алгебры A^2 (решетка целых чисел Эйнштейна)

Алгебраические поля чисел

Рассматрим поле комплексных чисел *C*. Понятие алгебраического поля подразумевает, что все его элементы являются корнями полиномиального уравнения с коэффициентами из *Q*. Алгебраическое поле целых состоит из чисел, являющихся корнями полиномиального уравнения с целыми коэффициентами из *Z* [3, 7, 8].

Поля Галуа и поля комплексных чисел. Рассмотрим расширенное алгебраическое поле *E*/*F* степени *n*. Обозначим кольцо целых чисел поля *E* как O_E. Кольцо O_E также имеет единственный максимальный порядок *E*. Расширение называют простым, если $E = F(\alpha)$, $\alpha \in E$. Алгебраическое расширение использует неприводимый полином. Обозначим минимальный полином элемента поля α как μ_α, степень которого $\deg(\mu_\alpha)$ определит степень расширенного поля.

Пример. Пусть $O(i)/O$ простое алгебраическое расширение степени 2 с минимальным полиномом $\mu_i = x^2 + 1$. Тогда кольцо целых $O_{Q(i)} = Z[i]$ и $O_Q = Z$.

Пример. Пусть $Q(\sqrt{5})/Q$ простое алгебраическое расширение степени 2 с кольцом целых $O_{Q(\sqrt{5})} = Z\left[\left(1+\sqrt{5}\right)/2\right]$ и $O_Q = Z$. Минимальный полином элемента $\theta = \left(1+\sqrt{5}\right)/2$ равен $\mu_\theta(x) = x^2 - x - 1$. Пусть полином $p(x) = F[x]$ имеет один корень в *E*. Поле называется нормальным, если, все корни $p(x)$ также лежат в *E*. Нормальное алгебраическое числовое расширенное поле E/F называется полем Галуа. Автоморфизмы такого поля формируют группу Галуа. $Gal(E/F) = \{\sigma_1, \ldots \sigma_n\}$. Норма элемента $e \in E$ определяется следующим образом: $N_{E/F}(e) = \sigma_1(e) \ldots \sigma_n(e) \in F$.

Группу $Gal(E/F)$ можно рассматривать как группу перестановок корней минимального полинома.

Пример. $Q(i)/Q$ образует циклическую группу Галуа, формируемую операцией комплексного сопряжения: $\sigma = *$: $H(z^{-1})Gal(Q(i)/Q) = \langle * \rangle = \{*, *^2\} = \{jd, *\} = \{j \mapsto j, j \mapsto -j\}$.

Пример. Поле $Q\left(\sqrt{5}\right)/Q$ образует циклическую группу Галуа с помощью отображения $\sigma:\sqrt{5}\mapsto-\sqrt{5}:\ H(z^{-1})Gal\left(Q\left(\sqrt{5}\right)/Q\right)=\langle\sigma\rangle=\left\langle\sigma,\sigma^2\right\rangle=\{jd,\sigma\}$.

Решетки расширенного поля

Предположим для простоты, что имеется циклическое расширение Галуа, т.е. $\sigma(E)\subseteq R$ для всех $\sigma\in Gal(E/F)$. Используя операцию канонического встраивания $\psi:E\to R^n$, можно получить: $\psi(e)=\left(e,\sigma(e),...,\sigma^{n-1}(e)\right),\forall e\in E$.

Тогда $\psi(O_E)\subseteq R^n$ является решеткой с неисчезающим минимальным расстоянием: $d_{p,\min}\left(\psi(O_E)\right)=\min_{e\in O_E}\prod_{i=0}^{n-1}\sigma^i(e)=\min_{e\in O_E}N_{E/F}(e)=1$.

Пример. Пусть $E=Q\left(\sqrt{5}\right),\ F=Q$ с $Gal(E/F)=\left\{jd,\sigma:\sqrt{5}\to-\sqrt{5}\right\}$ и $O_{Q(\sqrt{5})}=Z[\theta]$, $\theta=\left(1+\sqrt{5}\right)/2,\ \tilde{\theta}=\sigma(\theta)=\left(1-\sqrt{5}\right)/2$.

Бесконечное множество векторов решетки формирует операция встраивания $\psi(a+b\theta)=\left(a+b\theta,a+b\tilde{\theta}\right),\ a,\ b\in Z$.

Конечная решетка может быть получена, если ввести ограничение $|a|.|b|\le M$ для $M\in 2Z$. Сигнальное созвездие M-PAM состоит из нечетных целых [1, 2, 9, 10]: $H(z^{-1})2-\text{PAM}=\{-1,1\},...4-\text{PAM}=\{\pm1,\pm3\},...$.

Используя полученную решетку для 4-PAM, можно получить кодовую книгу размером 16:
$C=\{\left(1+\theta,1+\tilde{\theta}\right),\left(1-\theta,1-\tilde{\theta}\right),\left(-1+\theta,-1+\tilde{\theta}\right),\left(-1-\theta,-1-\tilde{\theta}\right),\left(1+3\theta,1+3\tilde{\theta}\right),\left(1-3\theta,1-3\tilde{\theta}\right),$
$\left(-1+3\theta,-1+3\tilde{\theta}\right),\left(-1-3\theta,-1-3\tilde{\theta}\right),\left(3+\theta,3+\tilde{\theta}\right),\left(3-\theta,3-\tilde{\theta}\right),\left(-3+\theta,-3+\tilde{\theta}\right),\left(-3-\theta,-3-\tilde{\theta}\right),$
$\left(3+3\theta,3+3\tilde{\theta}\right),\left(3-3\theta,3-3\tilde{\theta}\right),\left(-3+3\theta,-3+3\tilde{\theta}\right),\left(-3-3\theta,-3-3\tilde{\theta}\right)\}$.

Полученная решетка не является ортогональной структурой. В общем случае ортогонализация решетки не всегда возможная операция. Однако в рассматриваемом случае эту операцию можно выполнить, используя идеал решетки. Элемент $\alpha=3-\theta$ формирует основной идеал O_E. Запишем кодовую книгу в виде: $C=\left\{\left(\sqrt{\alpha}a+b\theta,a+b\tilde{\theta}\right)\,|\,|a|,|b|\le M\right\}$, что позволяет получить ортогональную решетку.

Задача оптимизации. Часто требуется получение решеток, $\psi(O_E)\subseteq R^n$, имеющих полное разнесение [3, 7, 8]. Для решения этой задачи используют инвариант, который носит название определителя.

Пусть $\{\boldsymbol{\beta}_1,...,\boldsymbol{\beta}_n\}$ – базис E над Q и $Gal(E/Q)=\{\sigma_1,...,\sigma_n\}$. Определитель задается выражением $d_E=\left[\det\left(\sigma_i(\boldsymbol{\beta}_i)\right)\right]^2$. Для решетки $\Lambda=\psi(O_E)\subseteq R^n$ ее объем равен $\text{vol}\left(\psi(O_E)\right)=2^{-n}\sqrt{|d_E|}$.

Следовательно, если минимизируется объем решетки, то минимизируется и ее определитель.

Для получения кода с порядком разнесения, равным *n*, необходимо, чтобы минимальный ранг матрицы $D\left(X^i,X^j\right)$ для любых $i\ne j$ был равен *n*. В свою очередь, для получения максимальной энергетической эффективности также необходимо, чтобы выполнялся критерий определителя (детерминанта) – минимальный определитель матрицы $D(X^i,X^j)$

был максимален. При этом $D(X^i, X^j) = \left(X^i - X^j\right)^H \left(X^i - X^j\right), i \neq j$, где X^i и X^j – две различные матрицы в пространственно-временном коде.

Коды на основе алгебраических систем с делением

Алгебраические системы с делением, являющиеся алгебрами над полем действительных чисел – системы комплексных чисел, кватернионов и октав.

Алгебра кватернионов. Пусть $\alpha, \beta \in F^*$. Алгеброй A обобщенных кватернионов над F называется 4-мерное векторное пространство с базисом $\mathrm{B} = \{e, i, j, k\}$. Будем считать, что e является единицей, т.е. $e^2 = e, ej = j$ и т.д. Зададим равенства $i^2 = -e\alpha,\ j^2 = -e\beta$, где α и β произвольные элементы поля F, и $ij = -ji = k$. Тогда $k^2 = ijij = -iijj = -e\alpha\beta$, $ik = iij = -e\alpha j = -j\alpha,\ ki = -jii = +ie\alpha = j\alpha,\ ik = -jji = +e\beta i = i\beta,\ kj = ijj = -ie\beta = -i\beta$.

Получившаяся алгебра A называется алгеброй обобщенных кватернионов. Ее элементы выглядят следующим образом: $\mathbf{x} = e\mathbf{x}_0 + i\mathbf{x}_1 + j\mathbf{x}_2 + kx_3, \{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4\} \in F$.

Элементы $e\mathbf{x}_0$ и $\mathbf{x}_0$ отождествляются, и поле F оказывается вложенным в алгебру A.

Матричное представление алгебры обобщенных кватернионов A получается тогда, когда она рассматривается как двойной модуль, для которого A служит областью левых, а $\Sigma = F(i)$ – областью правых мультипликаторов. Если считать, что $-\alpha$ не является квадратом в поле F, тогда $\Sigma = F(i) = F\left(\sqrt{-\alpha}\right)$ – поле.

Алгебра является двумерным векторным пространством над этим полем. В качестве базисных элементов можно взять, например, e и $-j$. Тогда векторы $\mathbf{x}$ представляются следующим образом: $\mathbf{x} = e(\mathbf{x}_0 + i\mathbf{x}_1) + (-j)(-\mathbf{x}_2 + i\mathbf{x}_3)$.

Если векторы $\mathbf{x}$ умножить справа на произвольный элемент, то получится линейное преобразование векторного пространства A, которое может быть представлено некоторой матрицей. Ее столбцы получаются, если умножить базисные элементы e и $-j$ на произвольный элемент. Если в качестве последнего используется j, k или l, то получатся следующие матрицы:

$$J = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix},\ K = \begin{bmatrix} 0 & \beta \\ -1 & 0 \end{bmatrix},\ L = \begin{bmatrix} 0 & i\beta \\ i & 0 \end{bmatrix}.$$

Если выбрать $\alpha = \beta = 1$, то получатся гамильтоновы кватернионы, алгебра H: $\mathbf{x} = e\mathbf{x}_0 + i\mathbf{x}_1 + j\mathbf{x}_2 + k\mathbf{x}_3$, с правилами оперирования $i^2 = j^2 = k^2 = -1,\ ij = k,\ ji = -k,\ jk = i,\ kj = -i,\ ki = j,\ ik = -j$.

Если F – вещественное числовое поле, то в матричном представлении алгебры элемент i может быть заменен на мнимую единицу $j = \sqrt{-1}$ Тогда получится:

$$J = \begin{bmatrix} j & 0 \\ 0 & -j \end{bmatrix},\ K = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},\ L = \begin{bmatrix} 0 & j \\ j & 0 \end{bmatrix}.$$

Если в качестве базисных элементов алгебры взять все элементы конечной группы, то получится групповое кольцо этой конечной группы.

Код Аламоути. Пусть $\{1, i, j, k\}$ будет базис 4-мерного векторного пространства над R. Гамильтонов кватернион представляет собой множество $\mathrm{H} = \{x + yi + zj + wk \mid z, y, z, w \in R\}$.

Гамильтоновы кватернионы являются алгеброй с делением. Кватернион, сопряженный с $q = x + yi + zj + wk$, определяется как $\tilde{q}^* = x - yi - zj + wk$.

Норма кватернионов задается следующим образом: $q\tilde{q}^* = x^2 + y^2 + z^2 + w^2;\ x, y, z, w \in R$.

Инверсный к q кватернион определяется по формуле $q^{-1} = \tilde{q}^* / q\tilde{q}^*$.

Любой кватернион $q = x + yi + zj + wk$ может быть записан в виде $(x + yi) + j(z - wi) = \alpha + j\beta,\ \alpha, \beta \in C$.

Умножим на q форму $(\gamma + j\delta)$:

$$\underbrace{(\alpha + j\beta)}_{q}(\gamma + j\delta) = \alpha\gamma + j\tilde{\alpha}^*\delta + j\beta\gamma + j^2\tilde{\beta}^*\delta = (\alpha\gamma - \tilde{\beta}^*\delta) + j(\tilde{\alpha}^*\delta + \beta\gamma).$$

Перепишем это равенство, используя матричную форму в базисе $\{1, j\}$:

$$\begin{bmatrix} \alpha & -\tilde{\beta}^* \\ \beta & \tilde{\alpha}^* \end{bmatrix}\begin{bmatrix} \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} \alpha\gamma - \tilde{\beta}^*\delta \\ \tilde{\alpha}^*\delta + \beta\gamma \end{bmatrix}.$$

Отсюда получаем код Аламоути: $q = \alpha + j\beta,\ \alpha, \beta \in C \Leftrightarrow \begin{bmatrix} \alpha & -\tilde{\beta}^* \\ \beta & \tilde{\alpha}^* \end{bmatrix}$.

Циклическая алгебра и Golden код. Для дальнейшего изложения полезно рассмотреть поля алгебраических чисел и ввести понятие циклической алгебры.

Пусть α – алгебраическое число над полем рациональных чисел Q, т. е. число, которое является корнем многочлена с рациональными коэффициентами $g(x) = b_0x^n + b_1x^{n-1} + ... + b_n = 0.$

Используя алгебраическое число α, можно построить множество чисел вида:

$\omega = a_0 + \alpha a_1 + \alpha^2 a_2 + ... + \alpha^{n-1}a_{n-1}.$

Относительно обычных операций сложения и умножения, определенных для многочленов $\alpha_n = \frac{b_1}{b_0}\alpha^{n-1} + \frac{b_2}{b_1}\alpha^{n-2} + ... + \frac{b_n}{b_{n-1}}$.

Множество таких чисел образует поле $Q(\alpha)$ алгебраических чисел степени *n*. Процесс построения поля $Q(\alpha)$ называется расширением поля рациональных чисел Q с помощью алгебраического числа α.

Пример. Пусть α – корень квадратного уравнения $x^2 + 1 = 0,\ (\alpha = j = \sqrt{-1})$. Множество чисел $Q(\alpha) = \{a_0 + a_1\alpha \mid a_0, a_1 \in Q\}$ образует поле комплексных рациональных чисел.

Пример. Пусть $\alpha = \sqrt[3]{2}\exp(j2\pi/2)$. Это число алгебраическое. Оно является корнем уравнения $x^2 - 2 = 0.$

Рассмотрим все числа вида $\omega = a_0 + a_1\sqrt[3]{2}\exp(j2\pi/2) + a_2\left(\sqrt[3]{2}\exp(j2\pi/2)^2\right) = a_0 + a_1\alpha + a_2\alpha^2.$ Множество таких чисел образует поле $Q(\sqrt[3]{2})$.

Циклическая алгебра. Пусть $L = Q(i, \sqrt{d}) = \{u + \sqrt{d}v,\ u, v \in Q(i)\}$.

Циклическая алгебра A определяется как $A = L \oplus eL,$ где $e^2 = \gamma,\ \lambda e = e\sigma(\lambda)$ и $\sigma(u + \sqrt{d}v) = u - \sqrt{d}v.$

Напомним, что $C = R \oplus iR$ и гамильтонова алгебра $H = C \oplus C,\quad j^2 = -1,\ ij = -ji.$ По аналогии с гамильтоновыми кватернионами $q = \alpha + j\beta \in H \leftrightarrow \begin{bmatrix} \alpha & -\tilde{\beta}^* \\ \beta & \tilde{\alpha}^* \end{bmatrix}$, можно ассоциировать элемент *x* с матричным представлением $x = x_0 + ex_1 \in A \leftrightarrow \begin{bmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{bmatrix}$.

C_G-код золотого сечения (Golden code). Для построения C_G-кода используется поле алгебраического числа (числа «золотого сечения») $\theta = \frac{1+\sqrt{5}}{2}$, которое является корнем уравнения $x^2 - x - 1 = 0$ и отношения сопряжения $\sigma(\theta) = \tilde{\theta} = \left(1-\sqrt{5}\right)/2.$

Код C_G определяется через матричное множество следующим образом:

$$C_G = \left\{ \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} = \begin{bmatrix} a+b\theta & c+d\theta \\ i\left(c+d\tilde{\theta}\right) & a+b\tilde{\theta} \end{bmatrix} : \; a,b,c,d \in Z[i] \right\},$$

где $Z[i]$ – кольцо целых комплексных чисел.

Структура кода определяется из циклической алгебры A:

$$\mathrm{A} = \left\{ y = (u+v\theta) + e(w+z\theta) \,|\, e^2 \right\} \Leftrightarrow i,u,v,w,z \in Q(i).$$

Код C_G является линейным кодом. Сумма кодовых слов принадлежит коду, т. е. $\mathbf{X}_1 + \mathbf{X}_2 \in C_G$ для всех $\mathbf{X}_1, \mathbf{X}_2 \in C_G$.

Алгебра A является алгеброй с делением, отсюда следует, что минимальный определитель кода не равен нулю $\delta_{\min}(C_G) = \min\limits_{\mathbf{X}_1 \neq \mathbf{X}_2 \in C_G} \left|\det(\mathbf{X}_1 - \mathbf{X}_2)\right|^2 = \min\limits_{0 \neq \mathbf{X} \in C_G} \left|\det(\mathbf{X})\right|^2 \neq 0.$

Свойство положительности определителя кода C_G. Пусть $\mathbf{X} \in C_G$, тогда

$$\det(\mathbf{X}) = \det \begin{bmatrix} a+b\theta & c+d\theta \\ i\left(c+d\tilde{\theta}\right) & a+b\tilde{\theta} \end{bmatrix} = (a+b\theta)\left(a+b\tilde{\theta}\right) - i(c+d\theta)\left(c+d\tilde{\theta}\right) =$$

$$= a^2 + ab\left(\tilde{\theta}+\theta\right) - b^2 - i\left[c^2 + cd\left(\tilde{\theta}+\theta\right) - d^2\right] = a^2 + ab - b^2 + i\left(c^2 - cd - d^2\right),$$

где $a,b,c,d \in Z[i]$.

Следовательно, $\det(\mathbf{X}) \in Z[i] \Rightarrow \delta_{\min}(C_G) = \left|\det(X)\right|^2 \geq 1$ и не зависит от кардинальности кода. Значения элементов конечного кода C_G согласуются со значениями информационных символов сигнального созвездия. Код реализует полную скорость модуляции.

Моделирование Golden-кода

В основе структуры Голден кода положим циклическую алгебру, $\mathrm{A} = \left(Q(i,\theta)/Q(i), \sigma, i\right)$, где $\theta = \left(1+\sqrt{5}\right)/2$ и отображение $\sigma : x \to \bar{x}$ такое, что $\sigma(\theta) = \bar{\theta} = 1 - \theta.$

Код использует множество $O = \left\{ \begin{bmatrix} x_1 & x_2 \\ j\bar{x}_2 & \bar{x}_1 \end{bmatrix}, x_1, x_2 \in Z[i,\theta] \right\}$ для получения максимального порядка A.

Множество O может быть записано в виде, $O = Z[i,\theta] \oplus Z[i,\theta]l$, где $l = \begin{bmatrix} 0 & 1 \\ j & 0 \end{bmatrix}$.

Каждое кодовое слово имеет форму $\mathbf{X} = \frac{1}{\sqrt{5}} \begin{bmatrix} \alpha x_1 & \alpha x_2 \\ \bar{\alpha} j \bar{x}_2 & \bar{\alpha} \bar{x}_1 \end{bmatrix}$, где $\alpha = 1 + j\bar{\theta}$ – масштабирующий множитель; $x_1 = s_1 + s_2\theta$, $x_2 = s_3 + s_4\theta$. Символы s_1, $s_2 s_3$, s_4 принадлежат сигналу с QAM модуляцией.

Пространственно-временная матрица неортогонального кода для (2×2) системы MIMO может быть представлена в виде $C_2(\theta_1, \theta_2, \theta_3, \theta_4) = \frac{1}{\sqrt{1+r^2}} \begin{bmatrix} \theta_1 + jr\theta_4 & r\theta_2 + \theta_3 \\ \theta_2 - r\theta_4 & jr\theta_1 + \theta_4 \end{bmatrix}$, где $r = \left(-1+\sqrt{5}\right)/2$ – числовой коэффициент, $j = \sqrt{-1}$.

Зависимость вероятности ошибки на бит (*BER*) от отношения сигнал / шум на входе приемника кода Golden – QPSK и различных алгоритмов декодирования показана на рис. 2.

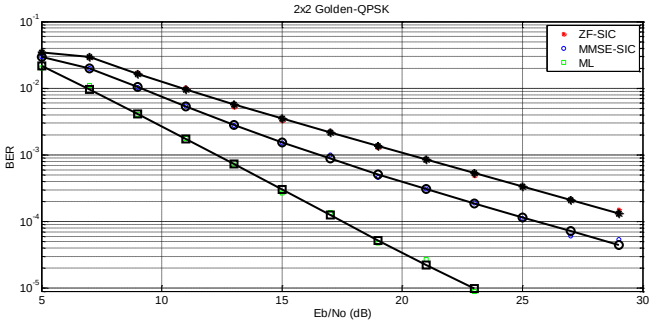


Рис. 2. Зависимость *BER* от отношения сигнал / шум на входе приемника кода Golden – QPSK

Скорость пространственно-временного кода равна $R_C = 2$. Применение кода Golden дает значительный энергетический выигрыш (1…2 дБ в зависимости от параметров системы связи) по сравнению с пространственным мультиплексированием, использующим N передающих антенн и более простую пространственно-временную матрицу $B_N\left(\theta_1,\theta_2,\theta_3,...,\theta_N\right)=\left[\theta_1,\theta_2,...,\theta_N\right]^T$.

Заключение

Алгебраические пространственно-временные коды позволяют разработать алгоритмы для сложных видов модуляции и кодирования, что, в свою очередь, позволяет решить задачу построения высокоскоростных систем связи, работающих в многолучевых каналах.

ALGEBRAIC SPACE-TIME CODES

S.B. SALOMATIN

Abstract

Constructing methods of space-time codes based on the theory of lattices, algebraic numbers and algebraic systems with division are considered. The basic decoding algorithms of space-time codes based on algebraic models of channels and signal processing systems are presented and analyzed.

Keywords: algebraic number, lattice theory, space-time code, signal.

