

3(70)/2014

INFORMATSIONNO- UPRAVLIAIUSHCHIE SISTEMY (INFORMATION AND CONTROL SYSTEMS)

REFEREED EDITION

Founder

«Information and Control Systems», Ltd.

Editor-in-Chief

M. Sergeev

Dr. Sc. Tech., Professor, St.-Petersburg, Russia

Deputy Editor-in-Chief

E. Krouk

Dr. Sc. Tech., Professor, St.-Petersburg, Russia

Executive secretary

O. Muravtsova

Editorial Council

L. Chubraeva

RAS Corr. Member, Dr. Sc. Tech., Professor, St. Petersburg, Russia

L. Fortuna

PhD, Professor, Catania, Italy

A. Fradkov

Dr. Sc. Tech., Professor, St. Petersburg, Russia

V. Kozlov

Dr. Sc. Tech., Professor, St. Petersburg, Russia

C. Christodoulou

PhD, Professor, Albuquerque, New Mexico, USA

B. Meyer

PhD, Professor, Zurich, Switzerland

A. Ovodenko

Dr. Sc. Tech., Professor, St. Petersburg, Russia

Y. Podoplyokin

Dr. Sc. Tech., Professor, St. Petersburg, Russia

Yu. Shokin

RAS Academician, Dr. Sc. Phys.-Math., Novosibirsk, Russia

V. Simakov

Dr. Sc. Tech., Professor, Moscow, Russia

V. Vasilev

RAS Corr. Member, Dr. Sc. Tech., Professor, St. Petersburg, Russia

R. Yusupov

RAS Corr. Member, Dr. Sc. Tech., Professor, St. Petersburg, Russia

Editorial Board

V. Anisimov

Dr. Sc. Tech., Professor, St. Petersburg, Russia

B. Bezruchko

Dr. Sc. Phys.-Math., Saratov, Russia

N. Blaunstein

Dr. Sc. Phys.-Math., Professor, Beer-Sheva, Israel

A. Dudin

Dr. Sc. Tech., Professor, Minsk, Belarus

V. Khimenko

Dr. Sc. Tech., Professor, St. Petersburg, Russia

G. Maltsev

Dr. Sc. Tech., Professor, St. Petersburg, Russia

V. Melekhin

Dr. Sc. Tech., Professor, St. Petersburg, Russia

A. Shalyto

Dr. Sc. Tech., Professor, St. Petersburg, Russia

A. Shepeta

Dr. Sc. Tech., Professor, St. Petersburg, Russia

A. Smirnov

Dr. Sc. Tech., Professor, St. Petersburg, Russia

Z. Yuldashev

Dr. Sc. Tech., Professor, St. Petersburg, Russia

A. Zeifman

Dr. Sc. Phys.-Math., Vologda, Russia

Editor: A. Larionova**Proofreader:** T. Zvertanovskaia**Design:** A. Koleshko, M. Chernenko**Layout and composition:** N. Karavaeva**Contact information**

The Editorial and Publishing Center, SUAI

67, B. Morskaia, 190000, St. Petersburg, Russia

Website: <http://i-us.ru/en>, E-mail: ius.spb@gmail.com

Tel.: +7 - 812 494 70 02

The Journal was registered in the Ministry of Press, Broadcasting and Mass Media of the Russian Federation. Registration Certificate JD № 77-12412 from April, 19, 2002. Re-registration in the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (ROSKOMNADZOR) due to change of the founder: «Information and Control Systems», Ltd., JD № FS77-49181 from March, 30, 2012.

The journal is distributed by subscription. Subscription can be made in the Editorial and publishing center, SUAI as well as in any post office based on «Rospechat» catalogue: № 48060 — annual subscript, № 15385 — semiannual subscript.

© Corporate authors, 2014

INFORMATION AND CONTROL SYSTEMS

Viktorov D. S., Chislov S. G. Method of Correction of the Non-Linear Distortions Entered by an Analog Key in Probing Signals 2

Turubanov M. A., Shishlakov V. F., Shyshlakov A. V. Impulse Control System for Combined Solar and Wind Installation with Superconductor Equipment 8

Zakharova O. L., Kirsanova J. A., Kniga E. V., Zharinov I. O. Algorithms and Software of Testing Onboard Digital Computer Systems Integrated Modular Avionics 19

SYSTEM AND PROCESS MODELING

Kuchmin A. Yu. Modeling of Equivalent Stiffness of Adaptive Platforms with the Parallel Structure Executive Mechanism 30

HARDWARE AND SOFTWARE RESOURCES

Balonin N. A., Marley V. E., Sergeev M. B. New Opportunities of the Mathematical Network for Collaborative Research and Modeling in the Internet 40

Marakhovsky V. B. CMOS Implementation of the Trainee's Threshold Logical Element. Part I. Design and Training Diagram 47

Kolchin I. V., Filippov S. N. The Architecture of Bare-Metal Real-Time Microhypervisor and Automated Measurement of Time Response 57

Shoshmina I. V. A Methodology of Eliciting Context Requirements to Program Logic Control Systems 68

INFORMATION SECURITY

Bezzateev S. V., Voloshina N. V., Sankin P. S. Safety Analysis Methodology of Complex Systems Taking Into Account the Threats to Information Security 78

Boyko A. A., Djakova A. V. Method of Developing Test Remote Information-Technical Impacts on Spatially Distributed Systems of Information-Technical Tools 84

INFORMATION CODING AND TRANSMISSION

Cheprukov Yu. V., Socolov M. A. Correlation Characteristics and Application of Some Binary Codes 93

Alekseev M. O. On the Detection of Algebraic Manipulations by Means of Multiplication Operation 103

INFORMATION AND MEASURING SYSTEMS

Allakhverdiyeva N. R. Development of a Method for Improving the Accuracy of the Measuring Channel 109

INFORMATION INSTRUMENTATION AND EDUCATION

D'yachuk P. P., Loginov D. A., Karabalykov S. A. Synergetic Approach to Management of Educational Activity in Verbal Problem Environments 118

CONTROL IN MEDICAL AND BIOLOGICAL SYSTEMS

Tichonov E. P. Adaptive Filtering Algorithms Electrocardiogram High Time Resolution Part I. Background Information and Analysis Approach to Solving the Problem 125

CHRONICLES AND INFORMATION

IV International Forum «TELECOM NETWORKS 2.0. Sharing, Engineering, Outsourcing, Development & Metering» 132

INFORMATION ABOUT THE AUTHORS

134

Submitted for publication 07.04.14. Passed for printing 17.06.14. Format 60×84/8. Offset paper. Phototype SchoolBookC. Offset printing.

Layout original is made at the Editorial and Publishing Center, SUAI.
67, B. Morskaia, 190000, St. Petersburg, Russia
Printed from slides at the Editorial and Publishing Center, SUAI.
67, B. Morskaia, 190000, St. Petersburg, Russia

Учредитель
ООО «Информационно-управляющие системы»

Главный редактор
М. Б. Сергеев,
д-р техн. наук, проф., С.-Петербург, РФ

Зам. главного редактора
Е. А. Крук,
д-р техн. наук, проф., С.-Петербург, РФ

Ответственный секретарь
О. В. Муравцова

Редакционный совет:
Председатель А. А. Оводенко,
д-р техн. наук, проф., С.-Петербург, РФ
В. Н. Васильев,
чл.-корр. РАН, д-р техн. наук, проф., С.-Петербург, РФ
В. Н. Козлов,
д-р техн. наук, проф., С.-Петербург, РФ
К. Кристоделу,
д-р наук, проф., Альбукерке, Нью-Мексико, США
Б. Мейер,
д-р наук, проф., Цюрих, Швейцария
Ю. Ф. Подоплекин,
д-р техн. наук, проф., С.-Петербург, РФ
В. В. Симаков,
д-р техн. наук, проф., Москва, РФ
Л. Фортуна,
д-р наук, проф., Катания, Италия
А. Л. Фрадков,
д-р техн. наук, проф., С.-Петербург, РФ
Л. И. Чубраева,
чл.-корр. РАН, д-р техн. наук, С.-Петербург, РФ
Ю. И. Шокин,
акад. РАН, д-р физ.-мат. наук, проф., Новосибирск, РФ
Р. М. Юсупов,
чл.-корр. РАН, д-р техн. наук, проф., С.-Петербург, РФ

