

**ՀՀ ԿՐԹՈՒԹՅԱՆ ԵՎ ԳԻՏՈՒԹՅԱՆ ՆԱԽԱՐԱՐՈՒԹՅՈՒՆ
ՀԱՅԱՍՏԱՆԻ ԱԶԳԱՅԻՆ ՊՈԼԻՏԵԽՆԻԿԱԿԱՆ ՀԱՄԱԼՍԱՐԱՆ**

ԳՈՍՑՑԱՆ ՀՈՎՀԱՆՆԵՍ ԱՎԱԳԻ

**ԻՆՖՈՐՄԱՑԻԱՅԻ ՄՇԱԿՄԱՆ ԹՎԱՅԻՆ ՀԱՄԱԿԱՐԳԵՐՈՒՄ
ԿԱՄԿԱՂԱՅԻՆ ԿՈՂԱՎՈՐՈՂ ԿԱՌՈՒՑՎԱԾՔՆԵՐԻ ԵՎ
ՍՈՂՈՒԼՑԱՑԻԱՅԻ ՍՈՂԵԼՆԵՐ ԵՎ ՄԵԹՈԴՆԵՐ**

Ե.12.03 «Հեռահաղորդակցական ցանցեր, սարքավորումներ և
համակարգեր» մասնագիտությամբ տեխնիկական գիտությունների
դոկտորի գիտական աստիճանի հայցման ատենախոսության

Ս Ե Ղ Մ Ա Գ Ի Ր

Ե Ր Ե Վ Ա Ն 2016

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ АРМЕНИЯ
НАЦИОНАЛЬНЫЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ АРМЕНИИ**

ГОМЦЯН ОГАНЕС АВАКОВИЧ

**МОДЕЛИ И МЕТОДЫ КАСКАДНЫХ КОДИРУЮЩИХ КОНСТРУКЦИЙ И
МОДУЛЯЦИИ В ЦИФРОВЫХ СИСТЕМАХ ОБРАБОТКИ ИНФОРМАЦИИ**

А В Т О Р Е Ф Е Р А Т

диссертации на соискание ученой степени доктора
технических наук по специальности
05.12.03 – “Сети, устройства и системы телекоммуникаций”

Ե Ր Ե Վ Ա Ն 2016

Ատենախոսության թեման հաստատվել է Հայաստանի ազգային
պոլիտեխնիկական համալսարանում:

Գիտական խորհրդատու՝

Ֆ.-մ.գ.դ. Ա.Գ.Ղուլյան

Պաշտոնական ընդդիմախոսներ՝

տ.գ.դ. Վ.Հ.Ավետիսյան

տ.գ.դ. Ա.Վ.Իսախանյան

Ֆ.-մ.գ.դ. Խ.Վ.Ներկարարյան

Առաջատար կազմակերպություն՝

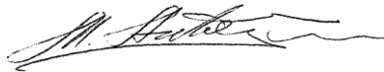
ՀՀ ԳԱԱ Ռադիոֆիզիկայի և
Էլեկտրոնիկայի ինստիտուտ

Պաշտպանությունը կայանալու է 2016թ. դեկտեմբերի 16-ին, ժամը 14⁰⁰-ին Հայաստանի
ազգային պոլիտեխնիկական համալսարանում գործող 046 “Ռադիոտեխնիկա և
Էլեկտրոնիկա” մասնագիտական խորհրդի նիստում (հասցեն՝ 0009, Երևան, Տերյան
փ., 105, 17-րդ մասնաշենք):

Ատենախոսությանը կարելի է ծանոթանալ ՀԱՊՀ գրադարանում:

Սեղմագիրն առաքված է 2016թ. նոյեմբերի 16 -ին:

046 մասնագիտական խորհրդի
գիտական քարտուղար, տ.գ.թ.



Մ.Յ. Այվազյան

Тема диссертации утверждена в Национальном политехническом университете Армении.

Научный консультант:

д.ф.-м.н. А.Г. Гулян

Официальные оппоненты:

д.т.н. В.Г.Аветисян

д.т.н. А.В.Ипатов

д.ф.-м.н. Х.В.Неркарян

Ведущая организация:

Институт радиофизики и электроники
НАН РА.

Защита диссертации состоится 16 декабря 2016г. в 14⁰⁰ на заседании
Специализированного совета 046 “Радиотехника и электроника”, действующего при
Национальном политехническом университете Армении (НПУА), по адресу: 0009, г.
Ереван, ул. Теряна 105, корпус 17.

С диссертацией можно ознакомиться в библиотеке НПУА .

Автореферат разослан 16 ноября 2016г.

Ученый секретарь Специализированного
совета 046, к.т.н.



М.Ը.Այվազյան

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. В современных цифровых системах обработки информации широкое применение нашли различные методы кодирования. В общем случае при кодировании осуществляется преобразование одной цифровой информации в другую как в передатчике, так и в приемнике. Такие преобразования обычно преследуют различные цели, например, устранение избыточности, содержащейся в информации, или специальное введение избыточности при помехоустойчивом кодировании, или шифрование информации и т.д. Современные системы передачи информации трудно представить без помехоустойчивого кодирования, позволяющего эффективно бороться с цифровыми ошибками, возникающими в линии связи. С другой стороны, известно, что повышение эффективности помехоустойчивых кодов может быть достигнуто увеличением длины кода, что приводит к резкому возрастанию сложности кода и, особенно, алгоритмов декодирования, т.е. практическая реализация длинных кодов затруднительна. Для решения этой проблемы были разработаны так называемые коды-произведения или итеративные коды и далее каскадные коды. При этом результирующий код произвольной размерности формируется при помощи последовательных преобразований произвольного количества соответствующих образующих (составляющих, компонентных) кодов.

Первые каскадные коды были предложены Форни в 1966 г. С тех пор теория и практика каскадного кодирования развиты многими исследователями, а работы в этом направлении продолжаются и по сей день.