Список литературы

1. *Бакулин М.Г., Варукина Л.А., Крейнделин В.Б.* Технология MIMO: принципы и алгоритмы. М.: Горячая линия – Телеком, 2014.
2. *Крейнделин В.Б., Варукина Л.А.* Методы обработки сигналов в системах с пространственно-временным кодированием. М.: МТУСИ, 2009.
3. *Кудряшов Б.Д.* Основы теории кодирования. СПб.: БХВ-Петербург, 2016.
4. *Саломатин С.Б.* Кодирование информации в сетях подвижной связи. Минск.: БГУИР, 2017.
5. MIMO System Technology for Wireless Communications / Edited by George Tsoulos. USA, FL, Boca Raton: CRC Press, 2006.
6. *Габидулин Э.М., Афанасьев В.Б.* Кодирование в радиоэлектронике. М.: Радио и связь, 1986.
7. *Monteiro F.* Lattices in MIMO Spatial Multiplexing: Detection and Geometry. Department of Engineering University of Cambridge, 2012.
8. Space-Time Processing for MIMO Communications / Ed. by A.B. Gershman, N.D. Sidoropoulos. Wiley&Sons, 2005.
9. *Vucetic B., Yuan J.* Space-Time Coding. Wiley, 2003.
10. *Oesges C., Clerckx B.* MIMO Wireless Communications. Channels. Techniques and Standards for Multi-Antenna, Multi-User and Multi-Cell Systems. U.K.: Academic Press, 2013.

УДК 004.056.55; 621.391.26

НАУЧНО-ТЕХНИЧЕСКИЕ ЗАДАЧИ, СВЯЗАННЫЕ С БИНАРНЫМИ МАТРИЦАМИ

[1]В.А. ЛИПНИЦКИЙ, [2]А.И. СЕРГЕЙ, [3]Н.В. СПИЧЕКОВА

[1]*Военная академия Республики Беларусь*
Минск-57, 220057, Беларусь

[2]*Гродненский государственный университет*
Ожешко, 22, Гродно, 230023, Беларусь

[3]*Белорусский государственный университет информатики и радиоэлектроники*
П. Бровки,6, Минск, 220013, Беларусь

Представлен краткий обзор научно-технических задач, возникающих в различного рода приложениях и связанных с бинарными матрицами, а также различных подходов к классификации множества бинарных матриц.

Ключевые слова: бинарная матрица, динамическое программирование, теория чисел.

Введение

Задачи, появляющиеся в процессе практической деятельности человека, дают мощный импульс для проведения новых теоретических и прикладных исследований. При этом проблемы, возникающие в различных отраслях человеческого знания, могут иметь общую природу и, следовательно, единый подход к решению. Увидеть единую природу проблемы за многообразием формулировок – заслуга и удача исследователя.

В теории и практике распознавания образов и изображений содержится много примеров задач, которые пришли из различных областей человеческой деятельности и имеют близкую формулировку. Здесь нужно упомянуть проблемы радиолокации, когда летающий объект, появившийся на локаторе, нужно распознать как «свой» или «чужой». Здесь и возникающая в медицине проблема классификации бактерий и микроорганизмов, наблюдаемых в бактометре. Здесь и задача классификации кратных ошибок в помехоустойчивых кодах-произведениях, в итерационных кодах с большим кодовым расстоянием.

Перечисленные выше задачи допускают следующее обобщение. На экране размером $n \times n$ пикселей «вспыхивают» n точек. Требуется дать классификацию возникающих при этом образов.

Описанный квадрат однозначно отождествляется с квадратной матрицей порядка n, в которой «вспыхнувшему» пикселю соответствует элемент, равный 1, а «спящему» пикселю – элемент, равный 0.

Проблема классификации бинарных матриц

Бинарные матрицы, т.е. матрицы с элементами 0 и 1, играют важную роль в различных областях математики – в теории графов, групп, дискретной математике, теории информации и помехоустойчивом кодировании [1–3]. В частности, во многих задачах возникает класс P_n бинарных матриц порядка $n, n \geq 2,$ содержащих в точности n единиц. На этот факт в начале XXI века обратил внимание английский математик Питер Кэмерон, приступивший к систематическим исследованиям множества P_n [4–7].

Мощность класса P_n для фиксированного n выражается биномиальным коэффициентом $C_{n^2}^{n} = \frac{n^2!}{n!(n^2-n)!}$. Величина $C_{n^2}^{n}$ очень быстро растет с увеличением n. Поэтому для получения классификации, пригодной для практического использования, целесообразно отождествить некоторые бинарные матрицы, введя в рассмотрение тождественные или эквивалентные преобразования одних матриц в другие.

Завораживающая стройность теории групп, а также ее неоспоримые успехи в применении к решению различных задач привели к тому, что с середины XIX века идея разбиения множества на орбиты – классы эквивалентности под действием на этих множествах тех или иных групп – стала очень популярна. Приложения класса P_n явственно демонстрируют, что наиболее естественными преобразованиями матриц этого класса являются перестановки строк или столбцов между собой. Другими словами, наибольший интерес представляют орбиты класса P_n, которые образуются под действием группы $G = S_n^2 = S_n \times S_n -$ квадрата симметрической группы S_n.

Группа S_n подстановок на n элементах являлась предметом пристального внимания математиков с XVIII века [8]. Несмотря на долгую историю исследований, в математике имеется немало нерешенных вопросов, относящихся к теории группы подстановок. Так, Питер Кэмерон сформулировал свой список из 27 нерешенных проблем в теории подстановок [9]. Третья проблема в упомянутом списке выглядит следующим образом. Найти общую формулу или алгоритм вычисления количества α_n орбит, на которые разбивается множество P_n под действием группы $G = S_n^2$.

Известные к настоящему времени значения α_n для $n \le 102$ приведены в On-Line Encyclopedia of Integer Sequences [10] как последовательность *A049311*.

Величина α_n допускает также и другие интерпретации [5, 10]. Так, с каждой матрицей $A = (a_{ij}) \in P_n$ можно связать неориентированный двудольный граф G. Вершины одной доли этого графа индексированы строками матрицы A, а вершины второй доли – столбцами матрицы A. G имеет в точности n ребер, причем ребро e_{ij} графа G соединяет вершины r_i и c_j, только если $a_{ij} = 1$. Тогда α_n равно количеству непомеченных двудольных графов с n ребрами с точностью до изоморфизма.

Ранговая классификация матриц

Разбиение множества P_n на подклассы можно произвести на основании ранга матрицы, отнеся к одной орбите матрицы одинакового ранга. В [11] показано, что орбиты с крайними значениями ранга имеют общее описание, не зависящее от значений основного параметра n. Так, установлено, что все матрицы ранга n принадлежат одной орбите порождаемой единичной матрицей. Доказано, что среди множества всех орбит имеется D орбит ранга 1, где $D = D(n) -$ количество всех делителей числа n, включая 1 и n. При $n > 2$ существует три орбиты ранга $n-1$. Для $n > 5$ множество P_n содержит 16 орбит рангом $n-2$.

Для каждой матрицы $A \in P_n$ ее ранг $r(A)$ принимает конкретное целое значение в диапазоне от 1 до n. Поэтому по значениям ранга матриц все многообразие S_n^2-орбит разбивается на n классов. Как показали исследования, ранговая классификация является достаточно грубой и неравномерной характеристикой. Однако она позволяет выявить закономерности в количестве орбит большого ранга.

Пусть $F_{n,r}$ – количество классов эквивалентности на множестве P_n, ранг которых равен r. Как уже упоминалось выше, $|F_{n,n}| = 1; |F_{n,n-1}| = 3$ при $n > 2; |F_{n,n-2}| = 15$ при $n > 6$.

Установлено, что величина $F_{n,r}$ зависит только от $n-r$, если $r \geq 2n/3$ [12]. А именно, доказано, что число орбит для фиксированного $d, d < n$, количество орбит ранга $n-d$ постоянно при $n \geq 3d$ и растет с ростом n при $n < 3d$, т.е. $| F_{3d,2d} | = | F_{n',n'-d} |$ для значений $n' > 3d$. Доказательство данного факта опирается на взаимосвязь матриц множества P_n с графами.

Связь с классической теорией чисел

Внутреннее строение орбит определяется расположением единиц по строкам и столбцам ее представителей. Описание этого расположения напрямую взаимосвязано с классической проблемой разбиения чисел, хорошо известной в теории чисел и комбинаторике [13–15].

Как известно, разбиением числа n называется последовательность положительных чисел, сумма которых равна n [13]. Слагаемые данной суммы называются частями разбиения. Разбиения, отличающиеся только порядком частей, считаются равными.

Важную роль в теории разбиений играет функция разбиений $p(n)$. Она определяется как количество всех не равных друг другу разбиений числа n. Значения $p(n)$ растут очень быстро с ростом n. Для вычисления $p(n)$ известна рекуррентная формула, называемая формулой Эйлера:

$$p(n) = p(n-1) + p(n-2) - p(n-5) - p(n-7) + \ldots +$$
$$+(-1)^{q+1}\left(p\left(n - \frac{3q^2-q}{2} \right) + p\left(n - \frac{3q^2+q}{2} \right) \right) + \ldots$$

Всякой матрице $A \in P_n$ соответствуют два вектора: $\bar{s}_A = (s_1, s_2, \ldots, s_n)$ и $\bar{c}_A = (c_1, c_2, \ldots, c_n)$. Это вектора распределений единиц по строкам и столбцам, здесь число s_i равно количеству единиц в i-й строке данной матрицы, число c_j – числу единиц в j-ом столбце матрицы A. Так как $\sum_{i=1}^{n} s_i = \sum_{j=1}^{n} c_j = n$, то каждой матрице $A \in P_n$ соответствует пара $(\bar{s}_A, \bar{c}_A)$ разбиений натурального числа n, если допускать наличие в разбиении нулевых частей.

Свойства векторов $\bar{s}_A$ и $\bar{c}_A$ позволяют сформулировать необходимые условия принадлежности двух матриц одной орбите [16, 17].

Динамическое программирование в подсчете числа α_n орбит

В теории групп известна лемма Бернсайда [18], согласно которой количество m орбит, на которые конечное множество M разбивается под конечной действием группы G, может быть найдено по формуле

$$m = \frac{1}{|G|} \sum_{l=1}^{|G|} | Inv(g_l) |, \qquad (1)$$

где $|G|$ – мощность группы G, $|Inv(g_l)|$ – количество элементов множества M, оставляемых на месте элементом $g_l \in G$, т.е. $|Inv(g_l)|$ – мощность множества $M^{g_l} = \{x \in M \mid g_l(x) = x\}$.

Лемма Бернсайда может быть применена к вычислению числа α_n орбит. В этом случае формула (1) можно переписать [19] в виде:

$$\alpha_n = \frac{1}{(n!)^2} \sum_{l=1}^{(n!)^2} \left| Inv(g_l) \right|. \qquad (2)$$

Здесь $|Inv(g)|$ – это количество матриц из множества P_n, инвариантных относительно действия элемента $g \in G = S_n^2$.

Непосредственное применение формулы (2) предполагает перебор всех элементов группы $G = S_n^2$, которая имеет мощность $(n!)^2$, что вызывает значительные вычислительные трудности. В [19] для вычисления α_n предложен алгоритм развертки, воплощающий идеи метода динамического программирования [20].

Динамическое программирование – это способ решения сложных задач путем разбиения их на вспомогательные, более простые задачи, и последующего объединения решений подзадач в единое общее решение. В алгоритме динамического программирования каждая подзадача решается только один раз, после чего ответ сохраняется. Это позволяет избежать повторных вычислений каждый раз, когда встречается данная, уже решенная, подзадача.

В рамках предлагаемого в [19] алгоритма развертки количество реально вычисляемых слагаемых формулы (2) значительно ниже заявленного числа $(n!)^2$. Сокращение числа перебираемых слагаемых происходит за счет того, что $|Inv(g)|$ оказывается одинаковым для всех подстановок $g = (g_1, g_2) \in S_n^2$, имеющих один и тот же цикленный тип. В случае если известен цикленный тип подстановки g (т.е. последовательность $\mu_1, \mu_2, ..., \mu_q$ мощностей множеств циклов длиной $i, 1 \le i \le q,$ в разложении подстановки g), то $|Inv(g)|$ может быть найдено по реккурентной формуле. Цикленный тип подстановки g определяется по цикленным типам подстановок $g_1, g_2 \in S_n$. Сложность предложенного в [19] алгоритма составляет $O(p^2(n)n^2 \log(n))$, где $p(n)$ – число неупорядоченных разбиений числа n.

Заключение

Представленный краткий обзор научно-технических задач, связанных с рассмотрением бинарных матриц, показывает, что бинарные матрицы являются «универсальным» математическим объектом, который позволяет свести практические задачи, возникающее в различного рода приложениях, к единой «эталонной» задаче. Рассматриваемая задача классификации множества бинарных матриц демонстрирует глубокие связи с различными областями математики: комбинаторикой, теорией групп, динамическим программированием.

SCIENTIFIC AND TECHNICAL TASKS, RELATED TO BINARY MATRIXES

V.A. LIPNITSKI, A.I. SERGEY, N.V. SPICHEKOVA

Abstract

A brief review of scientific and technical problems arising in various applications and related to binary matrixes, as well as various approaches to the classification of the set of binary matrixes are presented.

Keywords: binary matrix, dynamic programming, number theory.

Список литературы

1. *Яблонский С.В.* Введение в дискретную математику. М.: Наука, 1986.
2. *Оре О.* Теория графов. М.: Наука, 1980.
3. Теория информации и кодирование / Б.Б. Самсонов [и др.]. Ростов-на-Дону: «Феникс», 2002.
4. *Cameron P.J.* Sequences realized by oligomorphic permutation groups // Integer Sequences. 2000. Vol. 3 (1). Article 00.1.5.
5. *Cameron P.J., Prellberg T., Stark D.* Asymptotics for incidence matrix classes // The Electronic Journal of Combinatorics. 2006. Vol. 14.1.
6. *Cameron P.J., Gewurz D.A., Merola F.* Product action // Discrete Math. 2008. No. 308. P. 386–394.
7. *Cameron P.J.* Notes on counting: An introduction to enumerative counting [Электронный ресурс]. URL: http://www.maths.qmul.ac.uk/~bill/MTHM030/counting.pdf (дата обращения: 19.04.2018).
8. *Супруненко Д.А.* Группы подстановок. Минск: Навука і тэхніка, 1996.
9. *Cameron P.J.* Problems on permutation groups [Электронный ресурс]. URL: http://www.maths.qmul.ac.uk/~pjc/pgprob.html (дата обращения: 07.02.2018).
10. *N.J. A. Sloane* (ed.). The On-Line Encyclopedia of Integer Sequences [Электронный ресурс]. URL: https://oeis.org/search?q=2%2C+6%2C+16%2C+34%2C+90&sort=&language=english&go=Searc (дата обращения: 07.02.2018).
11. *Конопелько В.К., Липницкий В.А., Спичекова Н.В.* Общие семейства в орбитальной классификации точечных образов // Матер. МНТС «Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных». Минск, 2012. С. 18–25.
12. *Липницкий В.А., Сергей А.И.* О стабилизации количества орбит кэмеровских матриц большого ранга // Весці НАН Беларусі, сер. фіз.-матэм. навук. 2017. № 2. С. 60–70.
13. *Эндрюс Г.* Теория разбиений. М.: Наука, 1982.
14. *Холл М.* Комбинаторика. М.: Мир, 1970.
15. *Hardy G.H., Wright E.M.* An Introduction to the Theory of Numbers. Berlin, Springer, 1973.
16. Действие квадрата симметрической группы на специальном классе (0;1)-матриц. Отсутствие полных орбит / В.К. Конопелько [и др.] // Докл. БГУИР. № 5. 2010. С. 40–46.
17. *Конопелько В.К., Липницкий В.А., Спичекова Н.В.* Классификация точечных образов и классическая проблема разбиения чисел // Докл. БГУИР. 2010. № 8 (54). С. 137–141.
18. *Burnside W.* Theory of groups of finite orders. Cambridge: At The University Press, 1997.
19. *Липницкий В.А., Сергей А.И., Спичекова Н.В.* Алгоритм развертки при подсчете количества S_n^2-орбит кэмеровских матриц // Весн. Магілёўскага дзяржаўнага ўніверсітэта ім. А.А. Куляшова. Серыя В. Прыродазнаўчыя навукі. 2018. С. 23–37.
20. Алгоритмы: построение и анализ / Т.Х. Кормен [и др.]. М.: ООО «И.Д. Вильямс», 2014.

УДК 512 (075.8)

ПОЛИНОМИАЛЬНЫЕ ИНВАРИАНТЫ В НОРМЕННОЙ ОБРАБОТКЕ ПОМЕХОУСТОЙЧИВЫХ КОДОВ

[1]В.А. ЛИПНИЦКИЙ, [2]Е.В. СЕРЕДА

[1]*Военная академия Республики Беларусь*
Минск-57, 220057, Беларусь

[2]*Белорусский государственный университет информатики и радиоэлектроники*
П. Бровки, 6, Минск, 220013, Беларусь

Предлагается использование полиномиальных инвариантов при норменной коррекции многократных ошибок БЧХ-кодами.

Ключевые слова: норменная коррекция, ошибка, полиномиальный инвариант.

Классическое в теории помехоустойчивого кодирования семейство кодов Боуза–Чоудхури–Хоквингема (БЧХ-кодов) является наиболее популярным в приложениях, особенно в высокоскоростных системах передачи информации [1]. Определенная однородность этих кодов, возможность представления компонентов синдромов ошибок элементами конечного поля позволили развить различные алгебраические методы их обработки. К наиболее известным и применимым относится метод коррекции ошибок примитивными БЧХ-кодами путем решения уравнений в полях Галуа. На рубеже XX и XXI веков учеными белорусской школы помехоустойчивого кодирования разработана теория норм синдромов (ТНС) [2, 3]. Нормы синдромов – синдромные инварианты группы Г циклических сдвигов – подгруппы группы AutC автоморфизмов всякого циклического БЧХ-кода С, кодов Хемминга, реверсивных кодов, – являются своеобразными индикаторами Г-орбит. Установлено, что нормы синдромов Г-орбит ошибок декодируемой совокупности попарно различны. Таким образом, ТНС предоставляет новые эффективные норменные методы коррекции ошибок кодами семейства БЧХ. Декодер всякой инфокоммуникационной системы (ИКС), построенный на основе любого БЧХ-кода, в обязательном порядке вычисляет синдром $S(\bar{x})$ каждого принятого блока-сообщения $\bar{x}$. Условие $S(\bar{x}) \neq 0$ означает наличие в сообщении $\bar{x}$ ненулевого вектора-ошибки $\bar{e}$, которую декодер должен откорректировать. Вычислив $N(S(\bar{x})$ по установленным в [2, 3] формулам через компоненты синдрома $S(\bar{x})$, можно идентифицировать Г-орбиту *J*, которой принадлежит искомая ошибка $\bar{e}$ в сообщении $\bar{x}$. Не представляет особой сложности установить точное значение $\bar{e}$ внутри Г-орбиты *J* [2, 3]. Норменные методы оказались не только в *n* раз быстрее стандартных методов коррекции ошибок (*n* – длина кода), но и существенно проще в реализации, а декодеры на их основе хорошо реализуются на БИС нейросетевого типа.

Ниже предлагается дальнейшее развитие ТНС путем введения новых синдромных инвариантов – полиномиальных. Демонстрируется действенность этих инвариантов на конкретном примере.

Автоморфизмы БЧХ-кодов. Для всякого БЧХ-кода С его группа автоморфизмов AutC содержит некоммутативную подгруппу G, порожденную подгруппой Г и циклотомическим автоморфизмом φ [1, 3], порожденным автоморфизмом Фробениуса поля Галуа $GF(2^m)$ – поля определения кода С. Группа Г имеет порядок *n*, а группа *G* – порядок mn. Подавляющее большинство Г-орбит имеет мощность *n*, а *G*-орбиты имеют, как правило, мощность mn.

Каждая *G*-орбита состоит из Г-орбит и имеет следующую структуру: $I_G = \{J, \varphi(J), \varphi^2(J), \ldots, \varphi^{\mu-1}(J)\}$ для конкретной Г-орбиты *J*. Здесь μ – наименьший делитель m с условием: $\varphi^{\mu}(J) = J$. В большинстве случаев $\mu = m$.

Всякая Г-орбита *J* имеет похожую структуру: для автоморфизма σ циклического сдвига координат векторов: $\sigma(e_1, e_2, \ldots, e_n) = (e_n, e_1, e_2, \ldots, e_{n-1})$, и для любой своей вектор-ошибки $\bar{e}$: $J = \{\bar{e}, \sigma(\bar{e}), ..., \sigma^{\nu-1}(\bar{e})\}$, где ν – наименьшее натуральное число с условием: $\sigma^{\nu}(\bar{e}) = \bar{e}$. Известно, что мощность Г-орбиты делит *n* и, как правило, совпадает с *n*. В силу сказанного часто используются обозначения: $J = \langle \bar{e} \rangle$ или $J = \langle \bar{e}_\Gamma \rangle$.

Нормы синдромов и норменные декодеры для БЧХ-кодов. Классический примитивный БЧХ-код длиной n, исправляющий двойные ошибки, задается проверочной матрицей $H = \{\alpha^i, \alpha^{3i}\}^T$, $0 \le i \le 2^m - 2 = n - 1$, α – примитивный элемент поля $GF(2^m)$. Синдром ошибок в сообщении $\bar{x}$ вычисляется по формуле: $S(\bar{x}) = H \cdot \bar{x}^T$. В согласии со структурой проверочной матрицы $S(\bar{x}) = (s_1, s_2)^T$, где s_1, s_2 – компоненты синдрома, элементы поля $GF(2^m)$. Согласно предложению 3.1 [2], $S(\sigma(\bar{e})) = (\alpha \cdot s_1, \alpha^3 \cdot s_2)^T$. В силу этой формулы норма $N(S(\bar{x}))$ синдрома $(S(\bar{x}))$ вычисляется по формуле (см. [2], глава 4): $N(S(\bar{x})) = \frac{s_2}{s_1^3}$.