Редакционная коллегия:
В. Г. Анисимов,
д-р техн. наук, проф., С.-Петербург, РФ
Б. П. Безручко,
д-р физ.-мат. наук, проф., Саратов, РФ
Н. Блаунштейн,
д-р физ.-мат. наук, проф., Беэр-Шева, Израиль
А. Н. Дудин,
д-р физ.-мат. наук, проф., Минск, Беларусь
А. И. Зейфман,
д-р физ.-мат. наук, проф., Вологда, РФ
Г. Н. Мальцев,
д-р техн. наук, проф., С.-Петербург, РФ
В. Ф. Мелехин,
д-р техн. наук, проф., С.-Петербург, РФ
А. В. Смирнов,
д-р техн. наук, проф., С.-Петербург, РФ
В. И. Хименко,
д-р техн. наук, проф., С.-Петербург, РФ
А. А. Шалыто,
д-р техн. наук, проф., С.-Петербург, РФ
А. П. Шепета,
д-р техн. наук, проф., С.-Петербург, РФ
З. М. Юлдашев,
д-р техн. наук, проф., С.-Петербург, РФ

Редактор: А. Г. Ларионова
Корректор: Т. В. Звертановская
Дизайн: А. Н. Колешко, М. Л. Черненко
Компьютерная верстка: Н. Н. Караваева

Адрес редакции: 190000, Санкт-Петербург,
Б. Морская ул., д. 67, ГУАП, РИЦ
Тел.: (812) 494-70-02, e-mail: ius.spb@gmail.com, сайт: http://i-us.ru

Журнал зарегистрирован в Министерстве РФ по делам печати, телерадиовещания и средств массовых коммуникаций.
Свидетельство о регистрации ПИ № 77-12412 от 19 апреля 2002 г.
Перерегистрирован в Роскомнадзоре.
Свидетельство о регистрации ПИ № ФС77-49181 от 30 марта 2012 г.

Журнал входит в «Перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертации на соискание ученой степени доктора и кандидата наук».

Журнал распространяется по подписке. Подписку можно оформить через редакцию, а также в любом отделении связи по каталогу «Роспечать»: № 48060 — годовой индекс, № 15385 — полугодовой индекс.

© Коллектив авторов, 2014

ОБРАБОТКА ИНФОРМАЦИИ И УПРАВЛЕНИЕ

Викторов Д. С., Числов С. Г. Метод коррекции нелинейных искажений, вносимых аналоговым ключом в зондирующие сигналы 2

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

Турубанов М. А., Шишлаков В. Ф., Шишлаков А. В. Импульсная система управления комбинированной солнечно- и ветроэнергетической установкой со сверхпроводниковым оборудованием 8
Захарова О. Л., Кирсанова Ю. А., Книга Е. В., Жаринов И. О. Алгоритмы и программные средства тестирования бортовых цифровых вычислительных систем интегрированной модульной авионики 19

МОДЕЛИРОВАНИЕ СИСТЕМ И ПРОЦЕССОВ

Кучмин А. Ю. Моделирование эквивалентной жесткости адаптивных платформ с исполнительными механизмами параллельной структуры 30

ПРОГРАММНЫЕ И АППАРАТНЫЕ СРЕДСТВА

Балонин Н. А., Марлей В. Е., Сергеев М. Б. Новые возможности математической сети для коллективных исследований и моделирования в Интернете 40
Мараховский В. Б. КМОП-реализация обучаемого порогового логического элемента. Часть 1: Проектирование и схема обучения 47
Колчин И. В., Филиппов С. Н. Архитектура автономного микро-гипервизора реального времени и автоматизированное измерение его временных характеристик 57
Шошмина И. В. Методика составления контекстных требований к программным системам логического управления 68

ЗАЩИТА ИНФОРМАЦИИ

Беззатеев С. В., Волошина Н. В., Санкин П. С. Методика расчета надежности сложных систем, учитывающая угрозы информационной безопасности 78
Бойко А. А., Дьякова А. В. Способ разработки тестовых удаленных информационно-технических воздействий на пространственно распределенные системы информационно-технических средств 84

КОДИРОВАНИЕ И ПЕРЕДАЧА ИНФОРМАЦИИ

Чепруков Ю. В., Соколов М. А. Корреляционные характеристики и применение некоторых бинарных R3-кодов 93
Алексеев М. О. Об обнаружении алгебраических манипуляций с помощью операции умножения 103

ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ СИСТЕМЫ

Аллахвердиева Н. Р. Разработка метода повышения точности измерительного канала 109

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ОБРАЗОВАНИЕ

Дьячук П. П., Логинов Д. А., Карабалыков С. А. Синергетический подход к управлению учебной деятельностью в вербальных проблемных средах 118

УПРАВЛЕНИЕ В МЕДИЦИНЕ И БИОЛОГИИ

Тихонов Э. П. Адаптивные алгоритмы фильтрации и фрагментации электрокардиограмм высокого временного разрешения. Часть 1: Исходные сведения и анализ подхода к решению проблемы 125

ХРОНИКА И ИНФОРМАЦИЯ

IV Международный Форум «TELECOM NETWORKS 2.0. Sharing, Engineering, Outsourcing, Development & Metering» 132

СВЕДЕНИЯ ОБ АВТОРАХ

134

Сдано в набор 07.04.14. Подписано в печать 17.06.14. Формат 60×84/8. Бумага офсетная. Гарнитура SchoolBookC. Печать офсетная. Усл. печ. л. 16,0. Уч.-изд. л. 20,1. Тираж 1000 экз. Заказ 258.

Оригинал-макет изготовлен в редакционно-издательском центре ГУАП. 190000, Санкт-Петербург, Б. Морская ул., 67.

Отпечатано с готовых диапозитивов в редакционно-издательском центре ГУАП. 190000, Санкт-Петербург, Б. Морская ул., 67.

УДК 621.396:621.391.26

КОРРЕЛЯЦИОННЫЕ ХАРАКТЕРИСТИКИ И ПРИМЕНЕНИЕ НЕКОТОРЫХ БИНАРНЫХ R3-КОДОВ

Ю. В. Чепруков^а, канд. техн. наукМ. А. Соколов^б, доктор техн. наук, профессор^аРоссийский государственный университет туризма и сервиса, филиал, Сочи, РФ^бСанкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, РФ

Постановка проблемы: проведен обзор литературы и показано, что повышение эффективности различных систем возможно, если использовать более совершенные бинарные коды и ансамбли на их основе. Среди известных N элементных бинарных кодов, используемых в системах связи, радиолокации и управления, отсутствуют такие, которые позволяют получать достаточно низкий уровень боковых пиков автокорреляционной и взаимной корреляционной функций ансамблей кодов при изменении N в широких пределах. Целью работы является синтез N элементных бинарных кодов с заданными уровнями R и W боковых пиков автокорреляционной и взаимной корреляционной функций. **Метод:** метод решения задачи включает два этапа, изложена процедура построения различных по корреляционным характеристикам W -ансамблей. **Результаты:** приведены некоторые результаты синтеза кодов с $R = 3$ для $N \leq 32$, который позволил получить разнообразные коэффициенты сжатия. Синтезированы различные по корреляционным характеристикам W -ансамбли, содержащие от нескольких до сотен кодов, а также алфавиты передачи данных на их основе. Среди найденных кодов существует множество пар, для которых при сложении их корреляционных функций происходит компенсация боковых пиков. Найдены симметричные и асимметричные коды со специфическими свойствами. **Практическая значимость:** предложены варианты использования в системах управления, связи и радиолокации. Выдвинута идея разработки компьютеров на шумоподобных сигналах («тихий» компьютер) на основе стандартной системы кодирования ASCII с использованием ансамблей синтезированных кодов. Высказано предложение по осуществлению шифрования с помощью этих кодов. Системы связи и передачи данных на шумоподобных сигналах позволяют повысить информационную безопасность пользователей.

Ключевые слова — ансамбли, фазоманипулированные сигналы, бинарные коды, автокорреляционная функция, уровень боковых пиков, корреляционная функция.

Введение

В современных системах управления, связи и радиолокации широко используются шумоподобные сигналы (ШПС). Применение нашли как одиночные сигналы, так и ансамбли сигналов. Разновидностью ШПС являются фазоманипулированные сигналы (ФМС) [1], которые характеризуются бинарными кодовыми последовательностями или просто кодами.