Известные преимущества цифровых систем, методов и алгоритмов обработки информации выдвигают на первый план способы защиты данных от несанкционированного доступа и улучшения помехоустойчивости с использованием современных кодовых схем. Эти две основные задачи породили большое количество решений и приложений, начиная с простейших кодов до современных сложных турбоконструкций и др. В дополнительном исследовании нуждаются также методы цифровой модуляции и их использование совместно с каскадными кодами. Помехоустойчивое кодирование в сочетании с перемежением, аналого-цифровым преобразованием и удачными кодами передачи является эффективным средством для повышения качества записи и передачи информации по различным каналам. Шифрование и сжатие представляют дополнительную защиту каналов связи от несанкционированного доступа.

Таким образом, различное сочетание вышеуказанных схем и конструкций является мощным инструментом обработки информации в цифровых системах. В связи с этим исследование различных методов цифровой модуляции и каналов связи, а также разработка новых кодовых конструкций, совместно применяемых в современных цифровых системах обработки информации, является актуальным.

Цель и задачи работы. Целью диссертации является разработка и исследование сложной кодирующей системы, включающей шесть уровней кодирования, модуляцию и канал связи.

Исходя из намеченной цели, в работе были поставлены и решены следующие задачи:

1. Провести сравнительный анализ существующих каскадных кодирующих схем и методов цифровой модуляции в общей системе обработки информации.

2. Предложить новую каскадную кодовую конструкцию, включающую такие компоненты, как аналого-цифровой преобразователь, вокодер, шифратор, кодер Рида-Соломона (РС), перемежитель и кодер передачи.

3. Разработать методику цифрового моделирования систем связи с линейной и адаптивной дельта-модуляцией (ЛДМ и АДМ) с оценкой погрешностей формирования сигналов и шумов.

4. Исследовать вероятностные характеристики цифрового сигнала, а также искажения в системах с ЛДМ и АДМ.

5. Разработать методику машинной оптимизации систем связи с дельта-модуляцией (ДМ) на основе методов уменьшения дисперсии.

6. Проанализировать основные характеристики и свойства таких важных математических моделей теории кодирования, как группы, кольца и поля.

7. Изучить особенности, способы построения и технической реализации систематических и несистематических циклических кодов (ЦК).

8. Разработать структуры кодера и декодера Рида-Соломона (RS).

9. Развить алгоритм проверки правильности декодирования кодов РС.

10. Математически описать и разработать схему умножителя в конечном поле.

11. Исследовать различные типы перемежителей, вокодеров, шифраторов и кодов передачи, которые являются компонентами предложенной новой кодующей конструкции.

12. Разработать модели сложной схемы, состоящей из цифрового модулятора, канала связи и шести уровней кодирования.

13. Исследовать характеристики отдельных составляющих и предложенной кодовой конструкции, а также сложной схемы в целом.

Научная новизна. В процессе исследований получены следующие научные результаты:

1. Предложена новая схема построения каскадного кода, которая существенно отличается от классической каскадной конструкции тем, что в качестве кодера источника впервые использована ДМ, а в качестве кодера канала - кодер РС.

2. Впервые предложена новая конструкция: внешний кодер - помехоустойчивый кодер - перемежитель.

3. Разработаны методика, алгоритмы и программы цифрового моделирования систем с ДМ, которые позволили изучить три вида дельта-модуляции.

4. Решены задачи, которые не поддаются обычным методам исследований, в частности, получены распределения пачек символов ДМ сигнала, а также корреляционные функции (КФ) аппроксимирующего и цифрового сигналов.

5. Выведены уравнения для расчета цифровых фильтров нижних частот (ФНЧ) Баттерворта первого и второго порядков, по которым можно синтезировать указанные фильтры любого порядка с переменными частотами дискретизации и среза.

6. Произведена оценка точности цифрового моделирования сигналов в системах с ДМ. Получены соотношения между объемом выборки при моделировании и результирующей точностью воспроизведения основных статистических характеристик сигналов.

7. Осуществлена машинная оптимизация системы с ДМ с применением способов уменьшения дисперсии и различных методов оптимизации.

8. Показано, что различные математические формы представления ЦК соответствуют прямым и инверсным кодам.

9. Показаны этапы технической реализации ЦК.

10. Предложена обобщенная структурная схема декодера Рид-Соломона.

11. Показано, что для проверки безошибочного декодирования кодов РС можно использовать процедуру деления принятого кодового полинома на генераторный.

12. Выведены уравнения для комбинированного умножителя в поле $GF(2^8)$, на основе которых разработана его принципиальная схема.

13. По предложенной конструкции создана новая компьютерная модель каскадной кодирующей системы, с помощью которой подробно исследованы как каскадная кодовая схема, так и методы модуляции и каналы связи.

Практическая ценность работы. Практическая ценность работы заключается в том, что с одной стороны, отдельные результаты исследований и моделирования по ДМ, циклическим кодам и кодам РС могут иметь самостоятельное практическое применение в плане разработанных схем и алгоритмов; с другой стороны - предложенная модель каскадной кодирующей системы дает возможность значительно снизить сложность кодирования-декодирования по сравнению с системами, использующими длинные коды, а следовательно, и стоимость реализации систем. Многие теоретические формулировки и выкладки обоснованы и подтверждены многочисленными примерами и моделированием, позволяющими также судить об их практической ценности.

Основные результаты диссертации были использованы и внедрены в различных хозяйственных и госбюджетных работах, а также в учебном процессе ВЗЭИС - МТУСИ и ЕрПИ-ГИУА-НПУА.

Основные положения, выносимые на защиту:

1. Предложенная новая каскадная схема кодирования, где в качестве внешнего кодера использована ДМ, а в качестве внутреннего - кодер РС, а также несколько типов перемежителей, включенных не после внешнего кодера, а после внутреннего позволила значительно улучшить характеристики системы.

2. Точность цифрового моделирования сигналов в системах с ДМ влияет на погрешность моделирования всей системы в целом.