При таком определении норма синдрома одинакова для всех ошибок Г-орбиты $J = \langle \bar{e}_\Gamma \rangle$, т.е. является инвариантом этой орбиты, а потому и называется нормой этой Г-орбиты. Согласно теореме 4.1 [2], нормы множества *T* Г-орбит одиночных и двойных ошибок попарно различны. Составив список ET образующих $\bar{e}_i$ Г-орбит множества *T*, список *ST* синдромов образующих $S(\bar{e}_i)$ и список *NST* норм синдромов образующих можно реализовать работу норменного декодера по отмеченному во введении алгоритму.

Современные условия предъявляют высокие требования к инфокоммуникационным системам, прежде всего, к росту объемов информации, передаваемой в единицу времени. Это приводит к увеличению длин применяемых кодов, что, в свою очередь, отражается в увеличении названных выше списков и замедляет работу норменных декодеров. Один из выходов из сложившейся ситуации состоит в применении *G*-орбит и их полиномиальных инвариантов.

G-орбиты и их полиномиальные инварианты. В силу [3], $S(\varphi(\bar{e})) = (s_1^2, s_2^2)^T$. Отсюда следует, что $N(S(\varphi(\bar{e}))) = (N(S(\bar{e})))^2$. Действие φ на координаты векторов-ошибок подробно изложено в [3, с. 40–41]. Таким образом, почти автоматически строится селекция орбит множества *T* в *G*-орбиты, а также списков *ST* и *NST*. Список *EG* образующих *G*-орбит строится из списка *ET* и практически в *m* раз меньше списка *ET*.

Возьмем образующую $\bar{e}_i \in EG$. Ее норма $N_i = N(S(\bar{e}_i)) = \alpha^j$ – конкретный ненулевой элемент поля Галуа $GF(2^m)$. Как правило, *G*-орбита $<\bar{e}_i>_G$ состоит из *m* Г-орбит. Нормы этих Г-орбит получаются последовательным возведением в квадрат $N_i = \alpha^j$. Но возведение в квадрат элементов поля Галуа $GF(2^m)$ равносильно действию на автоморфизм Фробениуса, образующей φ циклической группы Галуа этого поля. Таким образом, список норм Г-орбит *G*-орбиты $<\bar{e}_i>_G$ имеет вид: $N(<\bar{e}_i>_G) = \{N_i, \varphi(N_i), ..., \varphi^{m-1}(N_i)\} = \{\alpha^j, \alpha^{2j}, ..., \alpha^{2^{m-1}j}\}$. Аналогично строятся и синдромы образующих этих Г-орбит. Построенный список норм Г-орбит, составляющих *G*-орбиту $<\bar{e}_i>_G$ есть множество всех элементов поля, сопряженных друг другу под действием группы Галуа. Такие элементы составляют полный список корней

неприводимого полинома над минимальным подполем $Z/2Z = GF(2)$. Этот полином называют минимальным полиномом любого из элементов названного списка и, как правило, обозначают $p(\alpha^j, x)$ [4, 5]. Полином $p(\alpha^j, x) = (x-\alpha^j)(x-\alpha^{2j})\cdot\ldots\cdot(x-\alpha^{2^{m-1}i}) = p(<\overline{e}_i>_G, x)$, очевидно, является однозначной характеристикой *G*-орбиты $<\overline{e}_i>_G$. *G*-орбита $<\overline{e}_i>_G$ содержит $\mu < m$ Г-орбит тогда и только тогда, когда α^j принадлежит подполю $GF(2^\mu)$ поля $GF(2^m)$.

Метод декодирования ошибок на основе *G*-орбит предполагает составление списка *PEG* неприводимых полиномов норм синдромов образующих *G*-орбит и двухступенчатую систему идентификации ошибки: найдя ненулевой синдром ошибки, можно вычислить ее норму, затем найти неприводимый полином этой нормы, данный полином сравнить со списком *PEG*. Отождествив вычисленный полином с каким-то полиномом списка *PEG*, далее можно сравнить вычисленную норму только со списком норм Г-орбит соответствующей *G*-орбиты и провести дальнейшие действия по коррекции, описанные выше.

Пример. Рассмотрим БЧХ-код C_5 длиной 127 над полем $GF(2^7)$ с проверочной матрицей $H = \{\alpha^i, \alpha^{3i}\}^T$, $0 \le i \le 30$, α – корень примитивного полинома $p(x) = x^7 + x + 1$. Здесь двойные ошибки делятся на 63 Г-орбиты, а те на 9 *G*-орбит по 7 Г-орбит в каждой. В табл. 1 представлен список образующих $\overline{e}_i = \overline{e}_{1,\mathrm{j}}$ *G*-орбит двойных ошибок (с равными единице первой и j-й координатами), синдромов, норм синдромов и неприводимых полиномов этих G-орбит.

Пусть ИКС с данным кодом приняла блок-сообщение $\overline{x}$ с синдромом $S(\overline{x}) = (s_1, s_2)^{\mathrm{T}} = (\alpha^{122}, \alpha^{48})^{\mathrm{T}}$. Тогда норма синдрома $N = N(S(\overline{x})) = \alpha^{63}$, а полином $p(N, x) = x^7 + x^6 + 1$, который совпадает с третьим полиномом из табл. 1.

Таблица 1. **Список образующих *G*-орбит двойных ошибок в БЧХ-коде C_5^{127}, синдромов образующих, норм синдромов и полиномиальных инвариантов этих орбит**

№ п/п	Образующая *G*-орбиты	Синдром $s_1(\overline{e}_{i,j})$	Синдром $s_2(\overline{e}_{i,j})$	Норма $N(S(\overline{e}_{i,j}))$	Неприводимый полином $p(x)$
1	$\overline{e}_{1,2}$	α^7	α^{63}	α^{42}	$x^7 + x^6 + x^3 + x + 1$
2	$\overline{e}_{1,4}$	α^{63}	α^{90}	α^{28}	$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$
3	$\overline{e}_{1,6}$	α^{54}	α^{31}	α^{123}	$x^7 + x^6 + 1$
4	$\overline{e}_{1,8}$	α	α^{57}	α^{54}	$x^7 + x^6 + x^5 + x^4 + x^2 + x + 1$
5	$\overline{e}_{1,10}$	α^{90}	α^{31}	α^{50}	$x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$
6	$\overline{e}_{1,12}$	α^{87}	α^{77}	α^{70}	$x^7 + x^6 + x^5 + x^2 + 1$
7	$\overline{e}_{1,14}$	α^{55}	α^{100}	α^{62}	$x^7 + x^6 + x^4 + x^2 + 1$
8	$\overline{e}_{1,20}$	α^{29}	α^{20}	α^{61}	$x^7 + x^6 + x^5 + x^4 + 1$
9	$\overline{e}_{1,22}$	α^{57}	α^{3}	α^{86}	$x^7 + x^6 + x^4 + x + 1$

Вычисленная норма N совпала с нормой образующей пятой Г-орбиты из табл. 2, в которой приведен список образующих $\overline{e}_{1,j}$ всех семи Г-орбит, составляющих названную *G*-орбиту, синдромов образующих и норм синдромов.

Результат сравнения синдрома $S(\overline{x})$ с синдромом $S(\overline{e}_{1,81})$: $\dfrac{s_1(\overline{x})}{s_1(\overline{e}_{1,81})} = \dfrac{\alpha^{122}}{\alpha^{102}} = \alpha^{20}$. Таким образом, искомый вектор в принятом сообщении $\overline{x}$ получается путем циклического сдвига вправо на 20 позиций координат образующей $\overline{e}_{1,81}$. Следовательно, $\overline{e} = \overline{e}_{21,101}$ – двойная ошибка с единичными координатами на позициях 21 и 101. Тогда истинное сообщение $\overline{c} = \overline{x} + \overline{e}_{21,101}$.

Таблица 2. **Образующая Г-орбит третьей *G*-орбиты из табл. 1, синдромы образующих и их нормы**

№ п/п	Образующая Г-орбиты	Синдром $s_1(\overline{e}_{i,j})$	Синдром $s_1(\overline{e}_{i,j})$	Норма $N(S(\overline{e}_{i,j}))$
1	$\overline{e}_{1,6}$	α^{54}	α^{31}	α^{123}
2	$\overline{e}_{1,11}$	α^{108}	α^{62}	α^{119}
3	$\overline{e}_{1,21}$	α^{89}	α^{124}	α^{111}
4	$\overline{e}_{1,41}$	α^{51}	α^{121}	α^{95}
5	$\overline{e}_{1,81}$	α^{102}	α^{115}	α^{63}
6	$\overline{e}_{1,34}$	α^{77}	α^{103}	α^{126}
7	$\overline{e}_{1,67}$	α^{27}	α^{79}	α^{125}

POLYNOMIAL INVARIANTS IN NORMAL PROCESSING OF INTERMEDIATE CODES

V.A. LIPNITSKI, E.V. SEREDA

Abstract

The use of polynomial invariants under the normal correction of multiple errors by BCH-codes is proposed.

Keywords: norm correction, error, polynomial invariant.

Список литературы

1. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
2. *Конопелько В.К., Липницкий В.А.* Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. М.: УРСС, 2004.
3. *Липницкий В.А., Конопелько В.К.* Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск: БГУ, 2007.
4. *Лидл Р., Нидеррайтер Г.* Конечные поля. М.: Мир, 1988.
5. *Липницкий В.А.* Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа. 2-е изд. Минск: БГУИР, 2006.

УДК 621.391

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ГЕНЕРИРОВАНИЯ СИГНАЛОВ РАЗЛИЧНЫХ ФОРМ И ВИДОВ МОДУЛЯЦИИ

[1]Н.И. БЕЛЕНКЕВИЧ, [1]В.А. ИЛЬИНКОВ, [1]В.Ю. ЦВЕТКОВ, [2]А.С. ВОЙТЕНКОВ, [1]Я.М. ЯРКОВ

[1]*Белорусский государственный университет информатики и радиоэлектроники*
П. Бровки, 6, Минск, 220013, Беларусь

[2]*ОАО «Конструкторское бюро «Дисплей»*
П. Бровки, 13а, Витебск, 210605, Беларусь

Определены структура, проблемы создания, требования и возможные области применения программно-аппаратного комплекса математического и физического моделирования сигналов различных форм и видов модуляции.

Ключевые слова: моделирование, программно-аппаратный комплекс, сигнал.

Введение

В настоящее время весьма актуальна проблема формирования и анализа параметров сигналов произвольной формы, что обусловлено следующим рядом факторов [1–5].

Во-первых, разработка и эксплуатация современных информационных систем требует большого количества источников электрических сигналов разных типов, форм, видов модуляции, диапазонов частот, времен и уровней. Проблема усугубляется моральным и физическим старением существующего парка генераторов, крайне недостаточным уровнем их производства в Республике Беларусь и странах СНГ.

Во-вторых, дальнейшее развитие информационных систем актуализирует проблему измерения и контроля параметров. В настоящее время ее, в основном, решают с помощью достаточно сложных специализированных измерителей, номенклатура которых стремительно расширяется. Такой подход требует создания (приобретения) большого количества измерителей и влечет весьма значительные материальные и интеллектуальные затраты. Поэтому в мире начали уделять большое внимание разработке измерительных систем и приборов с расширенными функциональными возможностями (в пределе универсальных), которые генерируют произвольные измерительные сигналы, измеряют параметры качества различных устройств и систем и пригодны для целей функциональной диагностики.

В-третьих, в современных условиях подготовка специалистов значительно усложняется моральным и физическим старением материально-технической базы, обновление которой по финансовым причинам весьма затруднительно. Ослабить это негативное влияние пытаются применением математического моделирования, что, однако, ухудшает практические навыки и резко увеличивает время адаптации молодых специалистов к задачам производства. Для совмещения хорошей теоретической и практической подготовки будущих специалистов на всем протяжении учебного процесса, помимо математического моделирования, необходимо широко использовать физическое моделирование. Это означает, что студенты радиоэлектронных, радиотехнических, телекоммуникационных и компьютерных специальностей должны постоянно изучать электрические сигналы разных типов, форм, видов модуляции и диапазонов частот, свободно владеть методами и средствами измерения их параметров в частотной и временной областях на входе и выходе реальных функциональных звеньев. Устаревшая материально-техническая база делает физическое моделирование практически невозможным.

С учетом изложенного перспективным направлением, интенсивно развиваемым в мире, является разработка и производство программно-аппаратных комплексов (ПАК) математического и физического моделирования сигналов и систем. Подобный ПАК должен обеспечивать генерирование аналоговых, импульсных, аналого-импульсных, цифровых и модулированных (различных видов цифровой и аналоговой модуляции) сигналов в широком диапазоне частот и времен; математическое моделирование радиоэлектронных систем (РЭС) в частотной, временной областях и на комплексной плоскости; электрическую имитацию в реальном масштабе времени функциональных звеньев РЭС [1–3].

Цель работы – определение структуры, проблем создания, требований и возможных областей применения ПАК, удовлетворяющего перечисленным требованиям.

Принципы и проблемы построения ПАК

Предлагается структура ПАК, содержащая многофункциональную систему генерирования (МСГ) сигналов и реакций произвольной формы, многофункциональную программу моделирования (МПМ) сигналов и систем, библиотеку виртуальных систем, систему подготовки формального описания, систему измерения и контроля, ПЭВМ [1, 3].

Наиболее сложной технологической задачей при создании ПАК является разработка МСГ сигналов и реакций. Сравнительный анализ патентно-информационных источников показывает, что в области генерирования сигналов произвольной формы в широком диапазоне частот существуют следующие основные проблемы [4–7]:

– недостаточная стабильность несущей частоты модулированных сигналов, особенно в случае сигналов с различными видами угловой модуляции;

– невысокая линейность и малая относительная ширина статической модуляционной характеристики;

– недостаточно мелкий для многих применений шаг сетки частот генерируемых сигналов и опорных колебаний;

– значительное время перестройки с одной несущей частоты на другую.

Предлагается комплексное решение данных проблем генерирования сигналов произвольной формы в широком диапазоне частот. Оно основывается на совместном применении так называемой обусловленной модуляции и детерминированной взаимосвязи служебных колебаний (рис. 1). Обусловленная набором требований, модуляция реализуется с помощью обусловленного (многофункционального) модулятора.

Рис. 1. Схема комплексного решения проблем генерирования сигналов произвольной формы в широком диапазоне частот

Основные требования к многофункциональному модулятору

Многофункциональный модулятор (ММ), являющийся наиболее сложной составной частью МСГ, должен удовлетворять следующим основным требованиям:

– виды модуляции: цифровая и аналоговая амплитудная, цифровая и аналоговая частотная, цифровая и аналоговая фазовая, комбинированные;

– форма модулирующих сигналов – произвольная;

– высокая верхняя граничная частота модулирующих сигналов;

– большая относительная ширина и высокая линейность статической модуляционной характеристики;

– высокая стабильность несущей частоты модулированных сигналов;

– возможность изменения в широких пределах несущей частоты и ее сверхбыстрой перестройки.

Возможные области применения ММ, МСГ и ПАК

В соответствии с предлагаемой концепцией основой МСГ сигналов и реакций произвольной формы и всего ПАК математического и физического моделирования сигналов и систем является ММ. Модулятор, удовлетворяющий сформулированным уникальным требованиям, в виде самостоятельного технологического продукта и в виде МСГ и ПАК имеет следующие области возможного применения.

1. *Системы и устройства генерирования измерительных сигналов различных форм, видов модуляции и диапазонов частот.* Современный генератор сигналов цифровой модуляции укрупненно представляет совокупность блоков модуляции, усиления и регулирования, управления, интерфейса и микропроцессора. При этом научно-технический уровень генератора, в основном, определяется уровнем решений, заложенных в модуляторе. Учитывая изложенное, разработка ММ с обозначенными требованиями позволяет создать семейство весьма конкурентных генераторов измерительных сигналов, отличающихся видом модуляции, диапазоном рабочих частот и ценовой шкалой.

2. *Информационно-измерительные системы и комплексы.* Как отмечено выше, теория и практика информационно-измерительных систем и комплексов развивается в направлении создания многофункциональных (в пределе универсальных) автоматизированных систем контроля и измерения параметров радиоэлектронных устройств и систем. Решением этой проблемы активно занимаются все ведущие мировые производители измерительной техники. Подобная измерительная система структурно включает в себя следующие подсистемы: математического моделирования, генерирования измерительных сигналов и реакций произвольной формы в широком диапазоне частот, времен и уровней, измерения квазистатических параметров, измерения частотно-динамических параметров, измерения время-динамических параметров. При этом функции, выполняемые подсистемами генерирования и математического моделирования, качественно и количественно соответствуют функциям ПАК. Таким образом, разработка ПАК эквивалентна разработке двух важнейших подсистем многофункциональной измерительной системы, реализующей концепцию универсального рабочего места исследователя.

3. *Системы связи, системы передачи информации.* Качество систем связи и систем передачи информации во многом зависит от свойств модулятора, который определяет вид и формат модуляции, диапазон рабочих частот, стабильность частоты и другие важнейшие параметры. Поэтому разработка ММ с обозначенными требованиями создает надежную технологическую основу для разработки новых и модернизации существующих систем за счет использования новых видов модуляции, коренного повышения динамических и точностных характеристик. Роль таких систем в современном мире стремительно растет, в том числе за счет интенсивного развития мобильных роботехнических комплексов гражданского и военного назначения.

4. *Системы и устройства специального назначения.* Анализ требований, предъявляемых к ММ, показывает, что они практически идеально подходят для решения задач реализации современных систем и устройств специального назначения: систем связи с постоянно перестраиваемой рабочей частотой, радиолокационных систем, систем постановки широкополосных и узкополосных помех (систем подавления радиосредств), устройств активной защиты компьютеров. Очевидно, добавление к рассматриваемому ММ усилителя мощности и антенны соответствует переходу к системе подавления радиосредств с варьируемыми характеристиками, а совместное применение ММ и антенны реализует высококачественное устройство активной защиты компьютеров.

5. *Программно-аппаратные обучающие комплексы математического и физического моделирования сигналов и систем.* Весьма перспективно применение рассматриваемого ПАК в качестве обучающего программно-аппаратного комплекса (ОПАК) в учебном процессе подготовки (переподготовки) специалистов и создание на основе ОПАК унифицированных учебных лабораторий моделирования сигналов и систем. Дело в том, что сокращение сроков получения высшего образования предполагает грамотную интенсификацию учебного процесса, основанную на эффективном совмещении теоретической и практической подготовки. Реализация занятий на базе ОПАК переводит обучение на новый технологический уровень,

повышает мотивацию студентов, их теоретическую и практическую подготовку. На базе ОПАК сравнительно просто реализовать виртуальные физические модели сложных и разнообразных по свойствам систем и устройств. Это делает возможным и весьма целесообразным применение ОПАК в учебном процессе студентов второй ступени (магистрантов) для усиления их теоретической и практической подготовки, а также для создания фронтальных циклов лабораторных работ по совокупности дисциплин радиоэлектронных, радиотехнических, радиофизических, телекоммуникационных и компьютерных специальностей (для студентов первой ступени); для постановки сложных физических экспериментов в научных исследованиях. Для оценки возможного объема рынка отметим, что в Российской Федерации имеется несколько сотен университетов (факультетов), где существует настоятельная потребность в ОПАК. При этом каждый такой факультет содержит не менее трех кафедр, на каждой из которых необходимо иметь, как минимум, две унифицированные учебные лаборатории, содержащие не менее 10–15 ОПАК.

Заключение

Проведенный анализ проблем и возможных путей их решения показывает, что разработка многофункционального модулятора, многофункциональной системы генерирования и программно-аппаратного комплекса математического и физического моделирования сигналов и систем с обозначенными требованиями является актуальной научно-технической задачей, решение которой позволит создать и наладить производство конкурентных комплексов, систем и устройств различного функционального назначения, выйти на новые емкие рынки товаров и услуг, адекватно реагировать на тенденции и запросы этих рынков.

HARDWARE AND SOFTWARE COMPLEX FOR GENERATION OF SIGNALS IN VARIOUS SHAPES AND MODULATION TYPES

N.I. BELENKEVICH, A.V. ILYNKOV, V.Yu. TSVIATKOU,
A.S. VOYTENKOV, Ya.M. YARKOV

Abstract

The structure, problems of creation, requirements and possible applications of the hardware and software complex for mathematical and physical modeling of signals in various forms and types of modulation are determined.

Keywords: modeling, software and hardware complex, signal.

Список литературы

1. Комплекс моделирования сигналов и систем / В.А. Ильинков [и др.] // Компоненты и технологии. 2017. № 5. С. 133–136.
2. *Ильинков В.А., Беленкевич Н.И.* Обучающие программно-аппаратные комплексы как эффективное средство интенсификации учебного процесса // Матер. VI междунар. науч.-метод. конф. «Высшее техническое образование: проблемы и пути развития». Минск, 28–29 ноября 2012 г. С. 213.
3. *Ильинков В.А., Беленкевич Н.И.* Комплексы моделирования сигналов и систем в учебном процессе подготовки специалистов // Матер. VIII междунар. науч.-метод. конф. «Высшее техническое образование: проблемы и пути развития». Минск, 17–18 ноября 2016 г. Ч. 1. С. 190–194.
4. *Прокис Дж.* Цифровая связь. М.: Радио и связь, 2000.
5. *Головин О.В.* Устройства генерирования, формирования, приема и обработки сигналов. М.: Горячая линия-Телеком, 2012.
6. *Ильинков В.А., Ярков Я.М., Ильинкова А.В.* Новый метод генерирования сигналов фазовой модуляции // Докл. БГУИР. 2016. № 8 (102). С. 17–21.
7. *Ильинков В.А., Ярков Я.М., Ильинкова А.В.* Метод и устройство генерирования сигналов частотной модуляции // Электросвязь. 2016. № 8. С. 37–42.

УДК 621.391

АНАЛИЗ ПОСТРОЕНИЯ ЦИФРОВЫХ ПРИЕМОПЕРЕДАЮЩИХ ТРАКТОВ УКВ-ДИАПАЗОНА

А.Л. ХОМИНИЧ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Рассматриваются методы построения приемопередающих трактов систем цифровой радиосвязи, широкополосного беспроводного доступа, телевизионного и звукового радиовещания, ориентированных на работу в диапазоне ультракоротких волн, т.е. в частотном диапазоне от 30 до 3000 МГц (МВ- и ДМВ-диапазоны). Отмечена тенденция последовательного замещения аналоговых узлов радиотракта цифровыми, вплоть до выполнения аналого-цифрового и цифро-аналогового преобразований непосредственно на несущей частоте. Рассмотрены проблемы реализации полностью цифровых приемопередающих трактов.