В работе [1] упоминаются системы связи с кодовым разделением абонентов путем представления каждому из них индивидуального кода. Все сигналы передаются в одной полосе частот, может обеспечиваться скрытная связь на уровне шумов. Для реализации системы необходимы ансамбли сигналов. Примером такой системы может считаться система мобильной связи стандарта CDMA (Code Division Multiple Access — системы с кодовым разделением каналов). Для повышения помехоустойчивости мобильных станций в их кодах применяются ансамбли функций Уолша [2]. При приеме все сигналы разделяются блоком корреляторов. Выбор этих сигналов связан с их ортогональностью, а корреляционные свойства в данном случае не учитывались. Кроме того, в указанных системах применяются короткие и длинные псевдослучайные последовательности (ПСП), составляющие ансамбли огромного ко-

личества элементов. Короткие ПСП используются для расширения полосы и разделения сигналов от различных базовых станций, а длинные ПСП — для шифрования сообщений. В качестве указанных сигналов применяются ансамбли Голда и Касами [3]. Они относятся к производным ансамблям и получают из производных кодов путем расширения спектра посредством ПСП [1]. В указанных системах с этой целью используются M -последовательности.

Из данных по M -последовательностям [1] следует, что минимальное значение уровня боковых пиков (УБП) автокорреляционной функции (АКФ) равно $B_1 \approx (0,7...1,25) / \sqrt{N}$. Аналогичная величина взаимной корреляционной функции (ВКФ) составляет $B_2 \approx (1,4...5) / \sqrt{N}$, где N — длина кодовой последовательности.

В таблицу бинарных ансамблей (название, длина, объем и предельное значение УБП АКФ кодов), перспективных для использования в CDMA [4], включены ансамбли Голда, Касами, Камалетдинова и объединение Касами с бент-последовательностями. Важно, что параметр длины кода для всех указанных ансамблей принимает дискретные значения и велика разность между соседними допустимыми значениями длин (например, для кодов Голда это числа 7, 31, 63, ...). Отмечается, что объем ансамблей пропорционален либо линейной функции, либо корню

квадратному из длины кода N . Значение УБП АКФ кодов, представленных в таблице, приближенно соответствует $1/\sqrt{N}$.

Вопросы разработки системы навигации малого мобильного робота по трем маякам изложены в работе [5]. За каждым маяком закреплен номер (сигнатура из пяти символов). Чтобы повысить помехоустойчивость сигнала, передаваемого от маяков к инфракрасному приемнику робота, используется система кодирования канала. Выбрано кодирование сигнала M -последовательностью из 31 символа. Символ 1 сигнатуры маяка кодируется прямым кодом, символ 0 — инверсным. Учитывая, что координаты маяков известны роботу заранее, полученная от маяков информация позволяет вычислить угол между направлением ориентации робота и системой координат. По трем углам вычисляются искомые координаты робота.

В информатике и компьютерной технике используется система кодирования ASCII (American Standard Code for Information Interchange — стандартный код информационного обмена) [6]. В ней выделяется базовая (значения кодов изменяются от 0 до 127) и расширенная (от 128 до 255) системы. Каждый из 256 символов ASCII характеризуется комбинацией из восьми импульсов, составляющих байт.

Итак, объем ансамблей, которые могут использоваться в разнообразных системах, может изменяться от двух (для передачи только логических значений «1», «0») до 256 (в случае использования всей системы ASCII) сигналов. Промежуточные значения объемов могут соответствовать, например, количеству символов русского или латинского алфавитов либо числу 128 (для расширенной системы ASCII).

Результаты исследования бент-последовательностей для широкополосных систем с кодовым разделением каналов представлены в работе [7]. Предложенные алгоритм и программа на его основе позволяют сформировать образцы бент-последовательностей различной длины и исследовать их основные корреляционные характеристики. Метод основан на широко используемых различных копиях M -последовательностей. В представленных примерах кодов с $N = 4095$ УБП АКФ имеет большее значение, чем B_1 , но соответствует интервалу для B_2 .

В работе [8] в класс ШПС включены еще сигналы Хаффмена, Цирлера, Лежандра, Пэли — Плоткина, Фрэнка и максимальные линейные рекуррентные последовательности. При синтезе использовался математический аппарат полей Галуа. УБП АКФ всех сигналов приближенно характеризуется зависимостью $1/\sqrt{N}$.

В работе [9] дана таблица и построен график $R_{\min \max} = f(N)$ минимаксных значений УБП

АКФ кодов в зависимости от N , но сами коды и их количество для разных N не приведены. Примененный метод анализа основан на связи периодической и импульсной АКФ и обобщен в работе [10]. Там же представлен обзор важнейших работ по данной тематике.

В обширной монографии [11] обобщен огромный научный опыт разработки систем на ШПС («тихий» радиолокационных систем). В работе, в частности, дана классификация ансамблей бинарных последовательностей и методов синтеза, указаны проблемы применения известных методов. Например, при синтезе ансамблей кодов на основе полей Галуа разработчики сейчас опираются на материалы таблиц полиномов первой половины прошлого века.

В работе авторов [12] сформулирована задача синтеза кодов с УБП АКФ, равным R (R -коды), предложен метод решения. Представлены результаты синтеза, иллюстрирующие методику. Приведены некоторые коды с $R = 2, 3; N \leq 25$. Показаны существенные преимущества синтезированных кодов по сравнению с M -последовательностями.

В данной работе получены коды с $R = 3, N \leq 32$, проведен анализ их корреляционных характеристик, сформулированы предложения по применению полученных результатов. Эти коды удобно называть $R3$ -кодами, они позволяют оптимизировать выбор ФМС для систем управления, связи и радиолокации. Далее показано, что $R3$ -коды составляют множество со специфическими свойствами. Очевидно, что коды с $R = 1$ (коды Баркера) и коды с $R = 2$ ($R2$ -коды) составляют подмножества $R3$ -кодов.

Итак, анализ показал актуальность вопроса получения бинарных кодов для создания более совершенных одиночных ФМС и их ансамблей, что позволит повысить эффективность разнообразных систем, в которых они применяются.

Задача и методика синтеза, особенности решения

Назовем ФМС, АКФ которых в области боковых пиков может изменяться в пределах $\pm R$ ($0 \leq R \leq N - 1, R$ — целое), сигналами R -го рода (ФМС- R), а соответствующие им коды $G_{R,N}$ — R -кодами [12]. Обозначим $B_3 = R/N$ — относительную величину УБП АКФ этих кодов. Рассмотрим последовательность N импульсов одинаковой длительности T , начальная фаза которых равна 0 или π , которые составляют ФМС. Обозначим $\{G_{R,N}^i\}$ множество бинарных последовательностей (R -кодов) условных значений начальных фаз $P_j^i = \pm 1$ импульсов ФМС. Здесь P_j^i — коэффициенты последовательностей, причем j — номер элементов в любой из i различных последова-

тельностью, количество которых $g_{R,N}$ зависит от допустимого уровня R УБП АКФ и численности N последовательностей [12]. Поэтому имеем

$$\{G_{R,N}^i\} = \{P_j^i, j = \overline{1, N}\}, P_j^i = \pm 1, i = \overline{1, g_{R,N}}. \quad (1)$$

Из этого множества R -кодов можно составить ансамбли, у которых абсолютные значения ВКФ изменяются в пределах $\pm W$ ($1 \leq W \leq N - 1$, W — целое). Назовем их W -ансамблями. Цель работы — получить $R3$ -коды (найти $G_{3,N}$ и $g_{3,N}$) для $N \leq 32$, построить W -ансамбли, провести анализ характеристик, высказать предложения по применению.

Введем для R -кодов функции $S^*(t)$ и $S(t)$, которые определяют, соответственно, АКФ и модуль АКФ. В моменты $t_k = kT$, отсчитываемые от начала АКФ ($k = 0$), эти функции принимают экстремальные или нулевые значения, причем $S(t_N) = N$. Аналогично введем $V_{x,y}^*(t)$ и $V_{x,y}(t)$ для ВКФ и модуля ВКФ пар $R3$ -кодов с индексами x и y (пояснения даны ниже). Эти функции также будем рассматривать в моменты $t_k = kT$, отсчитываемые от начала ВКФ. Тогда задачу синтеза можно представить в виде системы неравенств относительно коэффициентов кодов [12]

$$S(t_k) = \left| \sum_{j=1}^k P_j^i \cdot P_{N+j-k}^i \right| \leq R; \quad k = \overline{1, N-1}, i = \overline{1, g_{3,N}}. \quad (2)$$

В результате решения получим $R3$ -коды, которые можно пронумеровать ($1 \dots g_{3,N}$) и объединить в множество $G_{3,N}$. Эти коды могут быть включены в W -ансамбль, если для совокупности пар

$R3$ -кодов с номерами (индексами) x, y ($x \neq y$) выполняются условия

$$V_{x,y}(t_k) = \left| \sum_{j=1}^k P_j^x \cdot P_{N+j-k}^y \right| \leq W; \quad k = \overline{1, 2N-1}. \quad (3)$$

Таким образом, задача синтеза (2), (3) решается в два этапа.