3. Необходимый объем выборки при моделировании различных систем с ДМ зависит от вида передаваемой информации и точности оценок таких основных статистических характеристик случайных процессов (СП), как математическое ожидание, дисперсия и корреляционная функция.

4. Полученные соотношения для моделирования цифровых ФНЧ Баттерворта позволили синтезировать фильтры, варьируя такими параметрами, как частоты дискретизации и среза.

5. Выбор метода машинной оптимизации влияет на результаты исследований систем связи с ДМ. При оптимизации со случайной целевой функцией целесообразность применения того или иного метода оценивается на основе тщательного анализа сведений о ее характере.

6. Разработанные методики, алгоритмы, программы, а также полученные результаты цифрового моделирования различных систем с ДМ в сочетании с машинной оптимизацией и способами уменьшения дисперсии являются

эффективным методом исследований, дополняющим аналитические и экспериментальные методы.

7. Доказательство представления ЦК в двух формах: прямой и инверсной.

8. Методы и этапы построения циклических кодеров и их техническая реализация.

9. Алгоритмы и схема декодирования кодов РС, которые позволили произвести расчеты очень сложного декодера.

10. Метод проверки безошибочного декодирования недвоичных кодов РС, основанный на анализе остатка от деления принятого кодового слова (КС) на генераторное кодовое слово.

11. Разработанная принципиальная схема умножителя в конечном поле - самого сложного узла кодера-декодера РС - на основе выведенных уравнений более простая, чем известные аналогичные схемы.

12. Сопоставительный анализ различных кодов передачи, применяемых в цифровых системах обработки информации.

13. Разработка компьютерной модели каскадной схемы при работе в канале с аддитивным белым гауссовским шумом (АГБШ) и двумя видами цифровой модуляции.

14. Результаты моделирования предложенной схемы, включающей кодовую конструкцию, а также линию связи и методы цифровой модуляции, показали ее эффективность.

Апробация результатов. Основные результаты исследований представлены на: заседаниях научно-технического семинара “Машинные методы исследования и проектирования радиотехнических систем, радиоэлектронных цепей и систем связи” (М., 1976, 1977, 1981, 1982 гг.); III симпозиуме по совершенствованию систем связи с цифровыми методами модуляции (Л., 1979 г.); 33 Всесоюзной сессии НТОРЭС им. А.С. Попова (М., 1978 г.); республиканских НТК, посвященных дню радио (Ташкент, 1987 г.; Тбилиси, 1978, 1979 гг.); Всесоюзной НТК “Информационные методы повышения эффективности и качества систем связи и радиоэлектроники” (М., 1981г.); 6-ой Всесоюзной школе-семинаре “Распараллеливание обработки информации” (Львов, 1987 г.); 7-ой межрегиональной конференции “Обработка сигналов в системах двусторонней телефонной связи” (М., 1997 г.); 2-ом международном черноморском симпозиуме (Греция, 2000 г.); 5-ой международной конференции ISTON 2003 (Польша, 2003 г.); 10-й 11-ой и 13-й Международной научно-практической конференции “Современные информационные и электронные технологии” (Одесса, 2009, 2010 и 2012 гг.); 8-й научной конференции Российско-Армянского (Славянского) Университета (Ереван, 2014 г.); научных семинарах факультета Радиотехники и Систем Связи ГИУА-НПУА (1998-2016 гг.).

Публикации. По теме диссертации опубликовано 29 работ, список которых приведен в конце автореферата.

Структура и объем диссертации. Работа состоит из введения, пяти глав, основных выводов, списка литературы из 180 наименований и приложений. Основной объем состоит из 274 страниц без приложений, включая 24 таблицы, 107 рисунков. Диссертация написана на русском языке.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы, сформулированы цель и задачи работы, поставлены научная новизна и практическая ценность, приведены основные положения, выносимые на защиту, а также дано краткое содержание диссертации.

В первой главе проведен сравнительный анализ некоторых методов помехоустойчивого кодирования на основе обзора соответствующей научной литературы и расчетов с помощью пакета MATLAB R2008. Кроме того, осуществлен обзор и анализ существующих каскадных кодирующих конструкций.

В современных информационных технологиях одной из наиболее актуальных проблем является защита информации от искажений и ошибок. В кабельных и беспроводных линиях связи действуют преднамеренные и непреднамеренные помехи различной физической природы, которые искажают форму сигналов, что приводит к неоднозначному распознаванию информации на приемной стороне. Для систем и устройств хранения информации, например, в случае магнитных и оптических носителей опасны разного рода механические (физические) воздействия, в частности, царапины на компакт-диске или другие дефекты, которые выводят из строя отдельные участки этих устройств.

Мощным инструментом коррекции этих ошибок являются помехоустойчивые коды, которые хорошо освещены в большом количестве публикаций. В последние годы разработаны еще более эффективные методы, системы, алгоритмы устранения ошибок, к которым можно отнести каскадные коды, комбинации различных кодов, турбокоды и такие кодовые конструкции, как пороговые декодеры, алгоритм декодирования Витерби, коды Боуза-Чоудхури-Хоквингема (БЧХ), коды РС, коды-произведения, а также разработки последнего десятилетия: многопороговые декодеры (МПД) и коды с низкой плотностью проверок на четность (LDPC).

Для преодоления вышеуказанных проблем вначале были разработаны так называемые коды-произведения или итеративные коды и далее каскадные коды.

В двухкаскадной (двухступенчатой, двухуровневой) схеме кодирования-декодирования, впервые предложенной Форни и уже ставшей классической, в качестве внешнего кода предлагается всегда использовать корректирующий код РС, а в качестве внутреннего - рассмотрены как сверточный помехоустойчивый код, так и код БЧХ. В современной интерпретации внешний кодер часто называется кодером источника, а внутренний кодер - кодером канала.