Ключевые слова: радиоприемный тракт, модуляция, преобразование частоты, дискретизация на радиочастоте.

Введение

Частотный диапазон 30–3000 МГц в настоящее время является самым «загруженным» с точки зрения количества и разнообразия функционирующих в нем радиосредств. В нем работают многочисленные системы служебной радиосвязи, системы подвижной радиосвязи 2-го–4-го поколений, значительная часть систем широкополосного беспроводного доступа, ведется наземное и кабельное цифровое телевизионное и звуковое вещание. Кроме этого, эксплуатируются системы радиоопределения, радионавигации и пр. В результате формируется чрезвычайно сложная электромагнитная обстановка, соответственно повышаются требования к помехоустойчивости радиосредств, а также к параметрам их электромагнитной совместимости (ЭМС). Для приемопередающих трактов портативных и мобильных устройств актуальна также задача минимизации массогабаритных показателей и снижения потребляемой мощности.

Использование цифровых методов формирования и обработки сигналов и совершенствование элементной базы позволяют повысить качество обработки радиосигналов, реализовывать методы и алгоритмы, недоступные либо труднореализуемые при аналоговой обработке. Анализ методов построения приемопередающих радиочастотных трактов показывает, что наметилась тенденция перехода на полностью цифровые тракты, с аналого-цифровым (для приемника) и цифро-аналоговым (для передатчика) преобразованием непосредственно на несущей частоте.

Далее рассматриваются варианты построения радиочастотных трактов и способы улучшения их параметров за счет последовательного замещения аналоговых узлов цифровыми.

Современное состояние построения радиоприемных трактов

На протяжении многих десятилетий радиоприемные тракты в подавляющем большинстве строились по супергетеродинной схеме. Ее преимущества применительно к аналоговым системам общеизвестны и хорошо представлены в [1, 2]. В зависимости от диапазона рабочих частот, занимаемой радиосигналом полосы частот и требований к избирательности

по побочным каналам приема, варьировались количество ступеней преобразования и значения промежуточных частот (ПЧ).

Долгое время возможности цифровой обработки сигналов были ограничены, аналого-цифровое преобразование выполнялось уже после демодулятора либо на ПЧ, значение которой должно было быть достаточно низким [3]. Однако интенсивное развитие микро- и наноэлектроники привело к тому, что параметры аналого-цифровых преобразователей (АЦП) ведущих производителей (Analog Devices, Texas Instruments, Maxim Integrated и др.) позволяют устанавливать их практически в любой точке радиотракта. Соответственно, аналоговым остается только ВЧ-тракт, а все операции по обработке радиосигнала, включая его демодуляцию (DMD) и декодирование (DC), выполняются в цифровом модуле, реализуемом, как правило, на цифровом сигнальном процессоре (DSP), программируемой логической интегральной схеме (FPGA) либо специализированной интегральной схеме (ASIC).

Анализ супергетеродинной схемы (рис. 1) показывает, что основной проблемой остается подавление зеркального канала.

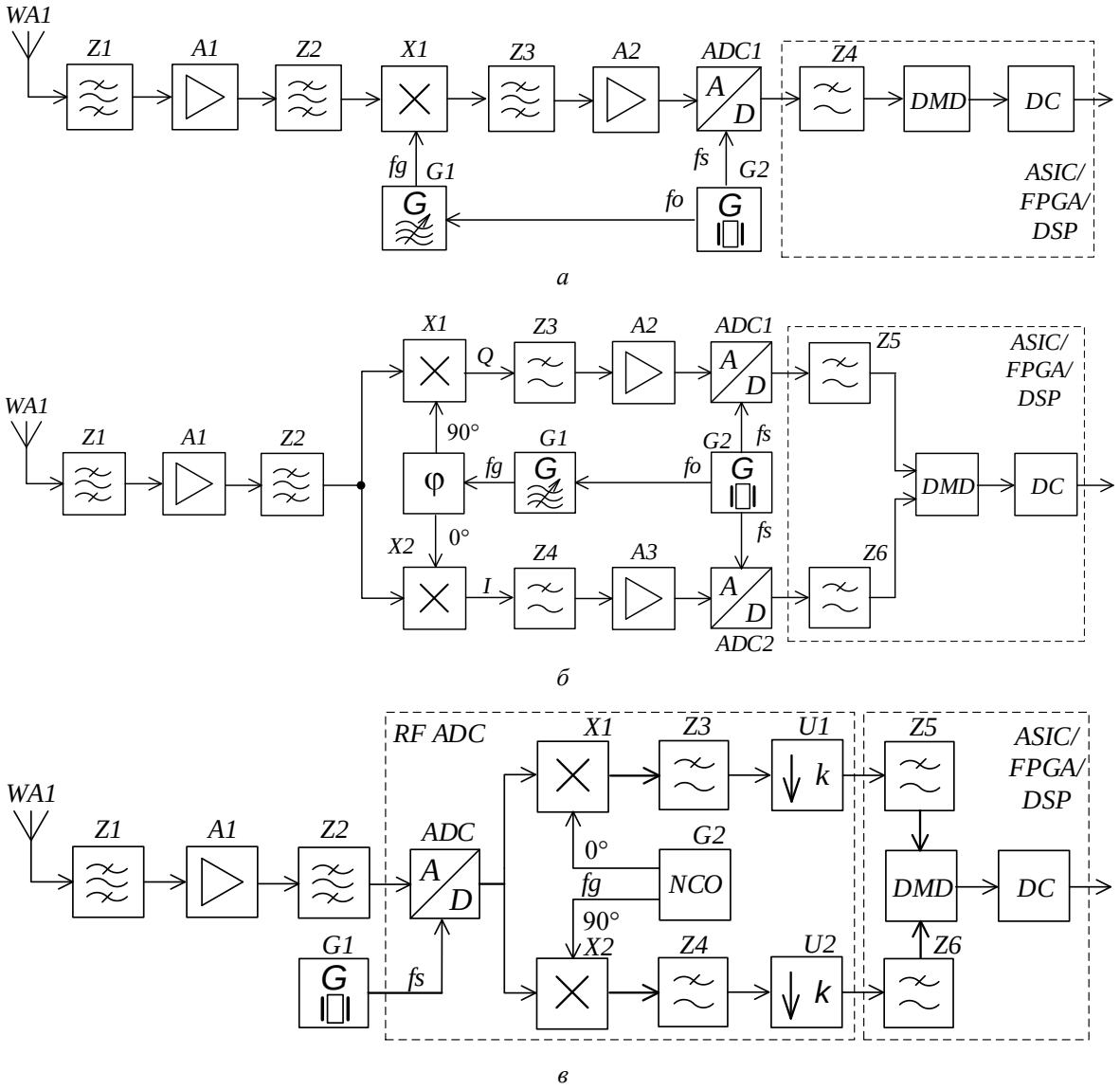


Рис. 1. Радиоприемные тракты: *а* – супергетеродинный; *б* – с квадратурным преобразованием частоты; *в* – с аналого-цифровым преобразованием на несущей частоте

С точки зрения избирательности по зеркальному каналу, желательно увеличение значения ПЧ, что снижает требования к крутизне склонов АЧХ фильтров *Z*1 и *Z*2 (рис. 2, *а*), но в то же время это повышает требования к фильтру *Z*3 (рис. 2, *б*, *в*), обеспечивающему

избирательность по соседним каналам. В современных системах радиосвязи, теле- и радиовещания ширина диапазона используемых частот $\Delta F_{ДРЧ}$ может быть значительной, например, от 470 до 862 МГц в наземном цифровом телевизионном вещании. Зеркальный канал в таком случае попадает в диапазон частот принимаемых радиосигналов (рис. 2, *а*), поэтому фильтры *Z*1 и/или *Z*2 должны быть перестраиваемыми, что существенно затрудняет их реализацию в интегральном исполнении. Использование 2-х и более кратного преобразования частоты с выбором $f_{ПЧ1} > f_В$ позволяет использовать неперестраиваемые фильтры, но усложняет схему и повышает требования к стабильности частот гетеродинов.

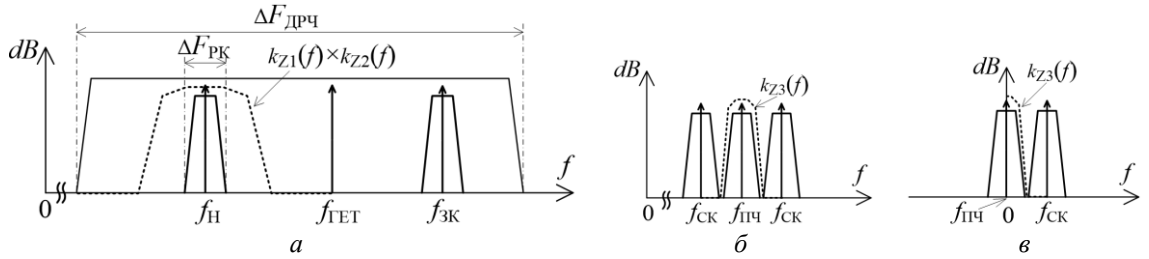


Рис. 2. Обеспечение избирательности: *а* – по зеркальному каналу; *б*, *в* – по соседним каналам

Проблемы с реализацией супергетеродинных трактов привели к переходу на тракты с квадратурным преобразованием частоты со значением $f_{ПЧ1} = 0$ (см. рис. 1, *б*). В этом случае зеркальный канал в его традиционном понимании отсутствует, но верхняя боковая полоса спектра частот радиосигнала становится зеркальной нижней, и наоборот [4]. Если нижняя и верхняя боковые полосы симметричны, например, в случае амплитудной модуляции с двумя боковыми полосами, квадратурное преобразование необязательно и схема вырождается в классический гетеродинный тракт. В остальных случаях (прием радиосигналов с квадратурной модуляцией, радиосигналов с множественными несущими) квадратурная схема обязательна.

В радиотрактах с нулевой ПЧ ВЧ-тракт строится широкополосным, фильтры *Z*1 и *Z*2 фиксированы, что существенно упрощает их реализацию. Также достоинством является использование для подавления соседних каналов фильтров нижних частот (ФНЧ), вместо полосовых, и возможность выбора частоты дискретизации f_S, значительно превышающей значение ширины полосы частот радиосигнала $\Delta F_{РС}$. Последнее позволяет упростить требования к аналоговым ФНЧ *Z*3 и *Z*4, основной задачей которых становится подавление спектральных составляющих с частотой, превышающей половину частоты дискретизации, а обеспечение избирательности по соседним каналам перекладывается на цифровые фильтры *Z*3 и *Z*4, возможности реализации которых существенно шире. Построение радиотрактов по схеме с нулевой ПЧ позволяет снизить их размеры и энергопотребление [5, 6], а значит и стоимость, поэтому в настоящее время именно они получили наибольшее распространение.

В тоже время в них усилитель радиочастоты *A*1 (см. рис. 1, *б*) является широкополосным, что увеличивает требования к его линейности, особенно при наличии мощных помех. Также проблемами являются просачивание сигнала гетеродина на сигнальные входы преобразователей частоты *X*1 и *X*2, приводящее к появлению на их выходах постоянной составляющей, и высокие требования к идентичности параметров квадратурных каналов – к примеру, для подавления зеркального канала на 50 дБ разность коэффициентов передачи *I*- и *Q*-каналов не должна превышать 0,05 дБ, а разность фаз – 0,1° [7]. Если оценивать качество обработки сигналов по критерию относительной ошибки модуляции (EVM – Error vector magnitude), то типовое его значение для радиотрактов с нулевой ПЧ, выполненных на современной элементной базе, составляет порядка 40 дБ [8].

Тракт с АЦП на несущей частоте (см. рис. 1, *в*) обеспечивает кардинальное решение проблем, связанных с неидентичностью каналов и просачиванием сигнала гетеродина [9, 10], поскольку цифровое преобразование частоты (и все последующие операции) выполняются с математической точностью, ограниченной только разрядностью вычислений. Также все блоки, расположенные после АЦП, не влияют на коэффициент шума приемника.

Основной проблемой тракта с АЦП на несущей частоте является обеспечение необходимого динамического диапазона при построении широкополосных трактов, в которых

ширина диапазона рабочих частот $\Delta F_{\text{ДРЧ}}$ значительно больше полосы частот одного радиоканала $\Delta F_{\text{РК}}$, как показано на рис. 2, *а*. В этом случае размах сигнала на входе АЦП определяется мощностями всех сигналов, как полезного, так и мешающих, попадающих в полосу пропускания фильтров *Z*1 и *Z*2 ВЧ-тракта. При этом мощности мешающих сигналов могут быть значительно выше мощности полезного сигнала. В результате, в зависимости от режима работы схемы автоматической регулировки усиления (АРУ) ВЧ-тракта, могут сложиться две ситуации:

– если схема АРУ управляется на основании информации о размахе суммарного сигнала на входе АЦП, то при наличии мощных мешающих сигналов либо при большом количестве мешающих сигналов коэффициент усиления ВЧ-тракта снижается, в результате чего повышается общий коэффициент шума приемника за счет увеличения вклада шумов квантования АЦП и, соответственно, снижается чувствительность;

– если схема АРУ управляется на основании информации о размахе полезного сигнала, полученной после фильтрации, то при наличии мощных мешающих сигналов либо при большом количестве мешающих сигналов велик риск перегрузки АЦП и, соответственно, необратимых искажений полезного сигнала, приводящих к резкому росту ошибок в принятом сигнале.

Решается данная проблема только за счет увеличения разрядности АЦП. Дополнительными ограничивающими факторами трактов с АЦП на несущей частоте являются:

– достаточно высокая на настоящее время стоимость АЦП с частотами дискретизации, превышающими 500 МГц, и разрядностью квантования в 14 и более бит/отсчет;

– сложность передачи высокоскоростного потока цифровых данных с АЦП на цифровую схему обработки;

– высокие требования к тактовым частотам цифровых схем, выполняющим операцию преобразования частоты.

Тем не менее, именно тракты с АЦП на несущей частоте имеют наилучшие перспективы развития. Элементная база совершенствуется, АЦП с разрядностью 16 бит при частотах дискретизации 1 ГГц и выше есть в линейке практически у всех ведущих мировых производителей (Analog Devices, Texas Instruments, Maxim Integrated и др.). В настоящее время подобные тракты для МВ- и ДМВ-диапазонов еще достаточно дорогостоящи и используются, в основном, в профессиональной аппаратуре. Однако цены на элементную базу неуклонно снижаются, что дает возможность ее использования и в радиоприемных трактах устройств массового применения.

Реализация радиопередающих трактов

Современные радиопередающие тракты строятся, как правило, по одной из 4-х представленных на рис. 3 схем. Наиболее часто встречается вариант с нулевой ПЧ (рис. 3, *а*). В нем в цифровой части формируется комплексная огибающая радиосигнала (сигналы *I*, *Q*), которая квадратурным преобразователем переносится на несущую частоту. Достоинство схемы – простота реализации, возможность достижения компромисса между увеличением тактовой частоты цифро-аналоговых преобразователей (ЦАП) DAC1, DAC2 и снижением требований к аналоговым фильтрам *Z*3, *Z*4. Квадратурное преобразование избавляет от необходимости подавления зеркального канала и позволяет перенести операции по формированию спектра радиосигнала на уровень его комплексной огибающей и выполнять их в цифровом виде фильтрами *Z*1 и *Z*2 (рис. 3, *а*–*в*). Проблемы аналогового квадратурного преобразования частоты в передатчике такие же, как и в приемнике, и способ их решения аналогичный – замещение аналоговой обработки на цифровую.

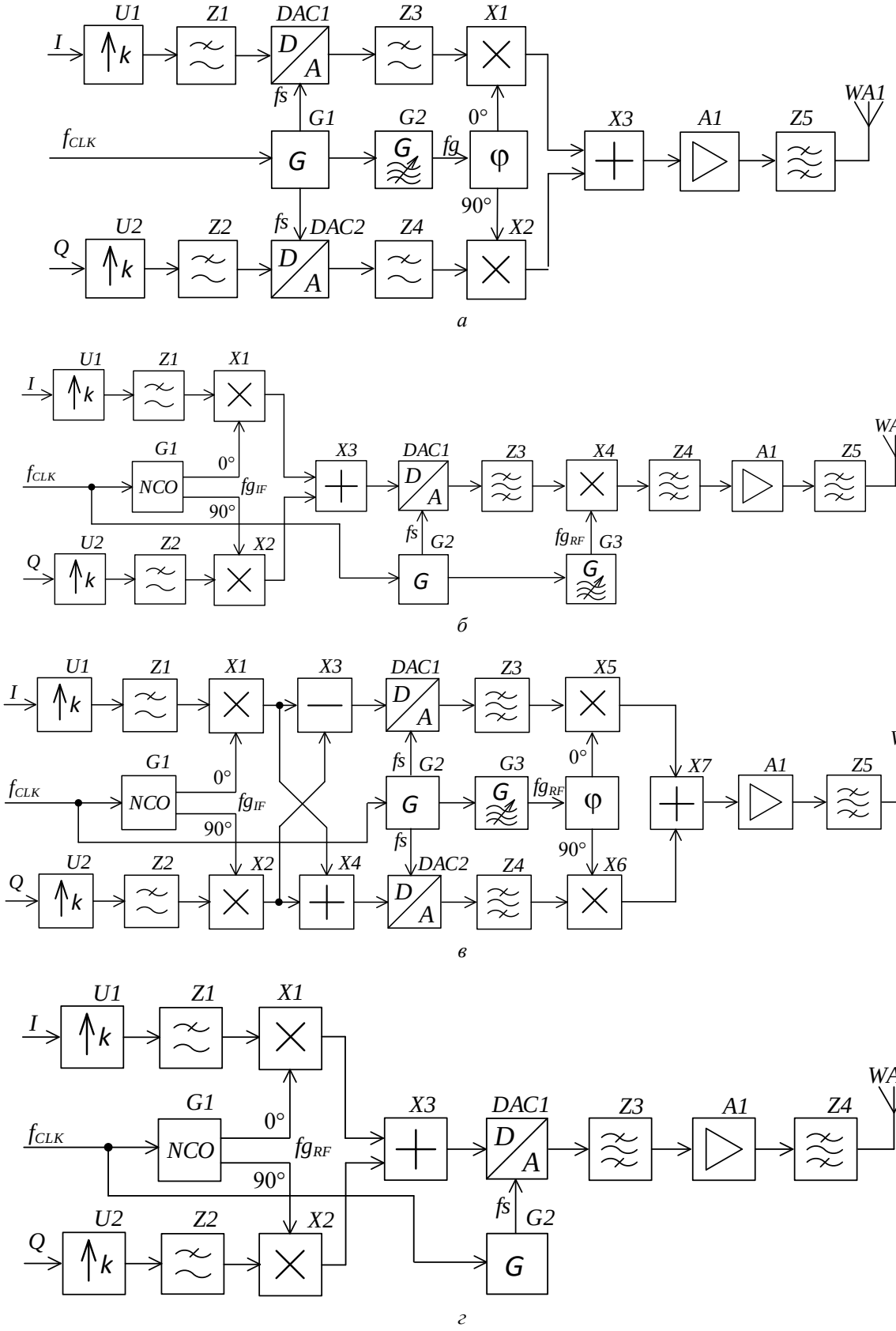


Рис. 3. Варианты построения радиопередающих трактов: *а* – с нулевой ПЧ;
б – с двукратным комплексно-вещественным преобразованием частоты;
в – с двукратным комплексным преобразованием частоты;
г – с полностью цифровым формированием радиосигнала

В зависимости от возможностей цифровой части тракта, возможны следующие варианты.

1. Цифровое преобразование на достаточно низкую (десятки, максимум – сотни мегагерц) частоту, а далее использование супергетеродинного преобразования [11] (рис. 3, *б*). Оно подходит для систем с малым отношением ширины диапазона рабочих частот $\Delta F_{\text{ДРЧ}}$ к полосе частот радиоканала $\Delta F_{\text{РК}}$, в противном случае, требуются перестраиваемые либо переключаемые фильтры *Z*4, *Z*5 для подавления зеркального канала.

2. Схема с двукратным комплексным преобразованием частоты. В ней цифровым способом на промежуточной частоте формируются две квадратурные составляющие радиосигнала со значением, аналогичным использованному в схеме на рис. 3, *б*. Перенос на несущую также квадратурный, соответственно, зеркальный канал возникает только при неидентичности аналоговых частей *I*- и *Q*-каналов, поэтому требования к фильтру *Z*5 существенно ниже.

3. Схема с полностью цифровым формированием радиосигнала (рис. 3, *г*). В ней вся операция по формированию радиосигнала и переносу его на несущую частоту выполняется в цифровом виде [12, 13], поэтому автоматически решаются все проблемы, связанные с неидентичностью каналов и проникновением сигналов гетеродина в выходной тракт. Остается проблема реализации ЦАП с высокой тактовой частотой (порядка 10 ГГц для преобразования радиосигнала на несущей частоте 3 ГГц; требования теоремы отсчетов здесь должны выполнятся с достаточным запасом для компенсации спада АЧХ по закону $\sin(f)/f$). Также в состав ЦАП должна входить схема интерполяции сигнала (блоки *U*1, *U*2 и *Z*1, *Z*2, см. рис. 3) до нужных значений тактовых частот, т.к. работа цифрового модуля кодирования и модуляции на таких частотах пока невозможна [14].

В целом, анализ построения передающих трактов показывает перспективность перехода на полностью цифровые методы формирования радиосигнала, по крайней мере, до значений несущих частот порядка 1…3 ГГц.

Заключение

Переход на полностью цифровую реализацию как радиоприемных, так и радиопередающих трактов УКВ диапазона позволяет улучшить их эксплуатационные параметры, повторяемость, а также повысить надежность работы. Элементная база для этого уже существует, причем ее доступность растет с каждым годом.

ANALYSIS OF CONSTRUCTION OF DIGITAL TRANSCEIVERS OF VHF BAND

A.L. KHAMINICH

Abstract

Methods for constructing the transceivers paths of digital radiocommunication systems, broadband wireless access, television and sound broadcasting, oriented to work in the frequency range from 30 to 3000 MHz (VHF and UHF bands) are considered. The tendency of successive substitution of analogue nodes of radiotransmission by digital devices has been noted, up to the implementation of analog-digital and digital-analog transformations directly on the carrier frequency. Problems of realization of completely digital transceiver paths are considered.