Этап 1: рассматривается система неравенств (2) и в соответствии с работой [12] определяются $R3$ -коды в количестве $g_{3,N}$, составляющие множество $G_{3,N}$. Перейдем к результатам, полученным на первом этапе.

Результаты синтеза $R3$ -кодов

Некоторые результаты синтеза $R3$ -кодов для $5 \leq N \leq 32$ (при $N < 5$ все бинарные последовательности являются $R3$ -кодами) представлены в табл. 1. Указаны лишь коды с первым коэффициентом (+1) (прямые коды). Имеются в том же количестве коды с противоположными знаками всех коэффициентов (инверсные коды). Корреляционные характеристики одинаковы. Прочерки во второй колонке означают, что для $N = 25 \dots 28$ общее количество $R3$ -кодов $g_{3,N}$ не определялось, даны лишь примеры. В третьей колонке указаны кодовые последовательности и половины их АКФ (в круглых скобках), так как они симметричны относительно максимума. Ниже представлены результаты вычислений, выполненных на общедоступном персональном компьютере, программы составлены на языке QBasic.

Анализ результатов синтеза $R3$ -кодов, приведенных в табл. 1, представлен ниже.

■ Таблица 1

N	$g_{3,N}$	$\{P_{i,j}\}; (S^*(t_k), k = 1 \dots N)$
5	14	1,1,1,1,-1; (-1,0,1,2,5). 1,1,-1,1,-1; (-1,0,1,-2,5)
6	28	1,1,1,-1,1,1; (1,2,1,0,1,6). 1,1,-1,1,1,1; (1,2,1,0,1,6)
7	42	1,1,1,-1,1,1,1; (1,2,3,0,1,2,7). 1,1,1,1,-1,1,1; (1,2,1,2,1,2,7)
8	74	1,1,1,1,-1,1,1,1; (1,2,3,2,1,2,3,8). 1,1,1,-1,1,1,1,1; (1,2,3,2,1,2,3,8)
9	120	1,1,1,-1,1,-1,1,1,1; (1,2,3,0,1,-2,3,0,9). 1,1,1,1,-1,1,-1,1,1; (1,2,1,2,-1,0,3,0,9)
10	202	1,1,1,-1,1,1,-1,1,1,1; (1,2,3,0,1,2,3,0,1,10). 1,1,1,-1,1,-1,-1,1,1,1; (1,2,3,0,-1,-2,-1,0,1,10)
11	232	1,1,1,1,-1,-1,1,-1,1,1,1; (1,2,3,2,1,-2,-3,0,1,2,11). 1,1,1,1,-1,1,-1,-1,1,1,1; (1,2,3,2,-1,0,-3,0,1,2,11)
12	412	1,1,1,1,1,-1,-1,1,-1,1,1,1; (1,2,3,2,3,0,-3,-2,1,2,3,12). 1,1,1,1,1,-1,1,-1,-1,1,1,1; (1,2,3,2,1,0,-1,-2,1,2,3,12)
13	532	1,1,1,1,-1,-1,1,-1,1,-1,1,1,1; (1,2,3,2,1,-2,-1,0,-1,-2,3,0,13). 1,1,1,1,-1,1,-1,1,-1,-1,1,1,1; (1,2,3,2,-1,0,-3,2,-1,-2,3,0,13)