Следующей модификацией этой схемы является включение перемежителя между кодерами источника и канала, как это показано на рис. 1. Перемежитель обеспечивает преобразование пачек цифровых ошибок в одиночные. Как видно из рисунка 1, кодовые слова на выходе предыдущего каскада используются как входные информационные символы для следующего каскада и т.д. Поскольку каждый кодер – это отдельное устройство, то в результате удается упростить техническую реализацию каждого более короткого кода по сравнению с однокаскадным кодированием, конечно, при большей длине общего кода.

Разработанная схема. Следует отметить, что в многочисленных работах, посвященных каскадным кодирующим конструкциям, почти нет сведений о структуре кодеров источника и канала, что приводит к трудностям в вопросе анализа и разработки систем обработки информации. В диссертации разработана и

предложена наиболее развернутая и полная модель методов каскадного кодирования и модуляции, показанная на рис. 2 [13,14,17-20,26].

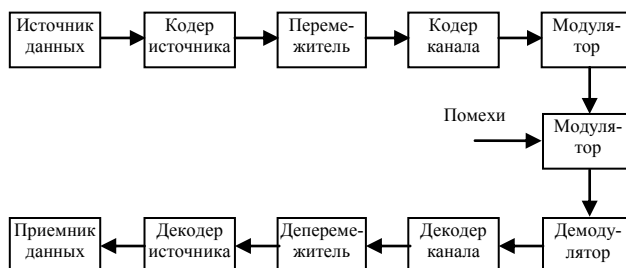


Рис. 1. Модификация классической каскадной конструкции

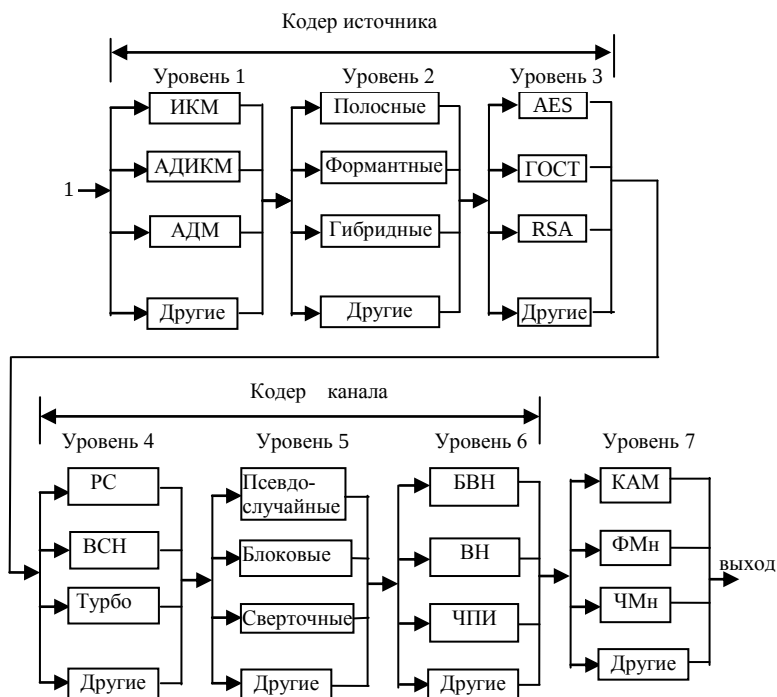


Рис. 2. Обобщенная модель каскадного кодирования и методов модуляции

Здесь источник сообщений 1 вырабатывает мультимедийную информацию (речь, музыка, изображение, текст и т.п.), которая далее преобразуется в цифровой формат на уровне 1 с помощью аналого-цифрового преобразователя (АЦП). Наиболее распространенные виды АЦП – это импульсно-кодовая модуляция (ИКМ) со скоростью 64 кбит/с, адаптивная дифференциальная ИКМ (АДИКМ) со скоростью 32 кбит/с, адаптивная дельта-модуляция и дельта-сигма-модуляция (ДСМ) со скоростью 16...32 кбит/с. Для понижения этих скоростей до значений 3...8 кбит/с на уровне 2 можно использовать вокодеры и гибридные кодеры. Классическими видами вокодеров являются формантные, полосные, ортогональные. Однако в последние годы появились и применяются вокодеры с линейным предсказанием типа LPC (Linear Predictive Coding) и др. Лучшие результаты в смысле качества передаваемой информации обеспечивают современные гибридные кодеры, такие как ACELP (Algebraic Code-Excited Linear Prediction), LTP-LPC (Long-Term Prediction-LPC), RPE-LPC (Regular Pulse Excitation-LPC) и др.

Дальнейшим этапом преобразования может служить шифрование с целью защиты системы от несанкционированного доступа, осуществляемое на уровне 3. Существует множество стандартов и алгоритмов шифрования, среди которых можно выделить AES (Advanced Encryption Standard), RSA (Rivest, Shamir, Adleman), ГОСТ 28147-89 (Россия) и др.

Уровни 1,2,3 могут быть объединены в кодер источника.

Кодер канала представлен также в виде трех уровней: помехоустойчивое кодирование, перемежение (интерливинг-interleaving) и линейное кодирование (коды передачи). Цифровые ошибки исправляются на уровне 4 с помощью таких корректирующих кодов, как Рида-Соломона, БЧХ, Турбо и др.

Часто ошибки, возникающие в линии связи, группируются в пакеты, и поэтому для их преобразования в одиночные используется перемежение на уровне 5. Последовательное соединение корректирующего кодера и перемежителя является эффективной системой для устранения пакетов ошибок.

На уровне 6 осуществляется линейное кодирование, при котором удастся решить такие проблемы, как согласование характеристик цифрового сигнала с линией связи, передача информации о синхросигнале и др. Существуют различные форматы линейных кодов такие, как без возврата к нулю (БВН), с возвратом к нулю (ВН), манчестерские, с чередованием полярности импульсов (ЧПИ) и многие другие.