Keywords: receivers part, modulation, frequency conversion, sampling.

Список литературы

1. Радиоприемные устройства / Под ред. Н.Н. Фомина. М.: Горячая линия – Телеком, 2007. 520 с.
2. *Qizheng Gu.* RF system design of transceivers for wireless communications. Springer: Science+Business Media, Inc. 2005. 487 p.
3. Цифровые радиоприемные системы / Под ред. М.И. Жодзишского. М. : Радио и связь, 1990. 208 с.
4. *Kearney F., Frizelle D.* Complex RF Mixers, Zero-IF Architecture, and Advanced Algorithms: The Black Magic in Next-Generation SDR Transceivers // Analog Dialogue. 2017. Vol. 51, № 1. P. 15–19.
5. *Brannon B.* Where Zero-IF Wins: 50% Smaller PCB Footprint at ⅓ the Cost // Analog Dialogue. 2016. Vol. 50, Num. 3. P. 21–27.
6. *Nash E., Toh Y., Hendrickson G.* Single Chip Realizes Direct-Conversion Rx // Microwaves & RF. October 2002. P. 55–67.
7. Nash E. Correcting Imperfections in IQ Modulators to Improve RF Signal Fidelity Application Note AN-1039 [Electronic resource]. URL: http://www.analog.com/media/ru/technical-documentation/application-notes/AN-1039.pdf (date of access: 20.04.2018).
8. CN-0248 Circuit Note, An IQ Demodulator-Based IF-to-Baseband Receiver with IF and Baseband Variable Gain and Programmable Baseband Filtering, Analog Devices
9. *Jayamohan U.* Crossing a New Frontier of Multiband Receivers with Gigasample ADCs // Analog Dialogue. 2016. Vol. 50, Num. 3. P. 14–16.
10. *Harris J.* What's Up With Digital Downconverters // Analog Dialogue. 2016. Vol. 50, Num. 3. P. 7–13.
11. AN-0996 Application Note. The Advantages of Using a Quadrature Digital Upconverter (QDUC) in Point-to-Point Microwave Transmit Systems. Analog Devices.
12. Wideband RF Mixing-DAC Achieving IMD < -82 dBc Up to 1.9 GHz / E. Bechthum [et al.] //IEEE Journal of Solid-State Circuits. 2016. Vol. 51, iss. 6. P. 1374–1384.
13. A 5.3GHz 16bit 1.75GSps wideband RF Mixing-DAC achieving IMD < –82 dBc up to 1.9 GHz / E. Bechthum [et al.] // Solid-State Circuits Conference. IEEE International, Feb. 2015.
14. *Michel Pecot* Enabling High-Speed Radio Designs with Xilinx All Programmable FPGAs and SoCs White Paper: All Programmable FPGAs and SoCs. WP445 (v1.0) January 20, 2014.

УДК 621.391

ОЦЕНКА РЕЗУЛЬТАТОВ СЕГМЕНТАЦИИ ИЗОБРАЖЕНИЙ АТОМНОЙ СИЛОВОЙ МИКРОСКОПИИ НА ОСНОВЕ ИНДЕКСА СТРУКТУРНОГО ПОДОБИЯ

[1]В.В. РАБЦЕВИЧ, [1]В.Ю. ЦВЕТКОВ, [2]А.С. БАЙКЕНОВ

[1]*Белорусский государственный университет информатики и радиоэлектроники*
П. Бровки, 6, Минск, 220013, Беларусь

[2]*Алматинский университет энергетики и связи*
Казахстан

Проведена оценка результатов сегментации изображений атомной силовой микроскопии со сложной топологией с помощью индекса структурного подобия.

Ключевые слова: сегментация изображений, наращивание областей, водораздел, индекс структурного подобия.

Введение

Сегментация изображений со сложной топологией, формируемых атомным силовым микроскопом (далее – АСМ-изображений), является актуальной задачей обработки данных. Она направлена на представление изображения в упрощенном для последующего анализа виде. Результаты сегментации имеют множество практических применений в распознавании отпечатков пальцев и лиц, выделении объектов на снимках, диагностике медицинских изображений и т.д. Целью статьи является оценка основных алгоритмов сегментации на примере АСМ-изображений с помощью индекса структурного подобия (*SSIM*).

Индекс структурного подобия

Индекс структурного подобия используется при определении схожести двух изображений и формируется в результате их сопоставления по яркости, контрасту и структуре. Два сравниваемых изображения можно представить в виде $x = \{x_i \mid i = 1,2,...N\mid\}$ и $y = \{y_i \mid i = 1,2,...N\mid\}$, где N – количество пикселей.

Средняя оценка яркости производится по формулам $\mu_x = \frac{1}{N}\sum_{i=1}^{N} x_i$ и $\mu_y = \frac{1}{N}\sum_{i=1}^{N} y_i$ для двух изображений. Далее для определения контраста используется стандартное отклонение (квадратный корень дисперсии) $\sigma^2{}_x = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \mu_x)$ и $\sigma^2{}_y = \frac{1}{N-1}\sum_{i=1}^{N}(y_i - \mu_y)$. Коэффициент корреляции определяется как $\sigma_{xy} = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \mu_x)(y_i - \mu_y)$, геометрически коэффициент корреляции соответствует косинусу угла между векторами $x - \mu_x$ и $y - \mu_y$.

После объединения полученных значений получается индекс структурного подобия, который рассчитывается по формуле $SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$, где $C_1 = (k_1 L)^2$, $C_2 = (k_2 L)^2$, L – динамический диапазон, $k_1 = 0,01$, $k_2 = 0,03$ – коэффициенты.

Значения индекса структурного подобия лежат в диапазоне $[-1,1]$, где 1 соответствует полному совпадению двух изображений.

Данный метод является усовершенствованием методов среднеквадратичной ошибки (MSE) и пикового отношения сигнала к шуму (PSNR) [1]. Анализируемые изображения представляются в формате uint16 из-за большого количества сегментов.

Особенности формирования АСМ-изображений

В настоящее время атомно-силовая микроскопия находит множество практических применений в таких различных областях науки, как биология, материаловедение, радиоэлектроника, медицина и др. Атомный силовой микроскоп сканирует поверхность исследуемого образца с помощью зонда, который закреплен на конце кантилевера. При движении зонда возникают силы, которые вызывают изгиб кантилевера. Далее с помощью детектора происходит измерение этих сил. На основании этих данных получаем, в зависимости от способа измерения, получаются изображения топографии образца, отклонения или скручивания зонда [2].

Для анализа были подобраны изображения, полученные при контактном методе сканирования в режимах отклонения (рис. 1. *а, г, ж, й*), топографии (рис. 1, *б, д, з, к*) и скручивания (рис. 1, *в, е, и, л*). Данные АСМ-изображения представляют собой сложные поверхности: решетка (рис. 1, *а, б, в*), группу однородных связанных элементов (рис. 1, *г, д, е*), группу однородных одиночных элементов (рис. 1, *ж, з, и*) и полосы (рис. 1, *й, к, л*).

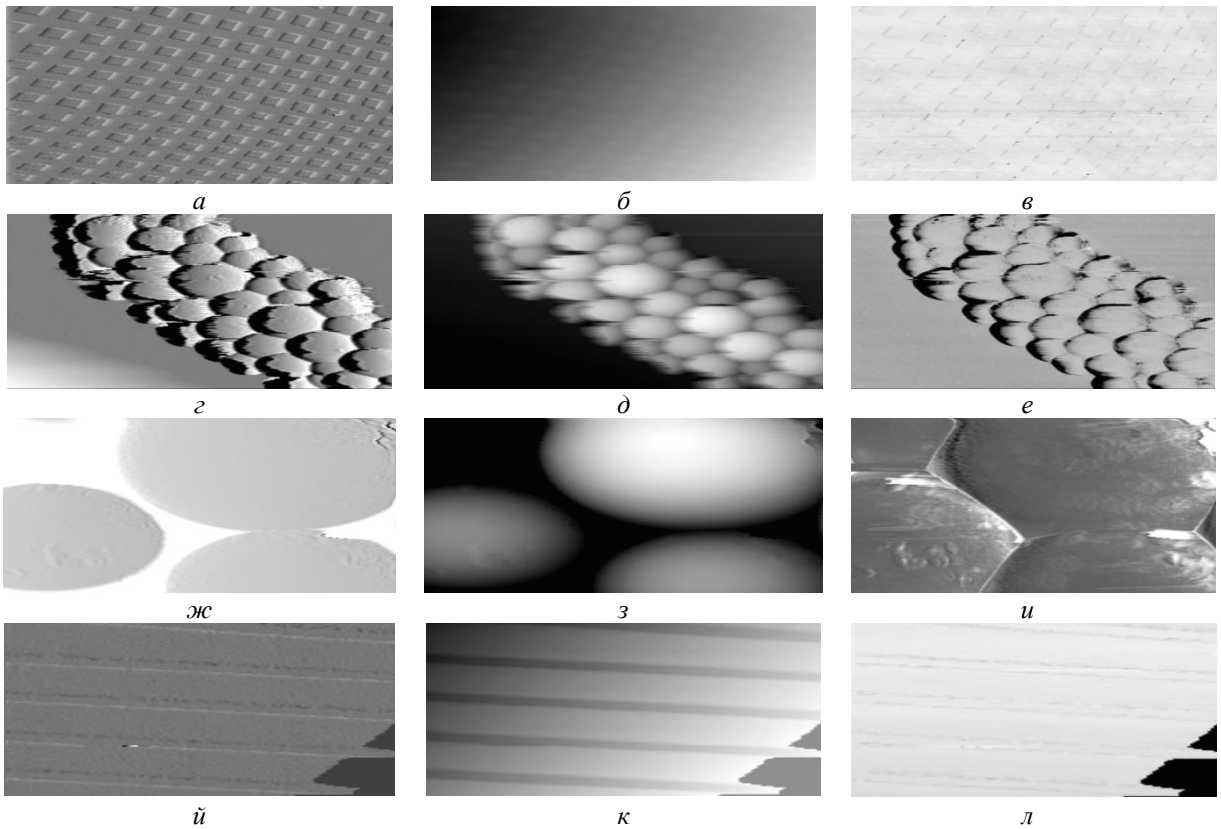


Рис. 1. АСМ-изображения, полученные в режимах:
а, г, ж, й – отклонения; *б, д, з, к* – топографии; *в, е, и, л* –скручивания

Результаты применения SSIM к оценке результатов сегментации АСМ-изображений

Далее представлены результаты функционирования разработанного алгоритма регрессивного волнового выращивания областей (рис. 2) [3], алгоритма маркерного

морфологического водораздела без участия оператора (рис. 3) [4–7] и водораздела по классическому алгоритму Винсента–Солли (рис. 4) [8, 9].

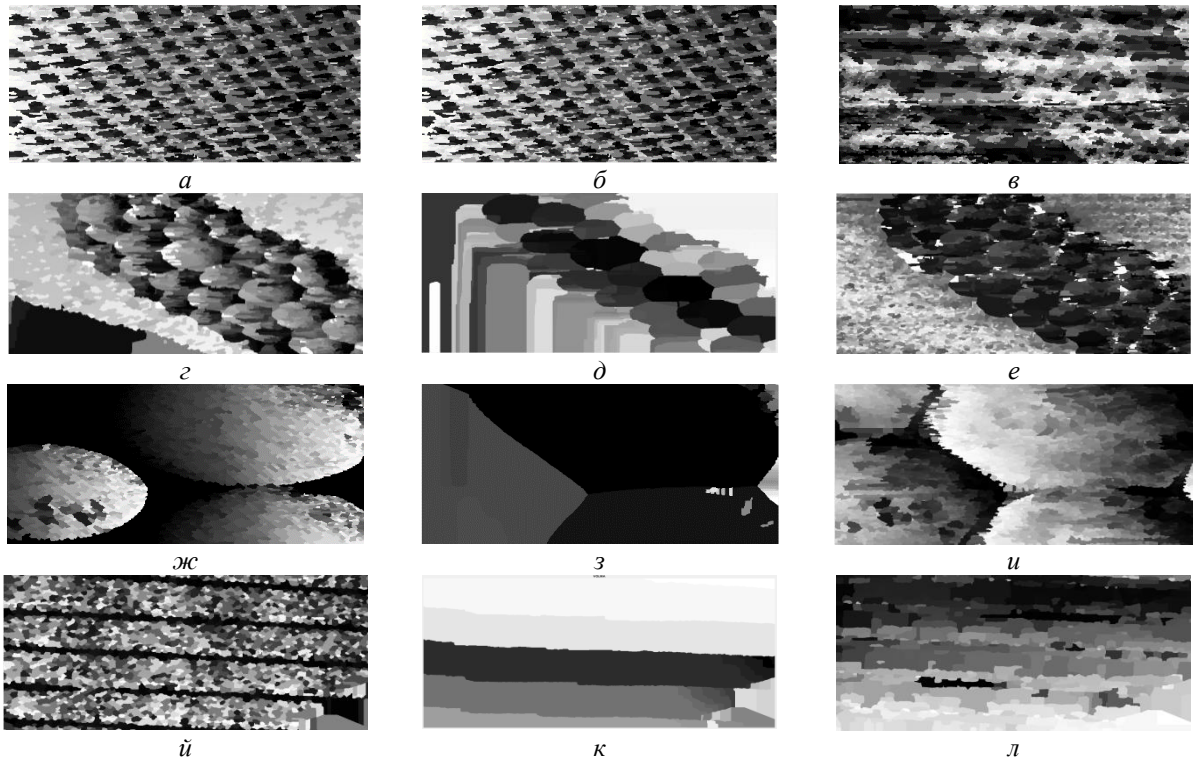


Рис. 2. Результат работы регрессивного волнового алгоритма выращивания областей для АСМ-изображений, полученных в режимах:
а, *г*, *ж*, *й* – отклонения; *б*, *д*, *з*, *к* – топографии; *в*, *е*, *и*, *л* –скручивания

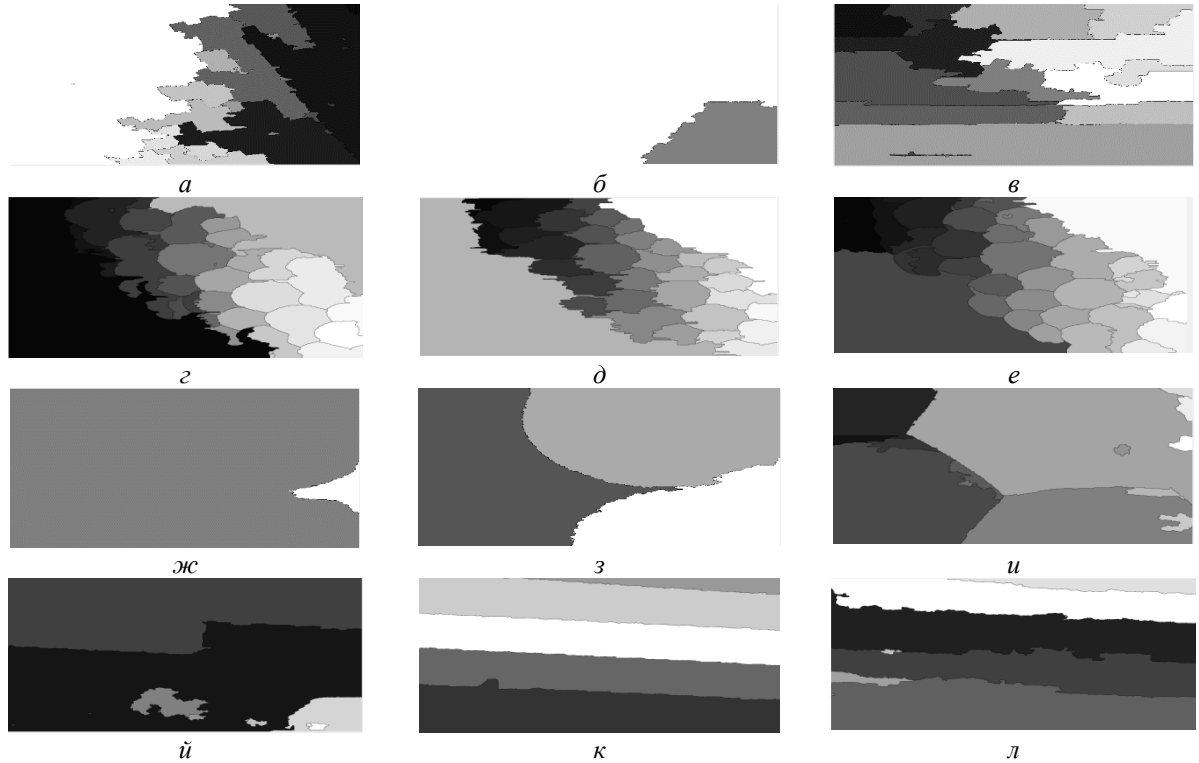


Рис. 3. Результат работы алгоритма маркерного морфологического водораздела для АСМ-изображений, полученных в режимах: *а*, *г*, *ж*, *й* – в режиме отклонения; *б*, *д*, *з*, *к* – в режиме топографии; *в*, *е*, *и*, *л* – в режиме скручивания

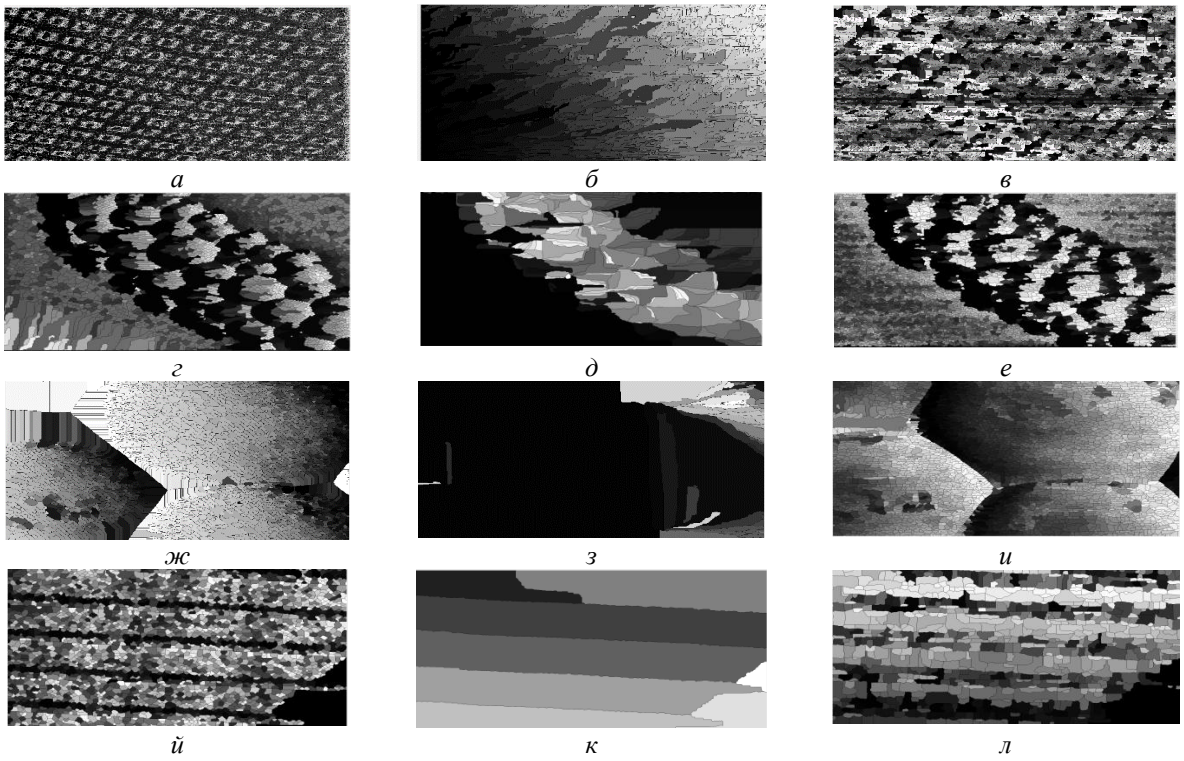


Рис. 4. Результат работы водораздела по классическому алгоритму Винсента-Солли для АСМ-изображений, полученных в режимах:
а, *г*, *ж*, *й* –отклонения; *б*, *д*, *з*, *к* –топографии; *в*, *е*, *и*, *л* – скручивания

На основе полученных результатов с помощью индекса структурного подобия выполнено сравнение каждого сегментированного изображения с исходным, представленным на рис. 1. Результаты сравнения сведены в таблице.

Оценка результаты работы алгоритмов сегментации с помощью *SSIM*

Алгоритм	Режим	1	2	3	4	Среднее значение
Волновой алгоритм	Отклонение	0,695	0,542	0,662	0,641	0,635
	Топография	0,573	0,369	0,291	0,295	0,382
	Скручивание	0,818	0,698	0,655	0,718	0,722
Маркерный водораздел	Отклонение	0,165	0,176	0,010	0,042	0,098
	Топография	0,047	0,454	0,139	0,047	0,172
	Скручивание	0,075	0,200	0,108	0,057	0,110
Водораздел по алгоритму Винсента–Солли	Отклонение	0,006	0,193	0,294	0,230	0,181
	Топография	0,315	0,377	0,178	0,050	0,230
	Скручивание	0,119	0,117	0,142	0,492	0,218

Из таблицы следует, что наибольшим индексом структурного подобия обладает разработанный алгоритм регрессивного волнового выращивания областей. Среднее значение указанного параметра в 4,6 раза больше, чем у алгоритма маркерного морфологического водораздела, и в 2,8 раза больше чем у водораздела по классическому алгоритму Винсета–Солли. Как видно из представленных данных, алгоритм волнового выращивания областей локальных максимумов дает возможность получить сегменты на исходном изображении с наибольшим индексом структурного подобия, водораздел по классическому алгоритму Винсента–Солли приводит к возникновению лишних сегментов, что уменьшает значение *SSIM*. Метод морфологического маркерного водораздела без участия оператора приводит, в свою очередь, к недостаточной сегментации изображений, что также уменьшает значение *SSIM*.

Заключение

Анализ результатов сегментации АСМ-изображений показал, что методы на основе водораздела выделяют области с существенной ошибкой, связанной с избыточной или недостаточной сегментацией. Сегментацию с наибольшим индексом структурного подобия обеспечивает алгоритм волнового выращивания областей локальных максимумов. В среднем, этот индекс в 4,6 раза больше, чем у маркерного морфологического водораздела без участия оператора и в 2,8 раза больше, чем у водораздела по классическому алгоритму Винсента–Солли.