■ Продолжение табл. 1

N	$g_{3,N}$	$\{P_{i,j}\}; (S^*(t_k), k = 1 \dots N)$
14	644	1, -1, 1, 1, 1, -1, -1, 1, -1, 1, 1, 1, 1; (1, 0, 1, 2, 3, 0, 3, -2, -1, 0, 1, 2, 1, 14). 1, 1, 1, 1, 1, 1, -1, -1, 1, -1, 1, 1, 1, -1; (-1, 0, 1, 2, 1, 2, 3, 0, -3, 0, 1, 2, 3, 14)
15	932	1, 1, -1, 1, 1, 1, -1, -1, 1, -1, 1, 1, 1, 1; (1, 2, 1, 2, 3, 2, 1, 2, -3, 0, 1, 2, 1, 2, 15). 1, 1, 1, 1, 1, 1, -1, -1, 1, -1, 1, 1, -1, 1; (1, 0, 1, 2, 1, 2, -1, 0, -3, -2, -3, 2, 3, 2, 15)
16	1484	1, 1, 1, 1, 1, 1, -1, -1, -1, 1, -1, 1, -1, 1, 1; (1, 2, 1, 2, 3, 2, 1, -2, -1, -2, -3, -2, 3, 2, 3, 16). 1, 1, -1, 1, 1, -1, 1, -1, -1, -1, 1, 1, 1, 1; (1, 2, 1, 2, 3, 2, 1, -2, -1, -2, -3, -2, 3, 2, 3, 16)
17	1234	1, 1, -1, -1, 1, 1, -1, -1, 1, -1, 1, 1, 1, 1, -1, 1; (1, 0, -1, 2, 3, 0, -1, 0, 1, -2, 1, -2, 3, 2, -3, 0, 17). 1, 1, -1, 1, 1, 1, 1, -1, -1, 1, -1, 1, 1, 1, -1, 1; (1, 0, -3, 2, 3, 0, -1, -2, 3, 2, 1, 2, -1, 0, -3, 0, 17)
18	1364	1, 1, 1, -1, 1, 1, 1, 1, 1, -1, -1, -1, 1, 1, -1, 1; (1, 0, 1, -2, 3, 0, 3, -2, -3, 0, 3, 2, 3, 0, -3, 2, 1, 18). 1, 1, 1, -1, 1, 1, 1, -1, -1, -1, 1, -1, 1, -1, 1, -1, 1; (1, 0, 1, -2, 3, 0, 3, -2, -1, 0, -1, -2, 3, 0, -3, 2, -3, 18)
19	1672	1, -1, -1, -1, -1, 1, 1, -1, 1, 1, -1, 1, 1, 1, -1, 1; (1, -2, 1, -2, 1, 2, -1, -2, -3, -2, 1, 0, 1, 2, -3, 2, 1, -2, 19). 1, -1, -1, 1, -1, 1, 1, 1, 1, 1, -1, 1, 1, 1, 1, -1, 1, -1, 1; (1, -2, -1, 2, 1, 2, -1, -2, -1, 0, -3, 0, 1, 2, 1, 0, 1, 2, 19)
20	2512	1, 1, 1, 1, 1, 1, -1, -1, 1, -1, 1, 1, 1, -1, 1, -1, 1, 1; (1, 2, 3, 2, 3, 2, 1, 0, 1, 2, -1, 0, 3, -2, -3, 2, 1, 2, 3, 20). 1, 1, 1, 1, 1, -1, 1, 1, -1, 1, -1, -1, -1, 1, 1, 1, -1, 1, 1; (1, 2, 3, 2, 3, 2, 3, 2, -3, -2, -3, 2, 1, 2, 1, 2, 3, 20)
21	2016	1, 1, 1, 1, 1, 1, -1, -1, 1, 1, -1, 1, -1, 1, -1, 1, 1; (1, 2, 3, 2, 3, 2, 1, -2, -3, 2, -1, 0, -1, 0, -1, 2, -1, 2, 3, 0, 21). 1, 1, 1, 1, 1, -1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, 1, -1, 1, 1; (1, 2, 3, 2, 3, 2, 1, 0, 3, 2, -1, 2, 1, 0, 3, 2, -1, 2, 3, 0, 21)
22	1512	1, 1, 1, 1, 1, -1, 1, 1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1; (1, 2, 3, 2, 3, 0, -1, 0, 3, -2, 1, 0, -1, 2, -1, 2, 3, 0, 3, 0, 1, 22). 1, 1, 1, 1, 1, -1, 1, 1, -1, 1, -1, 1, -1, 1, 1, -1, 1, 1; (1, 2, 3, 2, 3, 0, -1, -2, 1, -2, -1, 0, -3, 0, -1, 2, -1, 0, 3, 0, 1, 22)
23	2042	1, 1, 1, 1, 1, -1, 1, 1, -1, 1, -1, -1, 1, 1, 1, -1, -1, 1, 1; (1, 2, 3, 2, 3, 0, -1, -2, 1, -2, 1, 2, -3, 2, 1, 0, 3, 0, -3, 0, 1, 2, 23). 1, 1, 1, 1, 1, -1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, 1; (1, 2, 3, 2, 3, 0, -1, 0, 1, -2, -3, 2, -3, -2, -1, 0, -1, 0, -3, 2, 23). 1, 1, 1, 1, 1, -1, -1, 1, 1, 1, -1, -1, 1, -1, 1, -1, 1, -1, 1, 1; (1, 2, 3, 2, 3, 0, -1, -2, 1, 2, 1, -2, -3, 2, 1, 0, 3, 0, -3, 0, 1, 2, 23)
24	3432	1, 1, 1, 1, 1, 1, -1, -1, 1, -1, 1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1; (1, 2, 3, 2, 3, 2, 1, -2, -1, 2, 1, 0, 3, -2, 1, -2, 3, 2, -3, 2, 1, 2, -1, 24). 1, 1, 1, 1, 1, 1, -1, -1, 1, 1, 1, 1, -1, -1, 1, -1, 1, -1, 1, 1, 1; (1, 2, 3, 2, 3, 2, 1, -2, -3, 2, 1, 0, -1, -2, 3, 2, -1, 2, 1, -2, 1, 2, 3, 24)
25	—	1, 1, 1, 1, 1, -1, 1, 1, -1, 1, -1, -1, 1, 1, 1, -1, 1, -1, -1, 1, 1, -1, 1; (1, 0, 1, 2, 3, 0, 3, -2, -3, 0, -1, 2, 3, -2, 1, 0, 3, 2, 1, -2, -1, 0, 1, 0, 25). 1, 1, 1, 1, -1, 1, 1, 1, 1, -1, -1, -1, 1, -1, 1, 1, 1, -1, -1, 1, 1, -1, 1; (1, 0, 1, 2, -1, 2, -1, 0, 3, 2, -1, -2, -1, -2, -1, -2, -3, 2, -1, 2, -1, 0, 1, 0, 25)
26	—	1, 1, 1, 1, 1, -1, 1, -1, 1, -1, -1, 1, 1, 1, 1, -1, -1, 1, 1, -1, 1, 1, 1; (1, 2, 3, 2, 3, 2, 1, -2, 3, -2, 1, 2, 3, 0, -3, 0, 3, 0, -3, 0, -1, 0, 3, 0, 1, 26). 1, 1, 1, 1, 1, -1, -1, 1, 1, 1, 1, -1, 1, -1, 1, -1, -1, 1, 1, -1, 1, 1, 1; (1, 2, 3, 2, 3, 2, -1, -2, 3, 2, -3, 0, 3, -2, 1, 0, -1, 0, 3, 0, -1, 0, 3, 0, 1, 26)
27	—	1, 1, 1, 1, 1, -1, -1, 1, -1, 1, 1, -1, -1, 1, -1, 1, -1, 1, -1, 1, 1, 1, 1; (1, 2, 3, 2, 3, 2, 1, 0, 1, 2, -3, 0, -3, 2, -1, 2, -3, -2, -1, 2, 1, 0, 1, 0, 1, -2, 27). 1, 1, 1, 1, 1, 1, -1, 1, -1, -1, 1, -1, 1, 1, -1, 1, -1, -1, 1, 1, 1, -1, 1, 1; (1, 2, 3, 2, 1, 2, 1, 2, -1, 0, -1, -2, 1, 2, 1, 0, -1, 0, -3, -2, 1, 2, -3, 0, 1, 2, 27)
28	—	1, 1, 1, 1, 1, 1, 1, -1, 1, 1, 1, -1, -1, 1, -1, 1, 1, 1, -1, 1, -1, 1, 1, 1; (1, 2, 3, 2, 3, 2, 1, 0, -3, -2, 3, 2, -1, 2, 1, -2, 1, -2, 3, 0, -1, -2, -3, 2, 1, 2, 3, 28). 1, 1, 1, 1, 1, 1, -1, 1, 1, -1, -1, 1, 1, 1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1; (1, 2, 3, 2, 3, 2, 1, -2, -1, 2, -1, -2, 1, 2, 3, -2, 1, 2, 1, 2, 3, -2, -3, -2, -3, 2, 3, 28)
29	1122	1, 1, 1, 1, 1, 1, -1, -1, 1, 1, 1, -1, -1, 1, -1, 1, 1, -1, 1, 1, -1, 1, 1, 1; (1, 2, 3, 2, 3, 2, -1, -2, -1, 2, 3, 2, 3, 0, -3, 2, -1, 2, -1, 2, 3, 2, -1, 2, -1, 2, -1, 0, 29). 1, 1, 1, 1, 1, -1, 1, -1, 1, -1, 1, -1, 1, 1, -1, -1, 1, 1, 1, -1, 1, 1, -1, 1, 1; (1, 2, 3, 2, 3, 2, -1, -2, 3, 2, 3, 0, 3, -2, -1, -2, 1, 2, -1, 2, 3, -2, 3, -2, 3, 0, 29)

■ Окончание табл. 1

N	$g_{3,N}$	$\{P_{i,j}\}; (S^*(t_k), k = 1...N)$
30	344	$1,1,-1,1,1,1,1,-1,1,1,-1,-1,1,1,-1,1,-1,-1,1,1,-1,1,-1,1,-1,1,1,1;$ $(1,2,-1,0,3,0,3,-2,1,0,1,0,-1,-2,-1,0,-1,2,1,-2,1,0,-1,-2,-1,2,3,0,-3,30).$ $1,1,-1,1,1,1,1,-1,1,1,1,-1,-1,-1,-1,1,-1,-1,1,1,1,1,-1,-1,-1,1,-1,1,1;$ $(1,2,-1,0,3,-2,1,0,1,2,-3,0,1,-2,-3,0,-3,2,1,0,-3,-2,-3,0,3,-2,-1,0,1,30)$
31	1004	$1,1,1,1,-1,-1,1,-1,1,1,1,-1,1,1,-1,1,-1,-1,-1,1,1,-1,-1,1,1,-1,1,1,1;$ $(1,2,3,2,1,0,1,2,1,-2,3,0,3,-2,-1,0,-3,0,3,0,-3,2,-3,-2,-1,2,1,0,-3,2,31).$ $1,1,1,1,-1,-1,1,1,1,-1,-1,1,-1,1,1,-1,-1,1,-1,1,1,1,1,-1,1,-1,1,1,1;$ $(1,2,3,2,1,-2,-1,2,3,2,1,2,3,-2,-3,-2,1,0,-3,2,-3,0,1,0,1,2,-3,0,1,-2,31).$ $1,1,1,1,-1,-1,1,-1,-1,-1,-1,1,1,-1,-1,1,1,-1,-1,1,-1,1,1,1,-1,1,-1,1,1,1;$ $(1,2,3,2,1,-2,-1,2,1,0,1,-2,1,-2,-3,-2,-3,2,-3,-2,3,2,-3,0,-3,2,1,0,-3,2,31)$
32	1688	$1,-1,-1,-1,1,1,1,-1,-1,1,-1,-1,1,1,-1,1,-1,-1,1,1,1,1,1,1,1,1,1,-1;$ $(-1,2,1,0,-3,-2,-1,2,1,-2,-1,2,-3,2,-1,-2,1,2,-1,-2,-3,-2,3,-2,1,2,3,0,3,2,1,32).$ $1,-1,-1,-1,1,1,1,-1,1,1,-1,1,1,1,-1,1,1,-1,-1,-1,1,-1,-1,1,1,1,1,1,-1;$ $(-1,2,1,0,-3,-2,-3,2,3,2,3,-2,3,2,3,-2,1,2,1,-2,1,-2,-3,-2,-1,-2,-1,0,3,-2,1,32)$

Синтез W -ансамблей R -кодов

Перейдем к следующему этапу синтеза.

Этап 2: среди синтезированных на первом этапе кодов множества $G_{R,N}$ (см. табл. 1) ищутся совокупности пар кодов, удовлетворяющие неравенствам (3) и составляющие W -ансамбли. Иначе говоря, коды W -ансамблей должны соответствовать требованиям, предъявляемым к ВКФ всех пар кодов. Кратко методика сводится к тому, что среди всех возможных пар кодов из $G_{R,N}$ находятся такие, для которых УБП ВКФ имеет наибольшее значение. Этих пар может быть несколько. Из элементов $G_{R,N}$ составляется два подмножества (условно $M1$ и $M2$), в которых отсутствуют номера одного или другого кода той пары, для которой УБП ВКФ имеет наибольшее значение. Теперь УБП ВКФ кодов указанных подмножеств уменьшается, так как пары «разбиты» (коды разведены в подмножества $M1$ или $M2$). Если пар кодов с наибольшим значением УБП ВКФ несколько, то каждое подмножество $M1, M2$ разделяется повторно до получения необходимых W -ансамблей.