Последним этапом преобразования (уровень 7) является модуляция, с помощью которой осуществляется переход в область радиочастот. Здесь могут использоваться квадратурная амплитудная модуляция (КАМ-QAM), фазовая манипуляция (ФМн-PSK), частотная манипуляция (ЧМн-FSK) и др.

Итак, разнообразие методов и алгоритмов на всех уровнях разработанной каскадной конструкции требует дополнительных исследований отдельных ее составляющих, направленных на повышение эффективности современных систем обработки информации, что и осуществлено в последующих главах диссертации.

Во второй главе исследованы характеристики одной из компонент каскадной кодирующей системы, а именно, - дельта-модуляции. Дельта-модуляция является своеобразным согласующим элементом между аналоговым источником (потребителем) информации и импульсным трактом передачи – радиорелейная линия,

кабельная линия, спутниковая сеть и т.д. Поэтому было предложено большое число разновидностей ДМ применительно к конкретным приложениям [3,4,11,12].

Универсальным методом исследований может служить цифровое (компьютерное) моделирование, не требующее предварительного макетирования системы. Кроме того, цифровое моделирование, являясь как бы компромиссом между аналитическим и экспериментальными методами, не только позволяет исследовать работу системы, но и дает возможность имитировать различные дефекты, которые могут иметь место в реальных системах, а также воспроизводить результаты исследований различных авторов [2].

Обобщенная схема моделирования, которая применима для различных типов и параметров входного сигнала, вида и характеристик ДМ, типа и характеристик цифрового тракта связи с помехами или без них, представлена на рис. 3.

Как известно, схема самого дельта-модулятора состоит из следующих основных функциональных узлов: дискретизатора по времени и квантователя по амплитуде, которые охвачены петлей обратной связи с предсказателем, а также сравнивающего устройства [1,2]. Следовательно, цифровая модель должна содержать модели этих узлов и входного сигнала. Кроме того, в общую модель системы передачи информации с ДМ входят ФНЧ (на рис.3 не показаны), модель канала связи (с помехами или без помех) и модель демодулятора.

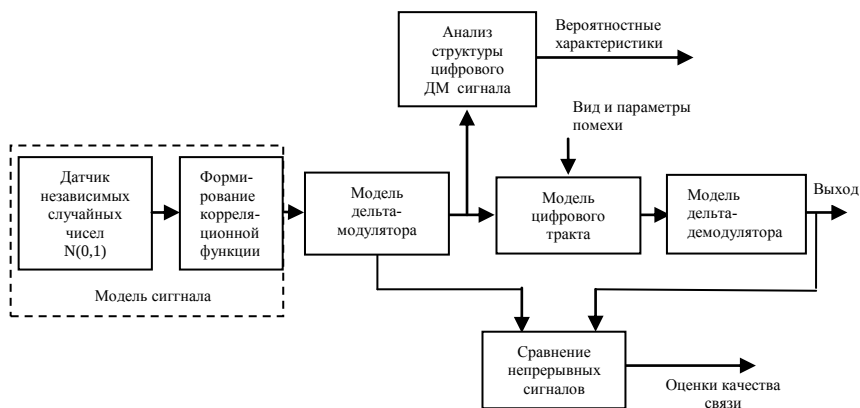


Рис. 3. Обобщенная схема моделирования систем с ДМ

Модели входных сигналов. Для гауссовских стационарных случайных процессов разработаны эффективные алгоритмы преобразования последовательности $U(n)$ независимых распределенных по гауссовскому закону случайных чисел с нулевым средним ($m=0$) и единичной дисперсией ($\sigma^2 = 1$) в последовательность $S(n)$ с

заданными корреляционно-спектральными характеристиками. Одно из таких экономичных преобразований, описываемое рекуррентно-разностными уравнениями, имеет вид [2,7]

$$S(n) = \gamma \sum_{k=0}^r \alpha_k U(n-k) - \sum_{l=1}^m \beta_l S(n-l), \quad (1)$$

где α_k, β_l - коэффициенты, определяемые по заданному закону корреляции на подготовительном этапе моделирования; γ - масштабный коэффициент, обычно равный единице.

Модель речевого сигнала. Достаточно простая и пригодная для практики модель речевого сигнала представляет собой стационарный случайный процесс с корреляционной функцией, определяемой следующим выражением [9]:

$$B_s(\tau) = \sigma^2 \cdot e^{-\omega_c |\tau|} \cdot \cos \omega_0 \tau, \quad (2)$$

где σ^2 - дисперсия сигнала, а величины $\omega_c \approx 10^3 \cdot c^{-1}$, $\omega_0 \approx 2.5 \cdot 10^3 \cdot c^{-1}$.

С целью получения рекуррентного алгоритма для моделирования случайного процесса с такой КФ упростим выражение (1), положив $\gamma = 1$; $\alpha_k = 0$ при $k = \overline{2, r}$, а

$\beta_l = 0$ при $l = \overline{3, m}$. Тогда получим следующее соотношение для моделирования речевого сигнала [1,2]:

$$S(n) = \alpha_0 U(n) + \alpha_1 U(n-1) - \beta_1 S(n-1) - \beta_2 S(n-2), \quad (3)$$

причем, коэффициенты α_k, β_k можно определить из [2].

Модель телевизионного сигнала. Для получения модели телевизионного сигнала сделаем дальнейшее упрощение выражения (1), положив $\alpha_k = 0$ при $k = \overline{1, r}$, а $\beta_k = 0$ при $l = \overline{2, m}$. Тогда получим модель входного сигнала, которая описывается следующим уравнением:

$$S(n) = \alpha_0 U(n) - \beta_1 S(n-1). \quad (4)$$

Следует отметить, что уравнение (4) является простой и достаточно точной моделью телевизионного (ТВ) сигнала, корреляционную функцию которого можно аппроксимировать следующим выражением [2,9]:

$$B_s(\tau) = \sigma^2 \cdot e^{-\omega_c |\tau|}, \quad (5)$$

где σ^2 - дисперсия сигнала, а $\omega_c \approx (250...410) \cdot 10^3 \text{ c}^{-1}$.