EVALUATION OF SEGMENTATION RESULTS FOR ATOMIC FORCE MICROSCOPY IMAGES ON THE BASIS OF STRUCTURAL SIMILARITY INDEX

V.V. RABTSEVICH, V.Yu. TSVIATKOU, A.S. BAYKENOV

Abstract

An evaluation of different types of segmentation for atomic force microscopy images was made using the index of structural similarity.

Keywords: image segmentation, area building, watershed, structural similarity index.

Список литературы

1. Image quality assessment: From error visibility to structural similarity / Z. Wang [et al.] // IEEE Transactions on Image Processing. 2004. Vol. 13, № 4. P. 600–612.
2. *Gaskell K., Ramsdell D.* AFM Standart Operating Procedure. Surface Analyse Centre Department of Chemistry and Biochemistry, University of Maryland. 2013. P. 14–15.
3. *Рабцевич В.В., Цветков В.Ю.* Алгоритм регрессивного волнового выращивания областей АСМ-изображений // Матер. междунар. науч.-техн. семинара «Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных». Минск, апрель–декабрь 2016 г. Ч. 2. С. 41–47.
4. *Gauch J.M.* Image segmentation and analysis via multiscale gradient watershed hierarchies // IEEE transactions on image processing. 1999. Vol. 8, № 1. P. 69–79.
5. *Khiyal M.S.H., Khan A., Bibi A.* Modified Watershed Algorithm for Segmentation of 2D Images // Informing Science and Information Technology. 2009. Vol. 6. P. 876–886.
6. *Gonzalez R.C., Woods R.E.* Digital Image Processing. Pearson Education, 2008.
7. *Arindrajit Seal, Arunava Das, Prasad Sen.* Analyzing the Image Quality in Various Applications using Segmentation Algorithms and Image recognition systems // Int. J. of Computer Science and Information Technologies (IJCSIT). 2015. Vol. 6, № 3. P. 2295–2297.
8. *Vincent L., Sollie P.* Watershed in Digital Spaces: an efficient algorithm based on immersion simulation // IEEE Transactions on Pattern Analysis and Machine Intelligence. 1991. Vol. 13. P. 583–598.
9. *Chang J.H., Fan K.Ch., Chang Y.L.* Multi-modal gray-level histogram modeling and decomposition // Image and Vision Computing. 2002. Vol. 20. P. 203–216.

УДК 004.932

КАК ОДНИМ ЧИСЛОМ ОБЪЕКТИВНО ОЦЕНИТЬ КАЧЕСТВО ИЗОБРАЖЕНИЯ?

В.В. СТАРОВОЙТОВ

Объединенный институт проблем информатики НАН Беларуси,
Сурганова, 6, Минск, 220012, Беларусь

Рассматривается понятие численной оценки качества цифрового изображения. Показано, что обобщенный параметр качества в виде среднего значения множества локальных оценок качества не лучший вариант единой оценки. Представлены результаты исследований описания локальных оценок параметрами распределения Вейбулла.

Ключевые слова: цифровое изображение, локальная оценка, параметры формы, распределение Вейбулла.

Введение

Рассмотрим понятие «оценки качества цифрового изображения». Широко известная статья профессора Бовика [1] всю проблему вместила в следующее название: «Почему оценка качества изображения так сложна?». Рассмотрим рис. 1. и попытаемся дать оценку качества каждому изображению, например, по 10-бальной системе. Это потребует некоторого времени у любого человека, причем оценки будут самые разные.

Рис. 1. Изображения, которые необходимо оценить по 10-балльной системе

А если требуется оценить сходство или отличия двух изображений? На рис. 2. представлены два варианта одного изображения. Корреляция между этими изображениями равна 0,9420. Они отличаются одной строкой.

Рис. 2. Изображения, отличающиеся одной строкой

Популярные оценки

Для сравнения цифровых сигналов используется множество оценок: коэффициент корреляции, среднеквадратичное отклонение (*MSE*), пиковое отношение сигнал / шум (*PSNR*) и др. Эти оценки часто применяются к цифровым изображениям. Однако они плохо соответствуют субъективным оценкам, что является их главным недостатком (см. рис.3).

Рис. 3. Оригинал (слева) и разные варианты искажений изображения
с одинаковым *MSE* относительно оригинала, равным 225

Для изображений разрабатываются оценочные функции, которые учитывают визуальные особенности (контраст, резкость и другие характеристики). Эти функции условно делятся на три группы:

– сравнение с эталоном (full-reference),

– с использование частичной информации об эталоне (reduced-reference),

– меры без эталона (no-reference).

Последняя группа – это фактически функции оценки качества. К первой группе относится широко используемая мера SSIM, которая определяет степень сходства с эталоном.

Как правильнее: similarity или dissimilarity?

В научной литературе для схожих понятий используются самые разные термины: метрики качества, меры сходства и различия изображений и т.п. Следует отметить, что большинство подобных функций не являются метриками в математическом смысле.

В 90-е гг. прошлого столетия при сравнении двух изображений чаще применялся термин dissimilarity или различие изображений.

Начиная с 2000-х гг., в основном, используется термин similarity или сходство изображений. Фактически это эквивалентные понятия. Как правило, similarity равно 1, когда анализируемое изображение совпадает с эталоном. При этом их различие или dissimilarity равно единице за вычетом Similarity. Иногда в таких случаях говорят, что качество анализируемого изображения идеально.

В 1997 г. была предложена методика построения функций сравнения изображений типа dissimilarity для оценки отличий в паре изображений [2]. Было показано, что оценка MSE является частным случаем, предложенным в книге. Основным признаком тех лет при сравнении изображений была яркость пикселов. Отличием предложенной методики сравнения был учет не только яркости пикселов с одинаковыми координатами, но в ближайшей окрестности. К сожалению такой, подход до сих пор не используется в мерах сравнения изображений.

Mean Opinion Score – усредненная субъективная оценка

Mean Opinion Score (MOS) [3] или усредненная субъективная оценка качества используется в области телекоммуникационных систем при анализе изображений и видеопоследовательностей. Определяется методикой субъективного оценивания с качественной шкалой: от 3 до 11 оценок (хорошо, плохо и т.п.). Каждый эксперт в заданной шкале ставит бальную оценку качества, после чего оценки, полученные для одного объекта анализа, усредняются. Таким образом, это оценка субъективного типа, выставленная усредненным пользователем.

К недостаткам такого типа оценок относятся следующие:

– при изменении группы экспертов могут измениться выставленные оценки;

– процесс довольно долгий и затратный;

– итоговые оценки субъективны и приближенны.

На рис. 4 показано, что субъективные оценки качества *MOS*, выставленные людьми, не имеют линейной зависимости от количественных оценок типа *PSNR*.

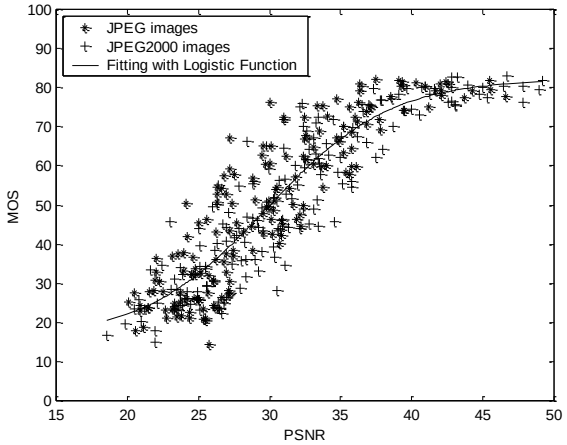


Рис. 4. Сложная зависимость *MOS* от *PSNR*

Исследуемая гипотеза об оценке качества нового типа

В настоящее время автор изучает следующую гипотезу. Оценку качества следует вычислять в 2 этапа – сначала оценить ряд локальных признаков, затем вместо их среднего значения использовать параметр формы их пространственного распределения.

Рассмотрим пример. Средние значения двух множеств локальных признаков, представленных на рис. 5, будут одинаковыми, но форма их расположения различна. Левое множество примерно образует круг, правое – эллипс. Из уравнения эллипса $kx^2+y^2r^2 = 0$ следует, что форма расположения этих данных определяется параметром k. При $k = 1$ это круг, при k, близком к единице – почти круг, при большем или меньшем k – это эллипс.

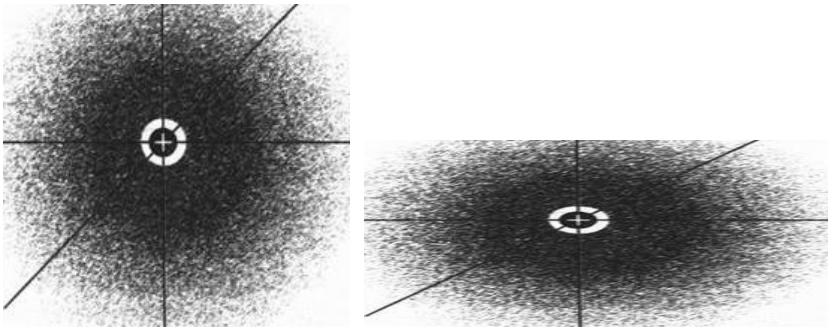


Рис. 5. Два множества локальных характеристик, имеющих одинаковый центр, но разную форму

Аналогичный вывод можно сделать для гистограмм локальных признаков, вычисленных для разных изображений. Например, на рис. 6 показаны три варианта кривых Гаусса, имеющих одинаковое средне значение, но разные формы из-за различий в дисперсии данных. Проведенными авторами исследования показали, что при оценке сходства двух реально похожих изображений локальные признаки не имеют нормального распределения. Это означает, что глобальная оценка в виде среднего значения не совсем верно отражает локальные отличия.

В качестве альтернативы нормальному распределению локальных признаков рассматривается распределение Вейбулла. Оно имеет достаточно разнообразную форму при изменении параметра формы k (см. рис. 7).

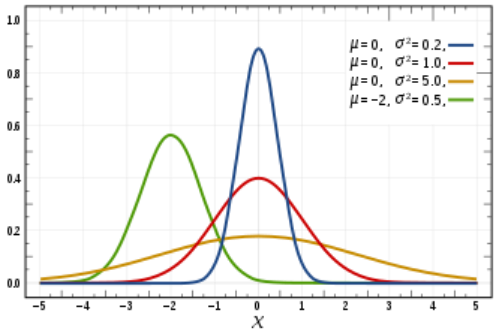


Рис. 6. Нормально распределенные локальные признаки

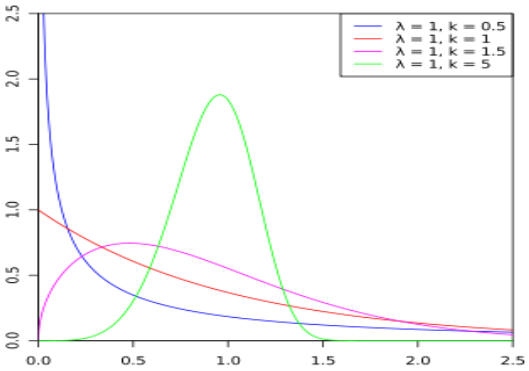


Рис. 7. Варианты распределения Вейбулла

Экспериментальные исследования

Один из независимых вариантов проверки вышеописанной гипотезы, использованный авторами, заключался в исследовании широко известной меры оценки качества двух изображений (т.е. первого типа) SSIM. Использовалась ее авторская реализация в системе Matlab. Для пары изображений, представленных на рис. 2, *SSIM* равен 0.9177, коэффициент корреляции – 0,9420, параметр масштаба кривой Вейбулла – 0,9553. Визуальный анализ показывает, что изображения практически одинаковы, т.е. оценка их сходства должна быть максимальна (в нормированном варианте – 1).

На рис. 8 представлены локальные отличия в паре этих изображений, полученные при вычислении меры *SSIM*. Значение меры *SSIM* равно 0,9177 и соответствует максимуму кривой Гаусса.

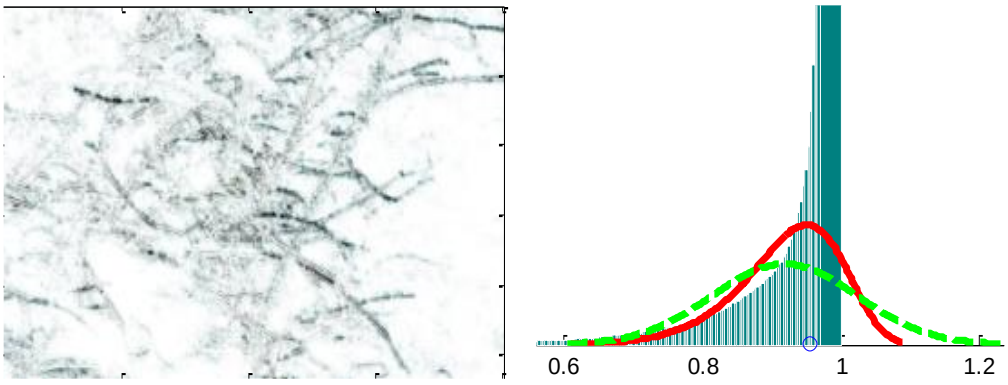


Рис. 8. Слева – карта локальных признаков меры SSIM, справа – их гистограмма, аппроксимированная кривыми Вейбулла (сплошная линия) и Гаусса (пунктирная линия)

Заключение

В работе рассмотрено понятие численной оценки качества цифрового изображения. Такие оценки должны удовлетворять противоречивым требованиям: быть точными и соответствовать визуальным оценкам, сделанным человеком. Показано, что среднее арифметическое локальных оценок не лучший вариант глобальной оценки качества. Исследована гипотеза его замены параметром формы распределения локальных данных. На основе первых результатов выполненного исследования можно сделать вывод о возможности получения принципиально новой количественной оценки качества цифровых изображений.

HOW EVALUATE OBJECTIVELY THE IMAGE QUALITY WITH USE OF ONE NUMBER?

V.V. STAROVOITOV

Abstract

The concept of numerical estimation of digital image quality is considered. It is shown that the generalized quality parameter in the form of the mean value of set of local quality estimates is not the best variant of a single assessment. Study results of the description of local estimates by the parameters of the Weibull distribution are described.

Keywords: digital image, local estimates, shape parameters, Weibull distribution.

Список литературы

1. *Wang Z., Bovik A.C., Lu L.* Why is image quality assessment so difficult? // IEEE International Conference on Acoustics, Speech, and Signal Processing, 2002. Vol. 4. P. 3313–3316.
2. *Старовойтов В.В.* Локальные геометрические методы цифровой обработки и анализа изображений. Минск: ИТК НАН Беларуси. 1997.
3. Recommendation ITU-R BT. 1788 Methodology for the subjective assessment of video quality in multimedia applications, 2007.

УДК 681.327

КОМБИНИРОВАНИЕ ИНФОРМАЦИОННЫХ ПРИЗНАКОВ ДЛЯ РАСПОЗНАВАНИЯ ОБЪЕКТОВ НА ИЗОБРАЖЕНИЯХ РАЗЛИЧНОГО СПЕКТРАЛЬНОГО ДИАПАЗОНА

В.В. ГАНЧЕНКО, Е.Е. МАРУШКО

Объединенный институт проблем информатики НАН Беларуси,
Сурганова, 6, Минск, 220012, Беларусь

Статья посвящена разработке алгоритмов обработки аэроснимков сельскохозяйственных полей картофеля для задачи мониторинга состояния посевов. Предлагаемые алгоритмы основаны на комбинировании цветовых, текстурных и фрактальных характеристик исходных изображений и предназначены для формирования карт заболеваемости растительности. Данные карты являются исходными данными для систем внесения средств защиты растений.

Ключевые слова: точное земледелие, детектирование заболеваний, классификация.

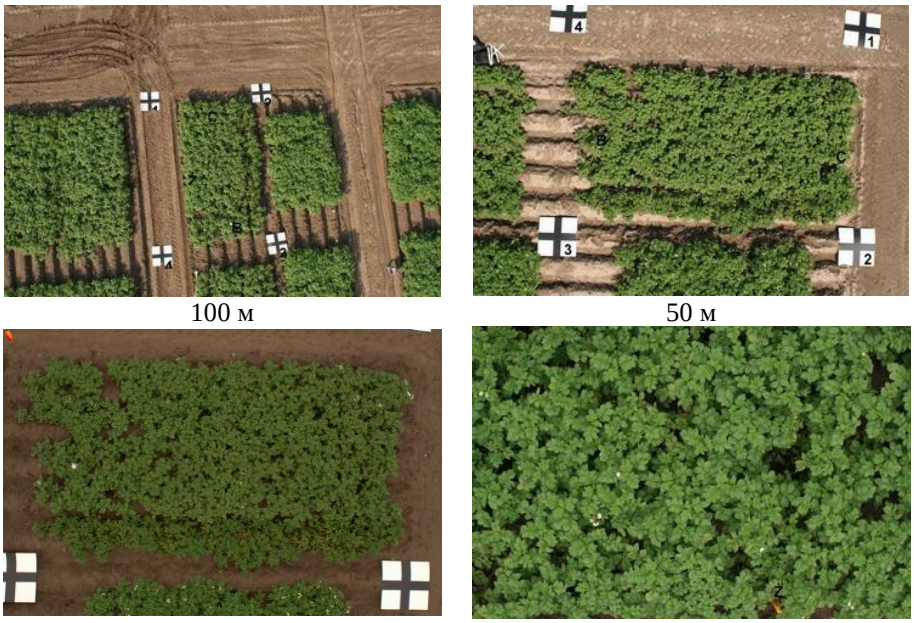
Введение

Развитие точного земледелия предполагает наличие точной и оперативно обновляемой информации о состоянии растительности и почвы. Получение подобной информации возможно только при использовании дистанционного зондирования. Дистанционные методы мониторинга сельскохозяйственных полей дают возможность оперативно выявить пораженные болезнью участки растительности. Выявление заболевания на ранних стадиях развития позволяет оперативно и с минимальными затратами локализовать и вылечить заболевание. Выделяют два основных подхода к решению задачи выявления пораженных участков: спектрометрический и оптический [1–7]. Спектрометрический подход позволяет определять многие заболевания на ранних стадиях развития. Однако этот подход требует наличия многоспектрального съемочного оборудования, что не всегда возможно.

Цель работы состоит в создании алгоритмов обработки цветных изображений растительных покровов, полученных с помощью цифровой съемки различного пространственного разрешения. Суть метода заключается в комбинированном применении цветовых характеристик растительности, а также текстурных характеристик Харалика и фрактальной размерности для построения пространства признаков и выделения объектов на цветных изображениях сельскохозяйственных полей.

Исходные данные

Объектом исследования являются цветные изображения сельскохозяйственных полей (см. рис. 1). Для получения данных был выделен небольшой участок поля при помощи четырех квадратных меток. Длина стороны квадрата равна одному 1 м, также на метку нанесены две черных линии шириной 20 см, образующие перекрестие. Наличие этих меток позволяет не только определять участок для исследований, но и вычислять пространственное разрешение снимков. Часть участка заражена заболеванием, симптомами которого является изменение цвета в связи с изменением уровня хлорофилла и увяданием листьев растений. Съемка выполнялась с использованием БПЛА с высоты 5, 15, 50 и 100 м.



100 м 50 м

15 м 5 м

Рис. 1. Примеры исходных аэрофотоснимков

Текстурные характеристики

Текстурные характеристики выражают разность значений интенсивности соседних пикселей, составляющих изображения, при этом значения оценок этой разности отличаются для различных типов подстилающих поверхностей. Это позволяет осуществлять кластеризацию данных на основании этих оценок, что обеспечивает возможность разделять площадные объекты с различными текстурами [8]. Для выбора текстурных характеристик, которые используются для сегментации снимков сельскохозяйственных полей, выполняется оценка возможности использования различных текстурных характеристик Харалика для выделения площадных объектов на снимках растительных покровов.

Вычисление текстурных характеристик снимка выполняется в так называемом «скользящем окне». Его размер выбран экспериментально и составляет 4×4 пикселя. То есть выбранные текстурные характеристики вычисляются для небольших участков изображения. Значения текстурных характеристик собираются в матрицы, которые преобразовываются к целочисленным значениям в диапазоне [0; 255]. Полученная матрица представляет собой полутоновое изображение, которое позволяет сравнить значения оценок текстурных характеристик для различных участков изображений (рис. 2). Суть вычисления фрактальной сигнатуры состоит в том, что квантованные значения интенсивности двумерного сигнала должны располагаться между двумя функциями, называемыми верхней и нижней поверхностями. Верхняя поверхность U содержит множество точек, значения которых всегда, по крайней мере, на один квант интенсивности превышают интенсивность входного сигнала. Нижняя поверхность L имеет значения, которые всегда ниже, по крайней мере, на один квант интенсивности входного изображения [9] (рис. 3).

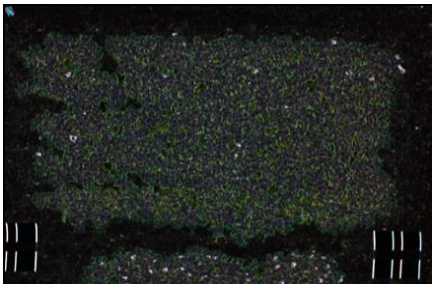


Рис. 2. Текстурная характеристика Contrast для снимка поля с высоты 15 м

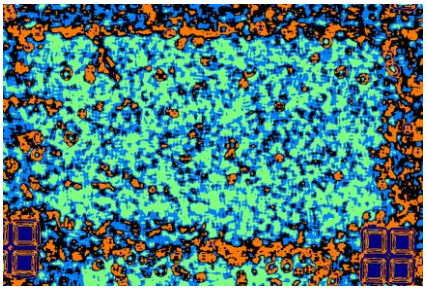


Рис. 3. Фрактальная размерность снимка поля

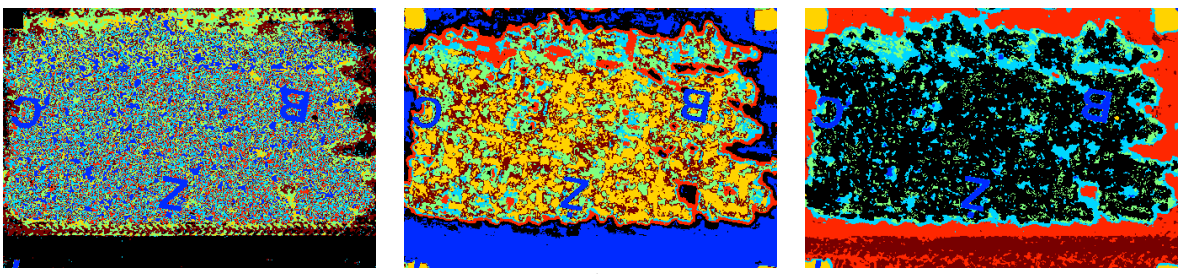
Совместная сегментация

Для выделения однородных областей на исходных изображениях используется алгоритм совместной сегментации. Его суть состоит в совместной обработке исходных изображений и их фрактальных и текстурных характеристик (т.е. имеющийся исходный снимок, мультиспектральный, в общем случае, дополняется изображениями текстурных и фрактальных характеристик). Схема работы алгоритма приведена на рис. 4.