Применим этот способ для R -кодов при фиксированных R, N . Для упрощения индексации заменим $G_{R,N}$ на $G0$. Выполняются следующие пошаговые операции.

Шаг 1. Из $g_{R,N}$ кодов составляются всевозможные пары (s, u) ($s \neq u$) (s, u — индексы R -кодов из $G0$), количество которых $P0 = g_{R,N}(g_{R,N} - 1)/2$. Вычисляются УБП ВКФ каждой пары и находится наибольшее значение, которое обозначим V_m . Удобно здесь же определить множество пар $p1$ индексов кодов $((s1, u1), \dots, (s_{p1}, u_{p1}))$, для которых УБП ВКФ равно V_m , хотя эти значения используются далее. Множество $G0$ соответствует единственному ($A_0 = 1$) $W = V_m$ -ансамблю.

Шаг 2. Множество $G0$ разделяется на два подмножества из $(g_{R,N} - 1)$ элементов. Первое полу-

чается после удаления кода с индексом $s1$ (обозначим $G1(s1)$), а второе — в результате удаления $u1$ (запишем $G1(\hat{u}1)$) (номера удаленных кодов отмечаются знаком $\hat{}$). Цифра в обозначении множества $G1$ соответствует первой операции удаления символов из исходного множества $G0$. Теперь для обоих множеств значение УБП ВКФ меньше V_m и если $p1 = 1$ (лишь одна пара), то надо перейти к следующему шагу. Если $p1 > 1$, то из каждого множества вновь поочередно удаляются коды второй пары и получаются множества $G1(\hat{s}1, \hat{s}2), G1(\hat{s}1, \hat{u}2)$ и $G1(\hat{u}1, \hat{s}2), G1(\hat{u}1, \hat{u}2)$. Процедура аналогично проводится и для других пар. В результате получаются множества, которые обозначим $G1^*(i), i = (1...A_1)$. Для дальнейшего использования (на шаге 3) для всех $G1^*(i)$ составляются пары входящих в них кодов и вычисляются УБП ВКФ этих пар. Среди них определяется наибольшее значение, одновременно удобно найти соответствующее множество пар $p2$ кодов с этим наибольшим значением. Пусть следующее по порядку убывания значение УБП ВКФ есть V_{m-1} (это не арифметическое вычитание, а следующее по убыванию значение, которое может быть меньше более чем на единицу). Таким образом, после первых удалений множества $G1^*(i)$ являются $W = V_{m-1}$ -ансамблями, количество которых A_1 . Отметим особенности. Некоторые из ансамблей могут состоять из кодов, для которых все пары имеют УБП ВКФ меньше V_{m-1} , поэтому для них на этом шаге удаления не производятся, они не делятся. Возможны пары, которые различаются одним индексом (например, $(s1, u1), (s1, u2)$), тогда после удаления получится не четыре, а два ансамбля (один без кода номер $s1$, а другой — без кодов $(u1, u2)$). То есть в общем случае размер W -ансамблей $A_1 \leq 2^{p1}$.

Шаг 3. Для всех множеств $G1^*(i)$, полученных на шаге 2, вновь выполняются те же операции: производятся вторые удаления и формируются

2. Ранее указывалось, что символам ASCII ставится в соответствие одна из 256 возможных восьми импульсных комбинаций, теперь каждому символу можно поставить в соответствие один из R3-кодов. Необходимо использовать $W = 21$ -ансамбль, включающий 289 кодов. Из него можно взять любые 256 кодов. Количество вариантов, отличающихся хотя бы одним кодом, определяется числом сочетаний C_{289}^{256} . Для каждого варианта имеется $256!$ расстановок кодов по символам ASCII, т. е. общее количество разнообразных алфавитов равно $A_{256} = C_{289}^{256} \cdot 256!$. При практическом применении необходимо выбрать несколько критериев различия и отбирать меньшее число алфавитов A_{256}^* . Если для алфавита достаточно 128 кодов, то можно использовать коды $W = 18$ -ансамбля. В случае, когда W недостаточно мало, нужно аналогичным образом рассмотреть задачу синтеза для $N > 30$.

3. Существуют симметричные и асимметричные R-коды.

Симметричность. Код $\{P_j^{(1)}\}$ является симметричным, если $P_j^{(1)} = P_{N+1-j}^{(1)}, j = \overline{1, N}$, $(1, -1, 1)$ — симметричный код.

Асимметричность. Код $\{P_j^{(2)}\}$ является асимметричным, если $P_j^{(2)} = -P_{N+1-j}^{(2)}, j = \overline{1, N}$, $(1, 1, -1)$ — асимметричный код.

R3-коды с одним или обоими указанными свойствами симметричности и асимметричности существуют для разных N в количестве от одного до четырех. Так, для $N = 10$ имеется по одному коду с указанными свойствами, для $N = 11$ — по два симметричных и четыре асимметричных, а если $N = 13$, то имеется четыре асимметричных кода. Вот примеры симметричных кодов: $(1, 1, 1, -1, 1, 1, -1, 1, 1, 1)$ — $N = 10$; $(1, 1, 1, -1, -1, 1, -1, -1, 1, 1, 1)$ — $N = 11$ (вертикальная линия симметрии проводится между пятым и шестым и по шестому элементу кодов соответственно). Асимметричные коды: $(1, -1, 1, 1, 1, 1, -1, -1, -1, 1, -1)$ — $N = 10$; $(1, 1, 1, -1, 1, 1, -1, 1, -1, -1, -1)$ и $(1, 1, 1, -1, 1, -1, -1, -1, -1, -1, -1)$ — $N = 11$; $(1, 1, 1, -1, 1, -1, 1, 1, -1, -1, -1)$ и $(1, 1, 1, -1, 1, -1, -1, -1, -1, -1, -1)$ — $N = 13$. Приведенные для $N = 11, 13$ асимметричные коды различаются лишь знаками центральных коэффициентов. АКФ кодов равны; например, для $N = 13$ половина АКФ приведенной пары кодов имеет вид $(-1, -2, -3, 0, -1, 2, -1, 2, -3, 0, 3, -2, 13)$. Получено, что R3-кодов с указанными свойствами симметричности и асимметричности для $14 \leq N \leq 24$ и $29 \leq N \leq 32$ не существует, а прочие значения ($N = 25 \dots 28, N > 32$) не рассматривались. Среди R3-кодов табл. 1 симметричные существуют для $N = (5 \dots 11)$, а асимметричные — при $N = (5 \dots 11); 13$.

4. Установлено, что при $N = (5 \dots 8)$ существует множество R3-кодов, УБП ВКФ которых так же, как и АКФ, равно трем, а при $N = 5$ имеются R3-коды с более низким значением, равным двум.

Особо отметим существование при $N = 6$ пары симметричного $(1, -1, 1, 1, -1, 1)$ и асимметричного $(1, 1, 1, -1, -1, -1)$ R3-кодов со сверхнизким, равным единице, УБП ВКФ. Сама ВКФ V^* имеет вид $(-1, 0, -1, 0, -1, 0, 1, 0, 1, 0, 1)$. Интересно, что эта функция асимметрична относительно центрального (шестого) значения. Важно отметить равенство нулю этого значения, что означает ортогональность пары R3-кодов.

5. Перед анализом следующих результатов рассмотрим неравенство, в котором S_0 — полусумма АКФ $S_x^*(t)$ и $S_y^*(t)$ двух R-кодов. Назовем пары R-кодов, суммарные (объединенные) АКФ которых в области боковых пиков изменяются в пределах $\pm U$ ($0 \leq U \leq N - 1, U$ — целое), U -кодами. То есть в области боковых пиков $S_0 = (S_x^*(t) + S_y^*(t))/2 \leq U$, где x, y ($x \neq y$) — номера (индексы) R-кодов из $G_{R, N}$ (полусумма берется для нормировки к единице). Например, при $U = 0$ АКФ таких пар R-кодов в области боковых пиков полностью взаимно компенсируются, а значения сигналов главных пиков складываются. При $U = 1$ происходит частичная компенсация и суммарные боковые пики равны $(0; \pm 1)$. Будем называть такие R-коды $U0$ - и $U1$ -кодами соответственно и обозначать $RU0$ и $RU1$. $RU0$ -коды составляют дополнительные последовательности [1], используемые для построения производных систем сигналов. В данной работе найдены коды с указанными свойствами из множества R3-кодов, т. е. рассмотрены R3U0- и R3U1-коды соответственно. Результаты приведены в табл. 3.