При моделировании систем связи с ДМ возникает необходимость цифровой фильтрации последовательностей на входе модулятора и выходе демодулятора. Известные способы расчета цифровых ФНЧ предполагают фиксированными частоты дискретизации и среза. На практике же при исследованиях часто необходимо варьировать этими параметрами. В этом случае, например, для синтеза ФНЧ Баттерворта второго порядка можно воспользоваться следующими полученными соотношениями:

$$C(n) = \alpha_0 S(n) + \alpha_1 S(n-1) + \alpha_2 S(n-2) - \beta_1 C(n-1) + \beta_2 C(n-2), \quad (6)$$

где S_n - отсчеты воздействия на входе фильтра; C_n - отсчеты выходного сигнала;
 $\alpha_0 = \alpha_2 = \omega_a^2 / \gamma_1$; $\alpha_1 = 2\alpha_0$; $\beta_1 = \frac{2(\omega_a^2 - 1)}{\gamma_1}$; $\beta_2 = \frac{1 - \omega_a \gamma + \omega_a^2}{\gamma_1}$; $\gamma_1 = 1 + \sqrt{2\omega_a + \omega_a^2}$;

$\omega_a = \text{tg} \frac{\omega_m T_0}{2} = \text{tg} \frac{f_m \pi}{f_0}$ - частота среза аналогового фильтра; ω_m - требуемая частота среза ЦФ; $f_0 = 1/T_0$ - частота дискретизации ЦФ [5].

При этом переход от исходного аналогового ФНЧ Баттерворта осуществлен методом билинейного преобразования.

Таким образом, изменяя f_m и f_0 , можно непосредственно рассчитать коэффициенты α_k , β_k , а значит, и синтезировать фильтры с желаемой полосой пропускания и частотой дискретизации.

Аналогичные соотношения для фильтров первого порядка и примеры расчетов порядков различных фильтров приведены в [5].

Как уже отмечалось, в цифровую модель системы связи с ДМ, кроме рассмотренных выше моделей сигналов и ФНЧ, входят также и модели модулятора и демодулятора, для которых в диссертации получены алгоритмы, использованные при моделировании [2].

Функциональную схему модулятора ДМ можно рассматривать, как замкнутую импульсную систему с существенно нелинейным элементом - квантователем на два уровня, для моделирования которой также получены рекуррентные соотношения [1].

Из (1) видно, что методы формирования входных случайных процессов основаны на идее преобразования исходных (базовых) последовательностей в производные. В качестве базовых обычно выбирают последовательности равномерно распределенных случайных чисел $R(0,1)$ на интервале $[0,1]$. Производные последовательности с желаемым распределением далее получаются в результате линейных или нелинейных биекционных преобразований [6].

Как формирование последовательности $R(0,1)$, так и последующие преобразования сопровождаются некоторыми ошибками, которые в дальнейшем могут накапливаться. Для оценки точности этих преобразований рассматривается следующая цепь преобразований: генерация последовательности $a \in R(0,1)$; формирование последовательности независимых гауссовских случайных чисел $U \in N(0,1)$; цифровой фильтр с дискретной передаточной функцией $K(Z)$, который формирует сигнал S на входе системы с нулевым средним значением и заданной КФ $B_s(\tau)$ или в дискретном варианте $B_s(n)$.

Пусть $a \in R(0,1)$ имеет среднее $\bar{a} = 0,5 + \Delta\bar{a}$, где $\Delta\bar{a}$ - погрешность среднего. Тогда в наиболее распространенном методе формирования последовательности $U \in N(0,1)$, а именно - $U = \sum_{i=1}^{12} (a_i - 0,5)$, имеем $\bar{U} = 12 \cdot \Delta\bar{a}$, т.е. погрешность увеличивается примерно на порядок и более. Если используется способ

$$U = \sqrt{-2 \ln a_1} \cdot \sin 2\pi a_2, \quad a_1, a_2 \in R(0,1),$$

то для определения $\bar{U}$ приходится задаваться конкретной формой "возмущенной" (в силу погрешности) плотности вероятностей $w_1(a)$. Например, если допустить

осциллирующую плотность вида $w_1(a) = 1 + A \sin 2\pi a, a \in [0,1]$, то, как показано в [6], среднее значение $\bar{a}$ смещается влево на величину $A/2\pi$, а $\bar{U} = \frac{[\sqrt{2} \text{AG}(\frac{3}{2})]}{2} \approx 0,63A$, где $\Gamma(\frac{3}{2})$ - гамма-функция. Если же $w_1(a) = \frac{1}{c}, c < 1, a \in [0,c]$, то $\bar{U} \approx 4(1-c)^2 = 16(\Delta\bar{a})^2$.

Таким образом, во всех рассмотренных случаях увеличение погрешности среднего имеет примерно один порядок.

На следующем этапе преобразований последовательность U преобразуется в последовательность S при помощи формирующего фильтра с передаточной функцией $K(Z)$. Как известно, среднее значение $\bar{S}$ процесса на выходе линейной дискретной системы равно $\bar{S} = \bar{U} \cdot K(e^{j0})$, где $K(e^{j0})$ - передаточная функция системы на нулевой частоте. С учетом этого для моделей речевого и телевизионного сигналов соответственно получены следующие соотношения для оценки погрешностей среднего значения [6]:

$$\bar{S} = \frac{\sigma \cdot \sqrt{\gamma_c} \cdot (1 - \cos \gamma_0 + \sin \gamma_0)}{\sqrt{2(1 + \sin \gamma_0)(1 - \cos \gamma_0)}} \cdot \bar{U}, \quad \bar{S} = \sigma \sqrt{\frac{1 + e^{-\gamma_c}}{1 - e^{-\gamma_c}}} \bar{U}, \quad (7)$$

где $\gamma_c = \omega_c \cdot \Delta t$; $\gamma_0 = \omega_c \cdot \Delta t$; Δt - шаг дискретизации.