Рис. 4. Схема алгоритма сегментации с использованием дополнительных признаков

Пространство признаков, на основании которых принимается решение, формируется из данных матриц цветовых характеристик исходного изображения, а также текстурных и фрактальных характеристик, вычисленных для каждого цветового канала исходного снимка.

Результаты, получаемые при сегментации, зависят от использованных каналов и алгоритма кластеризации. Так, применение только цветовых каналов позволяет выделять области, которые могут соответствовать пораженным растениям, однако в эти же кластеры зачастую попадают граничные области (области на изображениях, где находятся рядом пиксели, соответствующие растительности и почве), что осложняет дальнейшее использование результатов. При этом выбором того или иного алгоритма кластеризации можно получать большее либо меньшее количество кластеров малой площади (1–3 пикселя). Так, использование алгоритма Fuzzy C-Means [10] (рис. 5, *а*) дает большое количество мелких областей, состоящих порой всего из нескольких пикселей, что в значительной степени осложняет визуальную интерпретацию результатов. Однако этот алгоритм имеет наибольшую скорость работы. Наименьшее количество таких областей дает алгоритм Gath-Geva (рис. 5, *в*) [11], т.к. для его функционирования необходимо наибольшее количество машинных ресурсов по сравнению с другими алгоритмами. Алгоритм Gustafson-Kessel [12] дает средние результаты при средних затратах машинных ресурсов (рис. 5, *б*).

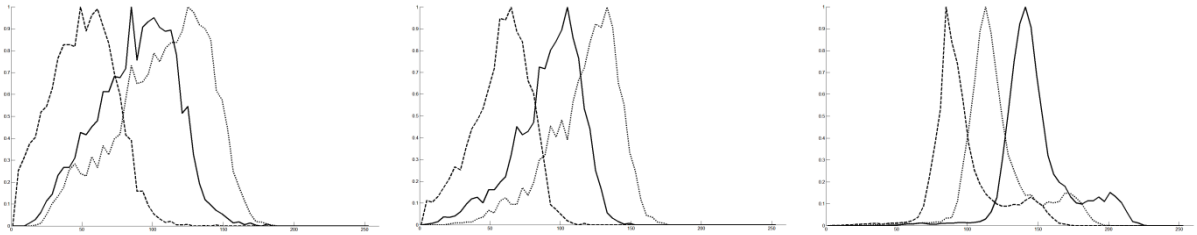


а *б* *в*

Рис. 5. Пример результатов кластеризации с помощью различных алгоритмов:
а – Fuzzy C-Means; *б* – Gustafson-Kessel; *в* – Gath-Geva

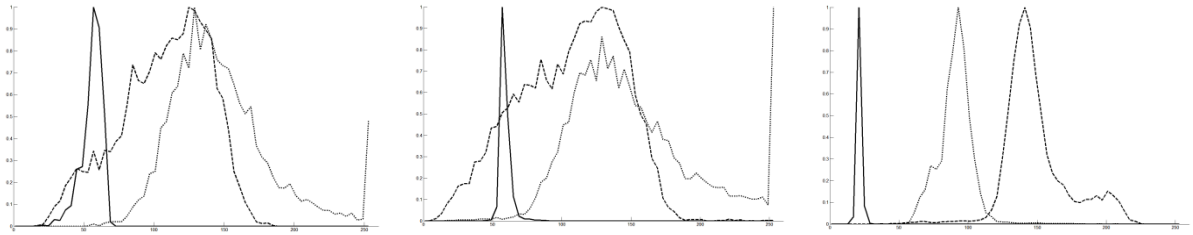
Цветовые характеристики

Использование нормализованных редуцированных гистограмм позволяет описывать в виде массива из 192 элементов цветовые характеристики некоторой окрестности пикселя распознаваемого площадного объекта, причем цветовые характеристики могут рассматриваться как в цветовом пространстве RGB (рис. 6), так и в пространстве HSV (рис. 7).



а *б* *в*

Рис. 6. Нормализованные редуцированные гистограммы, построенные для RGB-представления: *а* – «пораженные заболеванием растения»; *б* – «здоровые растения»; *в* – «почва»

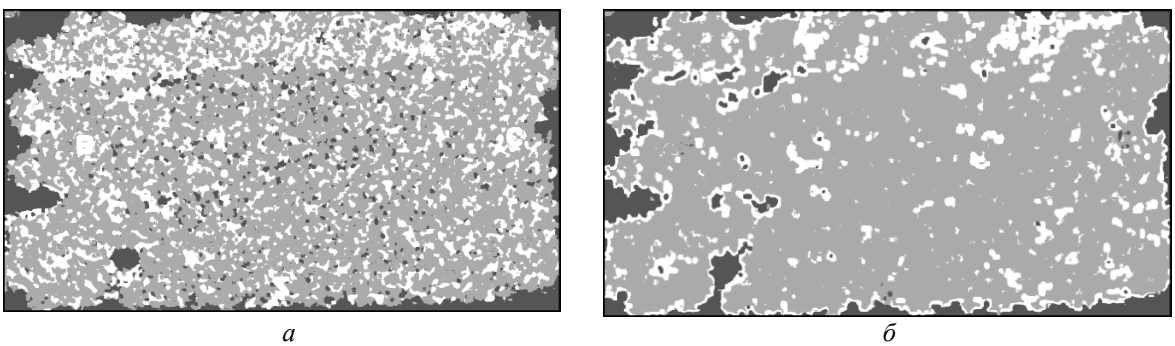


а *б* *в*

Рис. 7. Нормализованные редуцированные гистограммы, построенные для HSV-представления: *а* – «пораженные заболеванием растения»; *б* – «здоровые растения»; *в* – «почва»

В основе алгоритмов распознавания лежит предлагаемый нейросетевой классификатор, построенный на основе многослойного персептрона с 192 входами, использующего в качестве входных данных нормализованные редуцированные гистограммы с тремя выходами, соответствующими распознаваемым классам объектов: «пораженная растительность», «здоровая растительность» и «почва». Применение искусственных нейронных сетей для классификации позволяет осуществлять распознавание площадных объектов на аэроснимках сельскохозяйственных полей, полученных при различных условиях освещения, с помощью единого алгоритма. Для настройки весов персептрона использован алгоритм обратного распространения ошибки. При этом на вход персептрона подаются нормализованные гистограммы, полученные из выделенных оператором изображений объектов.

Выборка данных для распознавания осуществляется «скользящим окном» размером 21×21 пиксель, полученным экспериментально. Пример результатов распознавания приведен на рис. 8. Белым цветом выделены пораженные заболеванием растения, светло-серым – здоровые, темно-серым – почва.



а *б*

Рис. 8. Пример результатов распознавания: *а* – с использованием RGB; *б* – с использованием HSV

Заключение

Описаны разработанные алгоритмы, предназначенные для решения задачи мониторинга состояния сельскохозяйственной растительности на примере аэроснимков полей картофеля для задач точного земледелия. Предложенные алгоритмы основаны на совместном анализе цветовых характеристик, а также текстурных характеристик (текстуры Харалика и фрактальная размерность). Указанные характеристики используются как для нечеткой сегментации аэрофотоснимков сельскохозяйственной растительности, так и для дальнейшей нейросетевой классификации выделенных сегментов на базе цветовых характеристик, представленных в виде нормализованных редуцированных гистограмм.

Предложенные алгоритмы могут быть использованы при разработке специализированных программных приложений, в том числе и в виде модулей геоинформационных систем.

COMBINATION OF INFORMATION CHARACTERISTICS FOR OBJECT RECOGNITION ON IMAGES OF DIFFERENT SPECTRAL RANGE

V.V. GANCHENKO, E.E. MARUSHKO

Abstract

The article is devoted to development of algorithms for processing of aerial photographs of potato agricultural fields for the task of crops state monitoring. The proposed algorithms are based on combining of color, texture and fractal characteristics of the original images. These algorithms are designed to generate maps of crops diseases. These maps are the initial data for plant protection systems.

Keywords: precision agriculture, disease detection, classification.

Список литературы

1. *Беляев Б.И., Катковский Л.В.* Оптическое дистанционное зондирование. Минск: БГУ, 2006.
2. *Шовенгердт Р.А.* Дистанционное зондирование. Модели и методы обработки изображений. М.: Техносфера. 2013.
3. *Chao K.*, Chen Y.R., Kim M.S. Machine vision technology for agricultural applications // Elsevier science transactions on computers and electronics in agriculture. 2002. Vol. 36. P. 173–191.
4. Do leaf surface' characteristics affect agrobaeterium infection in tea / N. Kumar [et al.] // J. Biosci. 2004. Vol. 29, № 3. P. 309–317.
5. Identification of weed, corn using BP network based on wavelet features and fractal dimension / L. Wu [et al.] // Scientific Research and Essay. 2009. Vol. 4 (11). P. 1194–1400.
6. *Qin Zh., Zhang M.* Detection of rice sheath blight for in-season disease management using multispectral remote sensing // Int. J. of Applied Earth Observation and Geoinformation. 2005. Vol. 7. P. 115–148.
7. *Aksoy S., Akcay H.G., Wassenaar T.* Automatic mapping of linear woody vegetation features in agricultural landscapes using very high-resolution imagery // IEEE Transactions on Geoscience and Remote Sensing. 2010. № 48 (1, 2). P. 511–522.
8. *Haralick R.M., Shanmugam K., Dinstein I.* Textural Features for Image Classification // IEEE Transactions on Systems, Man and Cybernetics. 1973. No.6. P. 610–621.
9. *Федер Е.* Фракталы. Москва: Мир, 1991.
10. Fuzzy C-Means Clustering [Электронный ресурс]. URL: https://home.deib.polimi.it/matteucc/Clustering/tutorial_html/cmeans.html (дата обращения: 01.04.2018).
11. *Gath I., Geva A.B.* Unsupervised optimal fuzzy clustering // IEEE Transactions on Pattern Analysis and Machine Intelligence. 1989. Vol. 11, № 7. P. 773–781.
12. *Babuka R., van derVeen P.J., Kaymak U.* Improved covariance estimation for Gustafson-Kessel clustering // Proc. of the 2002 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE'02). USA, 12–17 May 2002. Vol. 2. P. 1081–1085.

УДК 519.725;007.001.362;528.85/.87(15)

БЛОЧНО-СУБПОЛОСНЫЙ ВЛОЖЕННЫЙ АЛГОРИТМ СЖАТИЯ ГИПЕРСПЕКТРАЛЬНЫХ ДАННЫХ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ ЗЕМЛИ

[1]Д.Ю. ПЕРЦЕВ, [2]А.А. ДУДКИН

[1]*Белорусский государственный университет информатики и радиоэлектроники*
П. Бровки, 6, Минск, 220013, Беларусь

[2]*Объединенный институт проблем информатики НАН Беларуси*
Сурганова, 6, Минск, 220012, Беларусь

Представлен блочно-субполосный вложенный алгоритм сжатия гиперспектральных данных дистанционного зондирования Земли. Проведена оценка эффективности работы представленного алгоритма и пропускной способности в зависимости от уровня вейвлет-разложения.

Ключевые слова: дистанционное зондирование, сжатие гиперспектральных данных, контекстное моделирование, вейвлет-разложение.

Введение

Дистанционное зондирование – способ получения информации об объекте без непосредственного физического контакта с ним. На борту летательного аппарата (например, спутника либо самолета) устанавливается спектрометр, задачей которого является фиксация излучения с поверхности. Бортовая система осуществляет предобработку полученных данных и передает их в центр управления. Результаты такой съемки используются в сельском и лесном хозяйстве, метеорологии, а также в целях контроля водных ресурсов, поиска полезных ископаемых и энергоносителей, военной разведка, мониторинга чрезвычайных ситуаций.

Различают мультиспектральные и гиперспектральные спектрометры. Основное отличие заключается в том, что гиперспектральные спектрометры фиксируют данные в виде непрерывного диапазона спектра с определенным шагом (например, в диапазоне от 500 до 700 нм выделяют 20 спектральных каналов с шагом 10 нм). В то же время, мультиспектральные данные могут иметь те же 20 спектральных каналов, но распределенных в спектральном диапазоне неравномерно (например, 5 каналов в диапазоне от 500 до 600 нм и 15 – в диапазоне от 600 до 700 нм).

В настоящее время широкому применению гиперспектральных данных для аэрокосмического мониторинга препятствуют отсутствие достаточного количества спутников и воздушных судов, оборудованных соответствующими спектрометрами, сложности, связанные с обработкой и интерпретацией больших потоков информации, формируемой этими приборами. В связи с этим одним из актуальных направлений в развитии систем дистанционного зондирования Земли сегодня является создание спутниковой гиперспектральной аппаратуры и технологий обработки, получаемой с помощью нее информации. Снимки, размещенные на портале AVIRIS [1, 2], обладают следующими характеристиками: пространственное разрешение – 512×677 пикселей, спектральное разрешение – 224 слоя, радиометрическое разрешение – 16 бит. Это приводит к формированию 148 Мбайт данных на один снимок, что, с учетом ограниченности пропускной способности радиоканала и непродолжительного сеанса связи с Землей, приводит к актуализации задачи сжатия данных снимков.

Разработанный алгоритм сжатия

Разработанный алгоритм сжатия (рис. 1) включает следующие этапы исполнения: определение опорного кадра и декорреляция каналов в спектральной области, вейвлет-разложение [3] результата, энтропийное кодирование с применением алгоритмов контекстного моделирования.

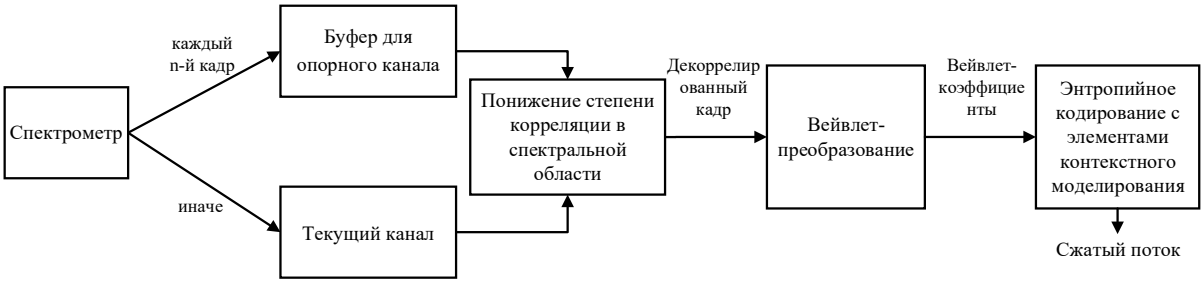


Рис. 1. Алгоритм сжатия гиперспектральных данных

На первом шаге формируются данные от спектрометра с разбиением на отдельные кадры по спектральной плоскости. При этом предполагается, что каждый *n*-й кадр является опорным и используется для декорреляции. Это необходимо для повышения производительности, т. к. появляется возможность параллельной обработки. Дополнительно каждый кадр, полученный от спектрометра, разбивается на блоки фиксированного размера и в дальнейшем эти кадры обрабатываются независимо друг от друга.

Отличительной чертой гиперспектральных данных является высокая избыточность в спектральной области, для минимизации которой введен шаг «Понижение степени корреляции в спектральной области». Для этого применяется вычитание опорного кадра.

На третьем шаге для опорного или декоррелированного кадра выполняется дискретное вейвлет-преобразование. Этот шаг позволяет выполнить декорреляцию кадров в пространственной области гиперспектрального куба. При тестировании использовалось вейвлет-разложение 5/3.

Финальным шагом является энтропийное кодирование со встроенным алгоритмом контекстного моделирования. В результате выполнения данного шага формируется сжатый поток, который передается в центр управления полетом.

Алгоритм энтропийного кодирования с элементами контекстного моделирования

В основе алгоритма энтропийного кодирования с элементами контекстного моделирования – кластеризация энергии (концентрация энергии в небольших областях), свойственная вейвлет-преобразованию. Блок-схема алгоритма кодирования представлена на рис. 2. Пусть **X** – матрица с результатами вейвлет-преобразования (новый кадр). Для преобразованного кадра X строится пирамида, корневым элементом которой является множество 2×2 элемента, содержащих вейвлет-коэффициенты. Каждый последующий уровень аппроксимирует и детализирует вейвлет-коэффициенты, расположенные на предыдущих уровнях. В основании пирамиды размещаются оригинальные значения вейвлет-коэффициентов $\{c_{i,j}\}$, находящиеся в позиции (i, j) в преобразованном кадре X (рис. 3). Идея применения пирамиды заключается в том, что велика вероятность, что бóльшая часть энергии будет сосредоточена на верхних уровнях разложения, и ее количество будет уменьшаться по мере приближения к основанию.

На втором шаге формируется множество значимых коэффициентов. При этом пирамидальное представление данных позволяет оптимизировать алгоритм поиска и максимально быстро сфокусироваться на областях с большим уровнем энергии. Некоторое множество T называется значимым по отношению к битовой плоскости n, если выполняется условие: $\max\limits_{(i,j)\in T}\{|c_{i,j}|\} \geq 2^n$, где $c_{i,j}$ – вейвлет-коэффициент с координатами (i, j), $n = \log_2(|c_{i,j}|)$ – число бит кодового слова вейвлет-коэффициента (максимальный уровень битовой плоскости).

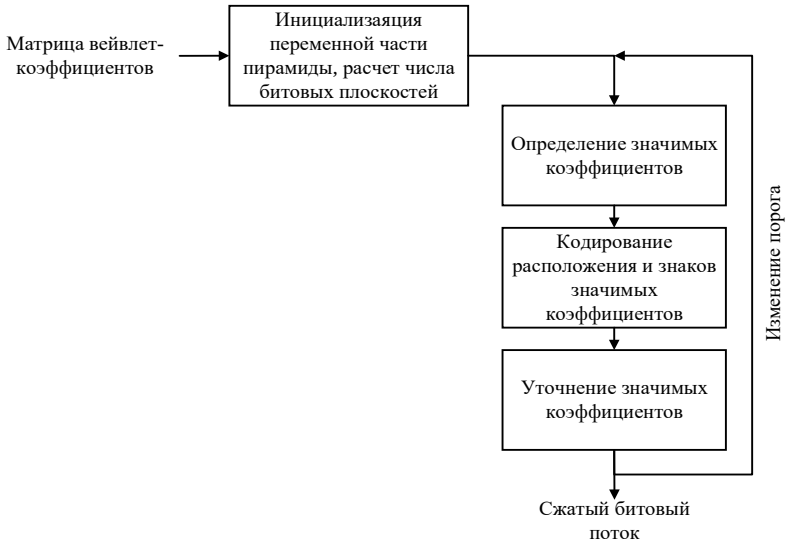


Рис. 2. Блок-схема энтропийного кодирования для вейвлет-коэффициентов

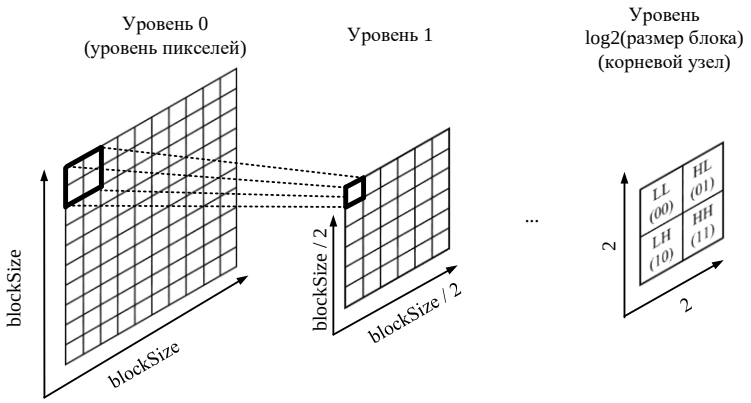


Рис. 3. Структура пирамиды

На следующем шаге области, которые содержат значимые коэффициенты, группируются и кодируются. Области, которые вероятнее всего содержат незначимые коэффициенты, группируются в новые множества, для которых выполняется уточнение значимости (шаг 4).

После обработки текущей битовой плоскости значение порога n изменяется и выполняется переход на следующую битовую плоскость. Если проанализированы все битовые плоскости или достигнута заданная точность, обработка прекращается.

Структура сжатого потока

Структура формируемого выходного битового потока для каждого блока изображения представлена на рис. 4.В выходной поток записываются следующие данные:

– n_{max} – максимальный размер битовой плоскости (1 байт);

– *refCount* – число секций с уточняющими байтами (1 байт);

– M_k, k = [0, *refCount*] – число значащих байт в секции k (3 байта);

– $sort_k$, k = [0, *refCount*] – поток значащих байт в секции k;

– N_k, k = [0, *refCount*] – число уточняющих байт в секции k (3 байта);

– ref_k, k = [0, *refCount*] – поток уточняющих байт в секции k.

Основным недостатком, представленной структуры, является кратность 1 байту, что для многих элементов на практике является избыточным.