Видно, что возможности выбора кодов велики, однако для $N = 30, 31$ кодов с $U = 0; 1$ не существует, имеются коды с $U = 2$, которые не рассматриваются. Среди R3U1-кодов при $N \leq 32$ наибольшее значение равно $N = 32$. Ниже даны примеры R3U0-кодов и симметричные половины их АКФ.

■ Таблица 3

N	U	$k_{3, N, U}$	N	U	$k_{3, N, U}$
5	1	62	17	1	3596
6	1	160	18	1	10 888
7	1	290	19	1	2548
8	0	24	20	0	40
	1	724		1	7720
9	1	1012	21	1	2460
10	1	2360	22	1	4256
11	1	1973	23	1	1512
12	1	4512	24	1	2024
13	1	5273	29	1	25
14	1	10 688	30	0; 1	0
15	1	8192	31	0; 1	0
16	0	148	32	1	24
	1	17 412			

При $N = 8$ (1,1,1,-1,1,-1,1,1; 1,1,1,-1,-1,1,-1,-1) — $R3$ -коды; (1,2,1,0,-1,2,-1,8) и (-1,-2,-1,0,1,-2,1,8) — индивидуальные АКФ; (0,0,...,0,0,8) — объединенная АКФ. Отметим, что при $N = 8$ среди 24 пар $U0$ -кодов имеется 8 пар $R2$ -кодов, составляющих, как отмечалось, подмножество $R3$ -кодов. При $N = 20$ (1,1,-1,1,1,1,1,1,-1,-1,1,1,-1,1,-1,-1,1,1; 1,1,-1,1,1,1,1,1,-1,-1,-1,1,-1,1,-1,1,-1,-1) — $R3$ -коды; (1,2,-1,-2,3,2,-1,2,-3,0,-1,2,1,2,1,2,1,-2,-1,20) и (-1,-2,1,2,-3,-2,1,-2,3,0,1,-2,-1,-2,-1,-2,-1,2,1,20) — их АКФ; (0,0,0,...,0,0,0,20) — результирующая АКФ.

Пример $R3U1$ -кодов при $N = 29$: (1,1,-1,1,1,1,1,-1,1,1,-1,1,-1,-1,-1,1,-1,-1,-1,1,1,-1,1,-1,-1,-1,1,1,-1,-1,-1,1,1,-1,-1,-1,-1,-1) — $R3$ -коды; (1,0,-3,0,1,0,-3,0,1,0,-3,0,1,0,-3,0,-3,0,-3,0,-3,0,1,0,1,0,1,0,29) и (1,0,1,2,1,2,1,2,1,0,1,0,-1,0,1,0,1,2,3,2,1,0,1,2,1,0,-1,-2,29) — частные АКФ; (1,0,-1,1,1,1,-1,1,1,0,-1,0,0,0,-1,0,-1,1,0,1,-1,0,1,1,1,0,0,-1,29) — полусумма частных АКФ, так что УБП равен $1/29$ (можно получить $1/32$ для $N = 32$). Кроме того, при $N = 8$ имеется восемь пар кодов лишь с одним ненулевым значением в середине области боковых пиков, они очень близки к $R3U0$ -кодам. То есть существует множество $R3$ -кодов с полной или частичной компенсацией боковых пиков суммарной АКФ этих кодов.

Применение

1. Пользователи средств вычислительной техники получают возможность выбора алфавита представления своих рабочих данных. Например, можно выбрать один из A_{256}^* алфавитов и передать его номер доверенным получателям, которые достоверно примут переданные данные. Прочие пользователи, даже зная все коды ансамбля, смогут принять сигналы, но они в совокупности не будут соответствовать переданным данным. Реализации способа шифрования путем выбора варианта алфавита из множества A_{256}^* наряду с применением известных достоинств ШПС [1] затруднит несанкционированный доступ к передаваемым данным. Назовем этот способ шифрования короткими R -кодами, в отличие от использования длинных ПСП [2, 3]. Однако могут возникнуть проблемы технической реализации быстродействующих систем при большом количестве алфавитов.

2. Возможности построения алфавитов передачи, соответствующих стандарту ASCII, позволяют высказать идею создания систем передачи данных и вычислительных систем, в том числе компьютеров на ШПС («тихий» компьютеров). Они станут обладать всеми известными достоинствами этих сигналов. В них возможно снижение опасности «заражения» вирусными программа-

ми благодаря скрытной работе. Это предполагает введение наряду с существующим каналом передачи параллельного канала для представления данных посредством $R3$ -кодов. Оба канала объединяются на выходе системы, и сигналы передаются на линию передачи. Оценим производительность. Каждый код алфавита соответствует по длине байту, поэтому если $TN = 8T_6$, где T_6 — длительность бита, то $T = T_6/(N/8)$, т. е. для обеспечения той же побайтной скорости необходимо использовать более короткие импульсы в $R3$ -кодах, что означает расширение полосы частот канала для их передачи в $N/8$ раз. Общая производительность системы из двух каналов удвоится. Если $T = T_6$, то полоса частот канала не расширяется, но длительность $R3$ -кодов будет в $N/8$ раз больше и побайтовая скорость уменьшится в $N/8$, так что производительность всей системы возрастет до $(1 + 8/N)$. Для $N = 32$ увеличение потенциально составит 25 %.

3. Передача от отправителя к получателям в компьютерных сетях осуществляется пакетами и обеспечивается согласно протоколу IP. В работе [6] указана структура IP-пакета, состоящего из заголовка и поля данных. Заголовок имеет поля, не все из которых кратны байту, а часто состоят из нескольких бит, а алфавиты, построенные на W -ансамблях, соответствуют байтам. Следовательно, потребуются согласования форматов и корректировки представления служебной информации IP-пакетов. Эти же принципы могут распространиться на локальные и глобальные компьютерные сети с возможностью создания «тихого» Интернета, что актуально в условиях несанкционированного доступа к электронной персональной информации. Вероятно, что, как и в системах CDMA, здесь потребуются регулирование мощности сигналов отправителей.

4. Посредством кодов W -ансамблей можно реализовать скрытное управление группой летательных аппаратов (например, беспилотных) или роботов («тихое» управление).

5. В медицинских внутриполостных системах управления и контроля использование ансамблей ШПС потенциально позволяет применить большое количество независимых датчиков с низкими уровнями сигналов, без возможной негативной интерференции с сигналами нервной системы.

6. Совершенствование бинарных кодов для построения ФМС- R перспективно для радиолокационных систем [13]. При обзоре пространства узким лучом антенны в каждом угловом направлении излучается конечное число импульсов, составляющих пачку. Обработка пачки позволяет увеличить выходное отношение сигнал/шум, реализовать доплеровские методы обнаружения

движущихся целей на фоне пассивных помех. Актуально использование излучения пачек из ШПС, например $R3U0$ - и $R3U1$ -кодов, что позволит улучшить функционирование систем, повысить качество выделения сигналов на фоне помех.

Для формирования и согласованной фильтрации часто удобно воспользоваться устройствами на поверхностных акустических волнах, применяемыми в системах мобильной связи [2, 3]. Возможно использование также конструкции на микроэлектронных элементах [14]. Существенное снижение УБП АКФ достижимо путем применения весовой обработки [15].

Заключение

Повышение эффективности современных систем возможно при использовании более совершенных бинарных кодов и основанных на них

сигналов. Сформулирована задача синтеза бинарных $R3$ -кодов и W -ансамблей из этих кодов. Приведены результаты синтеза, демонстрирующие широкие возможности выбора кодов с различными N . Получены симметричные и асимметричные коды, представлены их характеристики. Изложена методика синтеза W -ансамблей, приведены примеры. Показано, что имеется множество пар кодов, при сложении АКФ которых осуществляется полная или частичная компенсация их боковых пиков. Введены RU -коды, представлены результаты расчетов. Обоснована перспективность развития методов синтеза бинарных $R3$ -кодов для их применения в компьютерной технике и системах управления (для построения множества алфавитов для передачи данных), в связи (применение более совершенных кодов и ансамблей), в радиолокации (для улучшения характеристик обнаружения целей на фоне пассивных помех).