Расчеты по формулам (7) показали, что и на этом этапе преобразований погрешность среднего увеличивается опять примерно на порядок.

Итак, суммарное увеличение погрешности среднего после всех преобразований составит один-два порядка и более, что в ряде случаев может иметь существенное значение в общем балансе погрешностей моделирования.

При компьютерном моделировании различных систем важной задачей является определение необходимого объема выборки N , поскольку от этого зависят затраченное время и точность полученных результатов. Статистические характеристики случайных процессов в различных системах, полученные экспериментальным путем или компьютерным моделированием, обычно отличающиеся от своих истинных значений, называются оценками соответствующих статистических характеристик. В качестве меры точности оценок обычно используют дисперсию, среднее квадратическое отклонение оценок или, если это возможно, их вариации. Для повышения точности определения этих статистических характеристик следует увеличить объем выборки, что приводит к увеличению машинного времени. Поэтому, чтобы добиться заметного успеха в решении различных задач, важно обоснованно определять необходимый объем выборки при моделировании. Эта задача ниже решается на основании оценок таких статистических характеристик, как среднее значение, дисперсия и корреляционная функция случайных процессов.

Оценка математического ожидания. Как известно, для дискретной случайной последовательности X_i среднеарифметической оценкой математического ожидания может служить величина [9]

$$\bar{m}_x = \frac{1}{N} \sum_{i=1}^N X_i, \quad (8)$$

где $i = 1, 2, \dots, N$, а N – объем выборки.

Дисперсия оценки (8) равна

$$\sigma_{mN}^2 = \frac{\sigma^2}{N} \left[N + 2 \sum_{i=1}^N (N-i) r(k \cdot \Delta t) \right], \quad (9)$$

где $r(\tau) = (k \cdot \Delta t) = \frac{B(\tau)}{\sigma^2}$ - нормированная КФ случайного процесса; σ^2 - его дисперсия.

Рассмотрим эту величину для моделей телевизионных и речевых входных сигналов. Для телевизионного сигнала с КФ (5) при больших объемах выборки дисперсия оценки математического ожидания, определенная из формулы (9), равна

$$\sigma_m^2 = \sigma^2 \cdot \frac{2}{\omega_c T}. \quad (10)$$

Отсюда можно получить соотношение для расчета объема выборки:

$$N = \frac{2}{\gamma_c \varepsilon_0^2} = \frac{2 \cdot f_\phi}{\omega_c \cdot \varepsilon_0^2}. \quad (11)$$

Здесь $\sigma_m^2 / \sigma^2 = \varepsilon_0^2$, причем $\omega_c T = \omega_c \cdot N \cdot \Delta t = \gamma_c \cdot N$, а величина ε_0 , равная корню квадратному из этого выражения, называется нормированной среднеквадратичной ошибкой оценки.

В результате расчета необходимого объема выборки по выражению (11), например, при величинах $\varepsilon_0 = 10\%$ и $f_\phi = 48 \text{ МГц}$ получено значение $N=25000$ [9].

Теперь рассмотрим случай речевого сигнала с КФ (2). После аналогичных преобразований получено следующее соотношение для дисперсии оценки математического ожидания [9]:

$$\sigma_{mN}^2 \approx \sigma^2 \left[\frac{1}{N} \left(1 + 2 \cdot \frac{1 - e^{-\gamma_c} \cos \gamma_0}{1 - 2e^{-\gamma_c} \cos \gamma_0 + e^{-2\gamma_0}} \right) \right]. \quad (12)$$

Выражение (12) использовано в [9] при оценке погрешностей перехода от интегралов к суммам.

Оценка корреляционной функции и дисперсии. Как известно, несмещенной оценкой КФ стационарного случайного процесса $X(t)$ служит величина [9]

$$\tilde{B}_x(t) = \frac{1}{T - \tau} \int_{t_0}^{t_0 - T - \tau} [X(t) - m_x] [X(t - \tau) - m_x] \cdot dt, \quad (13)$$

где m_x - истинное математическое ожидание СП; t_0 - начало отсчета; τ — величина сдвига во времени.

За меру точности оценки КФ, как и в предыдущем случае, примем дисперсию:

$$\sigma_B^2(\tau) = M[\tilde{B}_x(\tau)] - B_x^2(\tau), \quad (14)$$

которая после преобразований и упрощений при $\tau = 0$ приобретает вид

$$\sigma_D^2 = \sigma_B^2(0) \approx \frac{4}{T} \int_0^\infty B_x^2(\tau_1) \cdot d\tau_1. \quad (15)$$

В случае телевизионного сигнала получены следующие формулы для дисперсии оценки КФ и дисперсии соответственно [9]:

$$\sigma_B^2(\tau) = \frac{\sigma^4}{\omega_c(T-\tau)} \left[1 + (1 + 2\omega_c\tau)e^{-2\omega_c\tau} \right] \quad \text{и} \quad \sigma_D^2 = \frac{2\sigma^4}{\omega_c T}. \quad (16)$$

Для речевого сигнала после преобразований имеем

$$\sigma_B^2(\tau) = \frac{2\tau^4}{T-\tau} \left[\frac{2\omega_c + \omega_0^2}{4\omega_c(\omega_c^2 + \omega_0^2)} + \frac{e^{-2\omega_c\tau}(\omega_c \cos \omega_0\tau) - \omega_0 \sin 2\omega_0\tau}{4(\omega_c^2 + \omega_0^2)} + \right. \\ \left. \frac{e - 2\omega_c\tau \sin 2\omega_0\tau}{4\omega_0} + \frac{\tau e^{-\omega_c\tau} \cos 2\omega_0\tau}{2} + \frac{e^{-2\omega_c\tau} \cos 2\omega_c\tau}{4\omega_c} \right]. \quad (17)$$

При $\tau = 0$ можно записать

$$\sigma_D^2 = \frac{\sigma^4(2\omega_c^2 + \omega_0^2)}{\omega_c T(\omega_c^2 + \omega_0^2)}. \quad (18)$$

Тогда после несложных преобразований получим

$$N = \frac{2\omega_c^2 + \omega_0^2}{\gamma_c(\omega_c^2 + \omega_0^2)\varepsilon_0^2} = \frac{f_0(2\omega_c^2 + \omega_0^2)}{\omega_c(\omega_c^2 + \omega_0^2)\varepsilon_0^2}. \quad (19)$$

Выполнив расчет по формуле (19), например, при $f_0 = 48 \text{ кГц}$ и десятипроцентной точности получим $N=5500$.