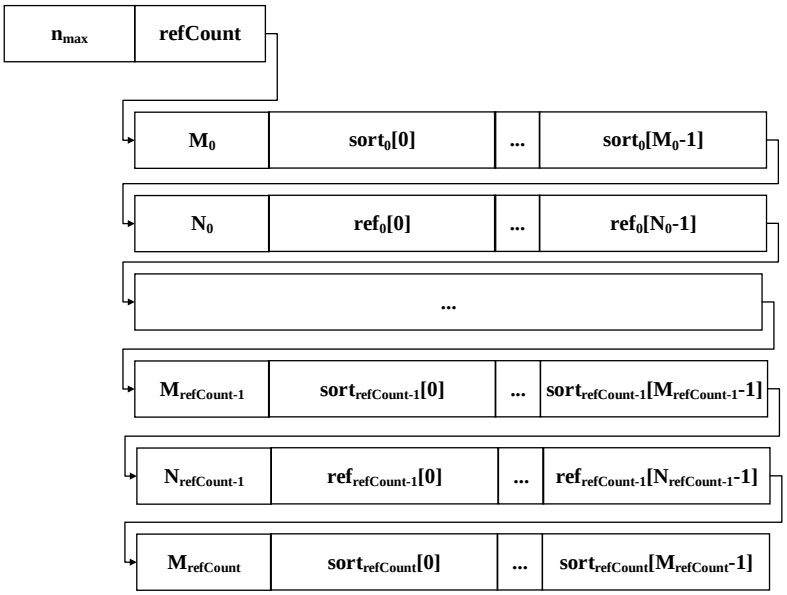


Рис. 4. Структура сжатого потока

Тестирование алгоритма сжатия

Для тестирования алгоритма использовались Фурье-интерферограммы, синтезированные на основе данных проекта AVIRIS [1], находящихся в свободном доступе.

Технические характеристики тестовых данных:

– пространственное разрешение: 1024×1024 пикселей;

– радиометрическое разрешение: 12 бит на пиксель;

– число спектральных каналов: 200.

В качестве тестовой системы использовался персональный компьютер со следующей конфигурацией:

– CPU: Intel Core i5-3570K (3.4 ГГц);

– ОЗУ: 8 Gb DDR3.

Полученная зависимость пропускной способности от уровня декомпозиции вейвлет-разложения показана на рис. 5 (при этом использовались 5/3 вейвлеты). На основе полученных данных можно сделать вывод, что оптимальная размерность блока – 128×128 либо 256×256, а оптимальный уровень декомпозиции начинается с 3. При тестировании коэффициента сжатия использовался уровень декомпозиции, равный 4.

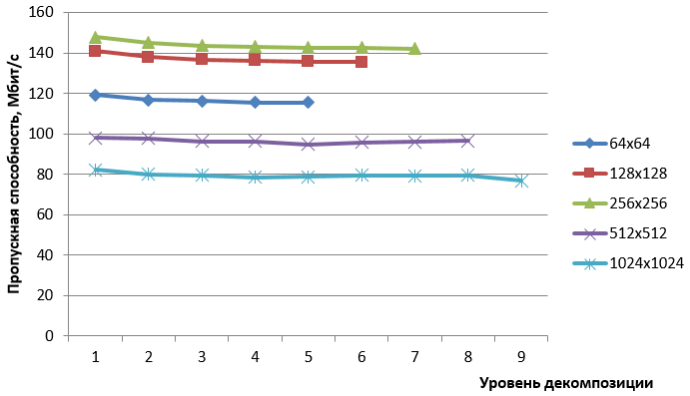


Рис. 5. Зависимость пропускной способности от уровня декомпозиции

Как видно из табл. 1 и 2, оптимальными параметрами для представленного алгоритма на тестовой выборке является размер блока в 128×128 элементов. Данный параметр позволяет достигнуть пропускную способность при сжатии потока данных от 121,5 Мбит/с для опорных кадров и до 146 Мбит/с – для последующих.

Таблица 1. Средние значения коэффициента сжатия и время кодирования для опорного кадра

Кадр 1				
Бит/пиксель	Размер блока	Коэффициент сжатия, раз	Время кодирования, мс	Пропускная способность, МБит/с
12	128	1,489	394,987	121,52
12	256	1,495	432,333	111,03
Кадр 101				
12	128	1,509	395,717	121,30
12	256	1,514	436,521	109,96

Таблица 2. Средние значения коэффициента сжатия и время кодирования для последующих кадров

Кадр со 2 по 5				
Бит/пиксель	Размер блока	Коэффициент сжатия, раз	Время кодирования, мс	Пропускная способность, МБит/с
12	128	1,649	371,071	129,36
12	256	1,656	411,522	116,64
Кадр со 101 по 104				
12	128	2,060	328,229	146,24
12	256	2,068	356,927	134,48

Заключение

Представленный алгоритм является универсальным и может быть применен для кодирования любых данных, имеющих трехмерную структуру. При этом оптимальные характеристики были получены с использованием следующих параметров:

– размер блока для кодирования – 128×128 элементов, т.к. данный размер обеспечивает максимальную производительность алгоритма в целом;

– уровень вейвлет-разложения – 3 либо 4, т.к. соотношение производительности и результирующего коэффициента сжатия в этом случае является оптимальным.

Дальнейшая работа связана с оптимизацией алгоритма для повышения быстродействия, исследованием возможности аппаратной реализации и тестированием на обширной выборке тестовых данных.

Исследование выполнено при финансовой поддержке БРФФИ (*проекты Ф18ПЛШГ-008 и Ф18В-005*).

THE BLOCK AND SUBBAND ENCLOSED ALGORITHM OF COMPRESSION OF HYPERSPECTRAL DATA OF REMOTE EARTH SENSING

D.Yu. PERTSAU, A.A. DOUDKIN

Abstract

The block and subband enclosed hyperspectral data compression algorithm is presented. Data stream compression throughput assessment depending on wavelet decomposition level is carried out, the overall performance of the presented algorithm is estimated.

Keywords: remote sensing, compression of hyperspectral data, context modeling, wavelet decomposition.

Список литературы

1. Airborne Visible/Infrared Imaging Spectrometer. Официальный портал AVIRIS [Электронный ресурс]. URL: http://aviris.jpl.nasa.gov/ (дата обращения: 20.04.2018).
2. *Chang, C.-I*. Hyperspectral data processing: algorithm design and analysis. New York: John Wiley & Sons, 2013.
3. *Sayood Kh*. Introduction to Data Compression. Morgan Kaufmann, 2017.

УДК 004.415.2

РАЗРАБОТКА МАКЕТНОГО ОБРАЗЦА ВЫСОКОПРОИЗВОДИТЕЛЬНОГО ВИДЕОПРОЦЕССОРА

С.А. БАЙРАК, М.М. ТАТУР, М.М. ЛУКАШЕВИЧ, НГУЕН ХОНГ ВУ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Системы технического зрения являются программно-аппаратными комплексами, предназначенными для обработки видеоданных и принятия решений о характеристиках реальных объектов и сцен. В настоящей статье анонсируются результаты разработки и создания макетного образца высокопроизводительного видеопроцессора с оригинальной параллельной архитектурой для решения задач технического зрения в промышленных системах.

Ключевые слова: система технического зрения, программно-аппаратный комплекс, видеоаналитика, процессор.

Введение

Система технического зрения – это программно-аппаратный комплекс, предназначенный для обработки видеоданных и принятия решений о характеристиках реальных объектов и сцен. В связи с развитием оптических и вычислительных компонентов таких систем в настоящее время область применения технического зрения существенно расширилась: от простых систем видеонаблюдения до автоматического интеллектуального неразрушающего контроля на разных стадиях производства (например, контроля упаковки и маркировки изделий, точности изготовления и окраски деталей, контроля позиционирования компонент и т.п.). В зависимости от решаемой прикладной задачи математическое обеспечение, алгоритмы, программное обеспечение и вычислительная аппаратура значительно отличаются, но вместе взаимообусловлены в рамках системы технического зрения. В настоящем исследовании акцент сделан аппаратную составляющую. Работа выполнена в рамках гранта фонда фундаментальных исследований (№Ф16ВГ-001 от 20.07.2016 г.).

Обоснование необходимости разработки

В ряде случаев, когда необходимо обрабатывать большие объемы видеоданных в реальном времени, универсальная (последовательная) архитектура вычислительного комплекса не в состоянии обеспечить необходимую производительность. В таких ситуациях прибегают к использованию либо универсальных параллельных вычислительных кластеров, что не всегда приемлемо по конструктивным и экономическим соображениям, либо созданию специализированных вычислительных комплексов с оригинальными параллельными архитектурами. Создание подобной архитектуры процессора и апробация в реальном технологическом процессе (выбранном в ходе работы) вынесено в цель проекта [1–7].

Современные методы и алгоритмы обработки изображений отличаются большим разнообразием. Архитектура процессора, на котором предполагается их реализация, должна быть оптимальной с точки зрения предоставления различных типов вычислительных ресурсов. Поэтому современный процессор для обработки изображений должен удовлетворять двум основным требованиям: универсальность и вычислительная мощь. С точки зрения аппаратных средств, данные для обработки – видеопоток или стационарные изображения –

характеризуются следующими основными параметрами: объемом, скорость поступления, тип методов и алгоритмов для их обработки.

Объем данных для обработки и скорость их поступления может сильно отличаться, в зависимости от конкретных условий применения систем обработки изображений. Данные параметры являются во многом определяющими в случае необходимости выполнения обработки в режиме реального времени. В этой ситуации скорость обработки данных должна быть равна или выше скорости их поступления. Очень часто оба этих параметра сводят к одному – так называемой пиксельной частоте, т.е. скорости поступления одного пикселя изображения.

Характер данных и цель их обработки определяют используемые в системе методы и алгоритмы, которых на сегодняшний день разработано большое количество. При их аппаратной реализации с использованием вычислительной системы можно воспользоваться двумя основными подходами: последовательным и параллельным.

Последовательный подход предполагает реализацию методов и алгоритмов путем последовательного выполнения отдельных операций на едином, часто универсальном, вычислительном ядре. Основные плюсы данного подхода – универсальность, простота и гибкость. Основной недостаток – скорость обработки данных. Чаще всего последовательный подход основывается на использовании современных микропроцессорных систем, в том числе и специально предназначенных для решения задач цифровой обработки сигналов (DSP-процессоры).

Параллельный подход предполагает реализацию методов и алгоритмов путем организации параллельно работающих модулей, выполняющих одновременную обработку различных частей поступающих данных. Для этого чаще всего используют различные микросхемы программируемой логики – FPGA. Основное достоинство данного метода – возможность построения системы с практически неограниченной вычислительной мощностью, а недостаток – низкая универсальность и сложность разработки такой системы.

При этом не все алгоритмы и методы одинаково хорошо реализуются с использованием обоих подходов. Чаще всего для конкретного алгоритма или метода хорошо подходит только один из подходов. Важным фактором универсальности процессора обработки данных является также наличие достаточного числа интерфейсов, выполняющих следующие основные функции:

– прием данных для обработки, при необходимости – в режиме реального времени;

– выдача результата обработки, при необходимости – в режиме реального времени;

– организация полнодуплексного канала управления системой обработки.

Структурная схема параллельного процессора

Создаваемый процессор с параллельной архитектурой планируется к применению в системах технического зрения, предназначенных для широкого круга задач (рис. 1).

Несмотря на различные области применения, общим процессинговым блоком будет являться оригинальный процессор с параллельной архитектурой, проблемно-ориентированной на алгоритмы обработки изображений и управления. Основное назначение процессора – обеспечение высокой производительности, достаточной для реализации алгоритмов в реальном времени.

Очевидно, что интерфейсы процессора и системное (сервисное) программное обеспечение должны быть унифицированы, в то время как функциональная спецификация будет определяться прикладным программным обеспечением и конструктивными особенностями конкретных контроллеров.

Структурная схема параллельного процессора обработки изображений представлена на рис. 2.

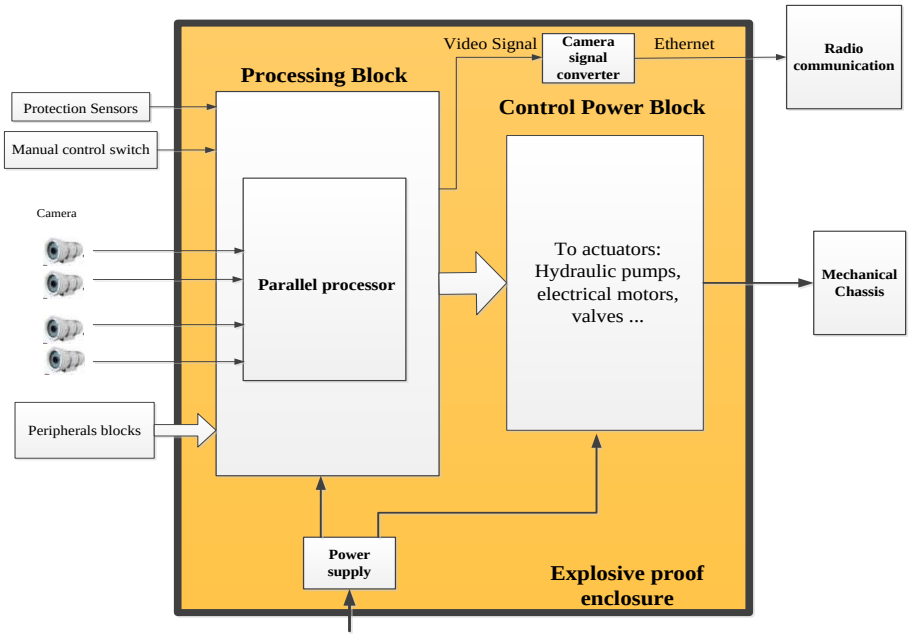


Рис. 1. Общая схема бортового контроллера мобильного робота

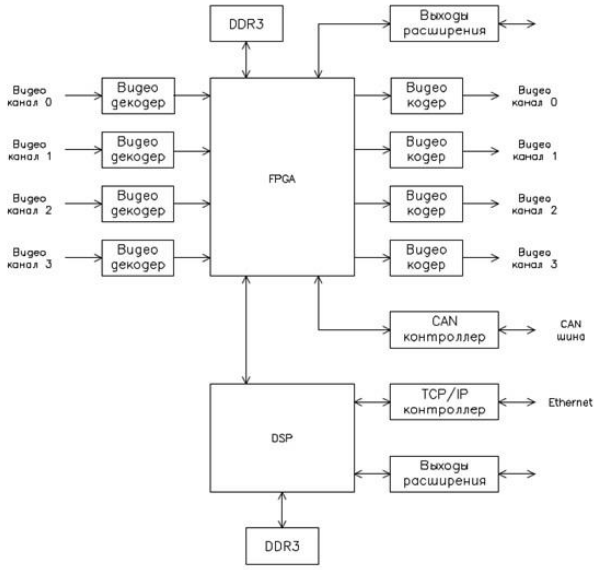


Рис. 2. Структурная схема параллельного процессора

Основные технические характеристики и ограничения.

Процессор состоит из двух вычислительных ядер: DSP процессор (Texas Instruments TMS320C6674/76/78), FPGA (Xilinx Artix / Kintex 7).

Каждое вычислительное ядро имеет свое ОЗУ размером 128МБ DDR3. Внешние интерфейсы:CAN, Ethernet 100/1000, 4 независимых видеовхода, 4 независимых видеовыхода. Вычислительные возможности: обработка видео HD 720p (разрешение 1280×720) при частоте кадров 60 кадров/с; выполнение следующих операций в режиме реального времени для видеопотока HD 720p60 (1280×720, частота– 60 кадров/с):

– коррекция цвета (color correction);
– коррекция гистограммы (гамма-коррекция. GAMMA correction);
– фильтрация изображения (noise reduction);
– подчеркивание границ (edge enhancement).

При реализации более интеллектуальных функций параметры входного видео, при котором будет обеспечиваться требование режима реального времени, может отличаться. Процессор обеспечивает 1600 MIPS и 16 GFLOPS.

Функциональная схема параллельного процессора

Функциональная схема процессора представлена на рис. 3.

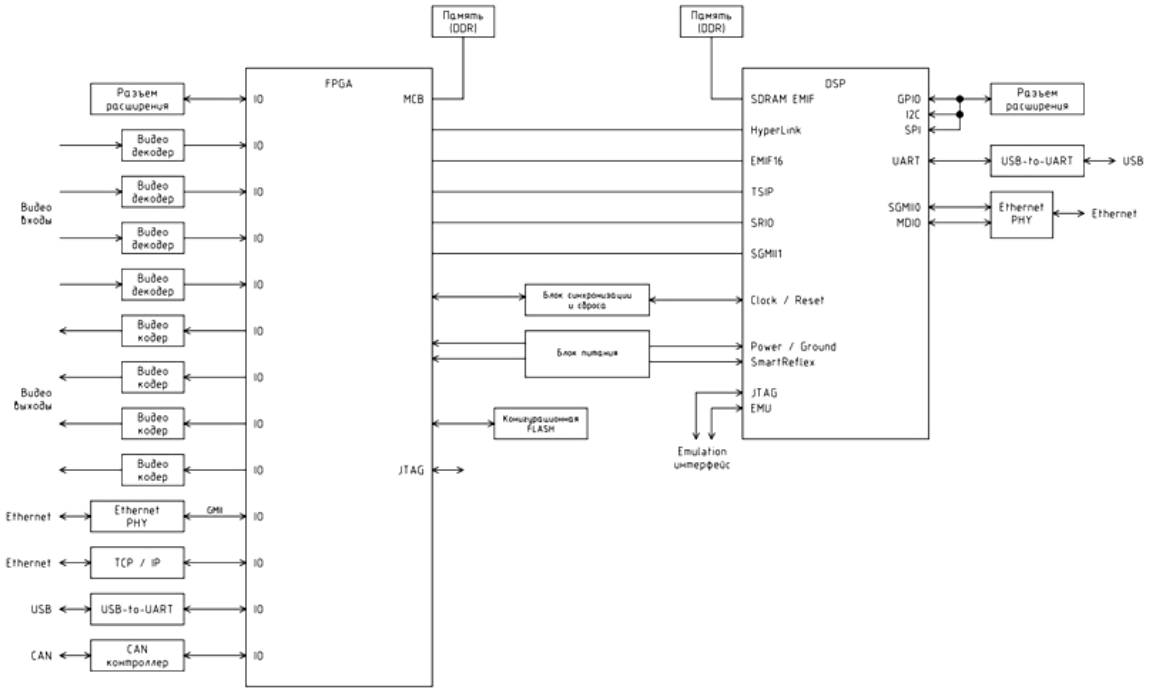


Рис. 3. Функциональная схема параллельного процессора

В качестве микросхемы FPGA используется микросхема Artix 7 компании Xilinx, а в качестве DSP процессора – процессор TMS320C6678 компании Texas Instruments. Основная задача при проектировании процессора, включающего два разнотипных вычислительных ядра, является обеспечение их взаимодействия и возможности обмена большими объемами данных между ними. Для этого используются следующие интерфейсы: HyperLink, EMIF16, TSIP, SRIO; SGMII. Интерфейс HyperLink разработан специально для межпроцессорного взаимодействия устройств, поддерживающих технологию KeyStone. Он обладает наибольшими скоростью и функциональными возможностями. При этом для его использования необходимо покупать дополнительные IP-ядра, так как документация от производителя не достаточна для его самостоятельной реализации. В связи с этим данный интерфейс пока не является основным для обмена данными.

Заключение

Разработана архитектура параллельного процессора обработки изображений на базе двух вычислительных ядер: микросхемы FPGA, предназначенной для реализации параллельных алгоритмов обработки, и DSP процессора, предназначенного для реализации последовательных алгоритмов обработки. Оба процессорных ядра имеют независимые блоки динамической памяти и выходы расширения, предназначенные для подключения дополнительных периферийных устройств. Основное управление осуществляется через TCP/IP-сеть или CAN-шину. Для обеспечения взаимодействия и возможности обмена большими объемами данных между вычислительными ядрами определены интерфейсы.

DEVELOPMENT OF THE LAYER SAMPLE OF HIGH-PERFORMANCE VIDEOPROCESSOR

S.A. BAIRAK. M.M. TATUR, M.M. LUKASHEVICH, NGUYEN HONG VU

Abstract

Computer vision system is software and hardware system designed to videoanalysis and decision-making about the characteristics of real objects and scenes. The aim of the work is to develop and create a prototype of a high-performance processor with an original parallel architecture for solving technical vision problems in industrial systems.

Keywords: computer vision system, software and hardware system, videoanalysis, processor.

Список литературы

1. *Байрак С.А., Одинец Д.Н., Татур М.М.* Параллельный процессор идентификации образов // Технологии безопасности. 2012. № 1 (22). С. 46–47.
2. *Вереник Н.Л., Сейткулов Е.Н., Татур М.М.* Разработка проблемно-ориентированных процессоров семантической обработки информации. Минск // Электроника Инфо. 2012. № 8. С. 95–98.
3. Моделирование алгоритмов управления автоматических трансмиссий по обеспечению плавного включения передач / А.В. Белевич [и др.] // Нейрокомпьютеры: разработка, применение. 2013. № 2. С. 40–44.
4. Имитационная модель векторного процессора на примере задачи поиска пути в графе / Н.Л. Вереник [и др.] //Искусственный интеллект. 2013. №4 (62). С. 89–100.
5. Алгоритм поиска кратчайшего пути в графе для семантического процессора / С.Н. Боранбаев [и др.] // Вест. КазНТУ им. К.И. Сатпаева. 2013. № 4 (98). С. 290–296.
6. Модель семантического процессора с параллельной архитектурой / Е.Н. Сейткулов [и др.] // Вест. КазНТУ им. К.И. Сатпаева. 2013. № 4 (98). С. 283–290.
7. *Tatur M.* Problem-Oriented Processors for the Solving of Classification Tasks // J. of Information, Control and Management Systems (Slovakia). 2013. Vol. 11, № 2. P. 155–164.

Всегда храню в душе своей…

Всегда храню в душе своей
Родных, друзей, учителей.
Ведь и они всегда со мной
Делились собственной душой.

Как много в помыслах своих
По жизни мы берем от них,
Не успевая осознать:
А сможем ли вернуть, отдать?

Быть может, даже и не им,
Пусть незнакомым и чужим,
Тем, кто их помыслы и труд
Возьмут, как зернышки, поймут,

Что мы живем, себя любя,
Но всё ж не только для себя,
Не для одних себя живём.
Беря, мы что-то отдаём.

И, если сможем и успеем,
Мы их зернышки посеем.
Пусть будет отдых или труд,
Но всё же зернышки взойдут.

И, может быть, пусть через годы
Дадут плоды когда-то всходы.
И потому в душе своей
Всегда храню родных, друзей, учителей.

Астровский Иван Иванович