Литература

1. Варакин Л. Е. Системы связи с шумоподобными сигналами. — М.: Радио и связь, 1985. — 384 с.
2. Карташевский В. Г., Семенов С. Н., Фирстова Т. В. Сети подвижной связи. — М.: ЭКО-ТРЕНДЗ, 2001. — 302 с.
3. Ипатов В. П., Орлов В. К., Самойлов И. М., Смирнов В. Н. Системы мобильной связи: учеб. пособие для вузов / под ред. В. П. Ипатова. — М.: Горячая линия-Телеком, 2003. — 272 с.
4. Ipatov V. P. Spread Spectrum and CDMA. Principles and Applications. — N. Y., John Wiley and Sons Ltd., 2004. — 373 p.
5. Карпов В. Э., Платонова М. В. Система навигации мобильного робота // Информационные средства и технологии: тр. 18-й Междунар. науч.-техн. конф. Москва, 19–21 октября 2010 г. Т. 2. С. 56–63.
6. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. — СПб.: Питер, 2002. — 672 с.
7. Юдачев С. С. Последовательности на основе бент-функций для широкополосных систем с кодовым разделением каналов // Инженерный вестник. МГТУ им. Н. Э. Баумана. 2013. № 1. С. 1–11.
8. Амиантов И. А. Избранные вопросы статистической теории связи. — М.: Сов. радио, 1971. — 416 с.
9. Пелехатый М. И., Голубев Е. А. Автокорреляционные свойства некоторых типов двоичных последовательностей // Проблемы передачи информации. 1972. Т. VIII. Вып. 1. С. 92–99.
10. Сврдлик М. Б. Оптимальные дискретные сигналы. — М.: Сов. радио, 1975. — 200 с.
11. Гантмахер В. Е., Быстров Н. Е., Чеботарев Д. В. Шумоподобные сигналы. Анализ, синтез, обработка. — СПб.: Наука и Техника, 2005. — 400 с.
12. Чепруков Ю. В., Соколов М. А. Синтез фазоманипулированных сигналов с требуемым уровнем боковых пиков АКФ // Радиотехника. 1991. № 5. С. 68–70.
13. Чапурский В. В. Избранные задачи теории сверхширокополосных радиолокационных систем. — М.: МГТУ им. Н. Э. Баумана, 2012. — 279 с.
14. А. с. 1709498 СССР, МКИЗ Н03 Н 15/02, 17/00. Согласованный фильтр / Ю. В. Чепруков, М. А. Соколов (СССР). — № 1709498; заявл. 06.12.1989; опубл. 30.01.92, Бюл. № 4. — 4 с.
15. Чепруков Ю. В., Соколов М. А. Метод оптимизации весовых фильтров сжатия фазоманипулированных сигналов // Изв. вузов. Радиоэлектроника. 1991. № 4. С. 31–37.

UDC 621.396:621.391.26

Correlation Characteristics and Application of Some Binary Codes

Cheprukov Yu. V.^a, PhD, Tech., chuv52@mail.ruSocolov M. A.^b, Dr. Sc., Tech., Professor, guap22@mail.ru^aRussian State University of Tourism and Service, 24/a, Kirpichnaia St., 354340, Sochi, Russian Federation^bSaint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaya, 190000, Saint-Petersburg, Russian Federation

Purpose: There has been reviewed technical literature and it has been shown that it is possible to increase efficiency of different systems using updated binary codes and ensembles based on them. Among the known N elementary binary codes applied in communication, radar and control systems there are no such codes which allow achieving a relatively low level of side peaks of autocorrelation and cross-correlation functions of code ensembles at changing N in wide limits. The purpose of the paper is to synthesize N elementary binary codes with the given levels R and W of side peaks of autocorrelation and cross-correlation functions. **Method:** A method of the problem solution consists of two steps. There has been stated a method of creation of W -ensembles with different correlation characteristics. **Results:** There have been envisaged some results of synthesis of codes with $R = 3$ for $N \leq 32$ allowing to obtain various compression coefficients. There have been synthesized W -ensembles with different correlation characteristics containing from several units to hundreds of codes as well as alphabets for data transfer based on them. The obtained codes include many couples for which compensation of side peaks occurs when adding their correlation functions. There have been found symmetric and asymmetric codes with specific properties. **Practical relevance:** The improved binary codes can be applied in control, radar and communication systems. There has been put forward an idea of developing computers operating with noise-like signals ("quiet" computers) based on the standard coding systems ASCII using ensembles of synthesized codes. There has been proposed to carry out encryption using these codes. **Social implications:** Communication systems and data transmission based on noise-like signals will increase information security of users.

Keywords – Ensembles, Phase-Shift Signals, Binary Codes, Autocorrelation Function, Side Peak Level, Correlation Function.

References

1. Varakin L. E. *Sistemy svyazi s shumopodobnymi signalami* [Communication Systems with Noise Signals]. Moscow, Radio i svyaz' Publ., 1985. 384 p. (In Russian).
2. Kartashevskii V. G., Semenov S. N., Firstova T. V. *Seti podvizhnoi svyazi* [Networks of Mobile Communication]. Moscow, JeKO-TRENDZ Publ., 2001. 302 p. (In Russian).
3. Ipatov V. P., Orlov V. K., Samoilov I. M., Smirnov V. N. *Sistemy mobil'noi svyazi*. V. P. Ipatov ed. [Mobile Communication Systems]. Moscow, Goriachaia liniia-Telekom Publ., 2003. 272 p. (In Russian).
4. Ipatov V. P. *Spread Spectrum and CDMA. Principles and Applications*. New York, John Wiley and Sons Ltd., 2004. 373 p.
5. Karpov V. Je., Platonova M. V. System of Mobile Robot Navigation. *Trudy XVIII Mezhdunarodnoi nauchno-tehnicheskoi konferencii "Informacionnye sredstva i tehnologii"* [Proc. XVIII Int. Conf. "Informational Facilities and Technologies"]. Moscow, Izdatel'skii dom MJeI Publ., 2010, vol. 2, pp. 56–63 (In Russian).
6. Olifer V. G., Olifer N. A. *Komp'yuternye seti. Principy, tehnologii, protokoly* [Computer Networks. Principles, Technologies, Reports]. Saint-Petersburg, Piter Publ., 2002. 672 p. (In Russian).
7. Judachev S. S. Sequences on the Basis of Bent-Functions for Broadband Systems with Code Division of Channels. *Inzhenernyi vestnik*. Moscow, MG TU im. N. Er. Bauman Publ., 2013, no. 1, pp. 1–11 (In Russian).
8. Amiantov I. A. *Izbrannye voprosy statisticheskoi teorii svyazi* [Chosen Questions of the Statistical Theory of Communication]. Moscow, Sovetskoe radio Publ., 1971. 416 p. (In Russian).
9. Pelehatyi M. I., Golubev E. A. Autocorrelation Characteristics of Some Types of Double Sequences. *Problemy peredachi informacii*, 1972, vol. VIII, no. 1, pp. 92–99 (In Russian).
10. Sverdlik M. B. *Optimal'nye diskretnye signaly* [Optimum Discrete Signals]. Moscow, Sovetskoe radio Publ., 1975. 200 p. (In Russian).
11. Gantmaher V. E., Bystrov N. E., Chebotarev D. V. *Shumopodobnye signaly. Analiz, sintez, obrabotka* [Pseudonoise Signals. Analysis, Synthesis, and Processing]. Saint-Petersburg, Nauka i Tehnika Publ., 2005. 400 p. (In Russian).
12. Cheprukov Ju. V., Socolov M. A. Synthesis of Phasemanipulated Signals with Required Level of Side Peaks ACF. *Radiotekhnika*, 1991, no. 5, pp. 68–70 (In Russian).
13. Chapurskii V. V. *Izbrannye zadachi teorii sverhshirokopolosnykh radiolokacionnykh sistem* [Selected Problems of Theory of Super Wide-Band Radiolocation Systems]. Moscow, MG TU im. N. Er. Bauman Publ., 2012. 279 p. (In Russian).
14. Cheprukov Ju. V., Socolov M. A. *Soglasovannyi fil'tr* [Matched Filter]. Author's certificate USSA, no. 1709498, 1992.
15. Cheprukov Ju. V., Socolov M. A. Method of Optimization of Weight Compression Filters of Phasemanipulated Signals. *Izvestiya vuzov. Radioelektronika*, 1991, no. 4, pp. 31–37 (In Russian).