Итак, для телевизионного сигнала получаются значительно большие объемы выборки, чем для речевого.

Рассмотрим теперь некоторые вероятностные характеристики сигнала ЛДМ при воздействии гармонического сигнала с частотой 800 Гц. Важной характеристикой двоичного ДМ сигнала (или дельта-потока) является корреляционная функция, которая необходима при исследовании энергетических характеристик импульсного сигнала, помехоустойчивости каналов с ДМ и др. [7].

На рис. 4 показана динамика формирования КФ дельта-потока $d(n)$ при возрастании амплитуды входного синусоидального сигнала U_m . При $\frac{U_m}{\varepsilon} \geq 20$ КФ приобретает треугольную форму, здесь ε - шаг квантования. Однако наблюдается и другая закономерность, заключающаяся в том, что КФ имеет строгую периодичность, определяемую частотой входного сигнала и частотой дискретизации.

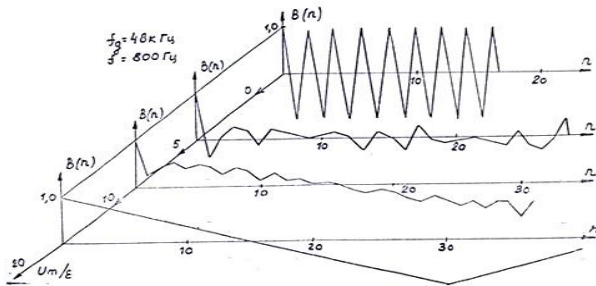


Рис. 4. Корреляционные функции дельта-потока

Важной проблемой при проектировании различных систем является их оптимизация, во многом определяющая технологичность и технико-экономическую эффективность этих систем. Широкое внедрение достижений микроэлектроники выдвигает на первый план проблему выбора оптимального решения на стадии проектирования, так как при этом практически затрудняется возможность экспериментальной оптимизации. В связи с этим большое значение приобретает машинная оптимизация различных систем. В настоящее время существует большое количество разнообразных машинных методов оптимального решения задач, которые, в отличие от аналитических методов, не требуют описания условий задачи в явном (аналитическом) виде. В главе 2 при исследовании систем с ДМ использованы следующие методы оптимизации: градиентный, золотого сечения, Хука-Дживса и статистического (случайного) поиска [8]. Выше было показано, что для получения достоверных оценок статистических характеристик сигналов и параметров системы необходимо увеличивать объем выборки, что ведет к увеличению затрат на моделирование в смысле машинного времени. Поэтому важное значение приобретают использование и разработка методов, обеспечивающих повышение точности оценок при фиксированном объеме выборки или позволяющих уменьшить объем выборки, требуемый для получения заданной точности оценок. Эти методы называют методами уменьшения дисперсии. Одним из них является метод дополняющей переменной согласно которому оптимизируемую случайную величину $Q(\vec{R})$, представляющую отношение сигнал/шум квантования дельта-модулятора, заменяем новой случайной величиной, определяемой следующим соотношением:

$$\tilde{Q}(\vec{R}) = \alpha Q(\vec{R}) + (1 - \alpha)X(\vec{R}), \quad (20)$$

где $\vec{R}$ - вектор из m равномерно распределенных на интервале (0, 1) случайных чисел; $X(\vec{R})$ - некоторая вспомогательная случайная величина с известным математическим ожиданием, равным $M(Q)$, а константа α лежит в интервале (0, 1).

Нетрудно показать, что среднее значение величины $\tilde{Q}(\vec{R})$ равно $M(Q)$, а дисперсия равна [8]

$$D(\tilde{Q}) = \alpha^2 D(Q) + (1 - \alpha)^2 D(X) + 2\alpha(1 - \alpha)\text{Cov}(Q, X), \quad (21)$$

где D – знак дисперсии; $\text{Cov}(Q, X)$ – ковариация между величинами Q и X .

Из этого следует, что если ковариация между Q и X отрицательна, то величина дисперсии $D(\tilde{Q})$ может быть меньше $D(Q)$. В результате проведенных машинных экспериментов удалось добиться отрицательной ковариации между величинами Q и X и сократить дисперсию для разных объемов выборки входного процесса (от 5000 до 11000) в 2...4 раза. При этом система характеризуется следующим показателем качества

$$Q = 10 \lg (P_c / P_{KB}), \text{ дБ}, \quad (22)$$

где P_c – мощность сигнала на входе дельта-модулятора после входного фильтра; P_{KB} – мощность шума квантования. Эта мощность отсчитывается после выходного ФНЧ.

Оптимизация осуществлена для адаптивного дельта-модулятора, который функционирует в соответствии со следующим алгоритмом. На выходе модулятора в

такты моменты времени производится анализ выходной двоичной последовательности. Если в начальный момент два соседних элемента этой последовательности оказываются одинаковыми, то начальный и минимальный шаг квантования с увеличивается в p раз; если же эти элементы различны, то устанавливается шаг sq . В дальнейшем эта процедура непрерывно повторяется, только вместо начального шага уже текущий шаг умножается на величину p , если два соседних символа последовательности одинаковы, или на q - в противном случае. При этом шаг квантования не может превышать некоторого значения x [8].

В диссертации приведены результаты оптимизации данного алгоритма ДМ при различных параметрах, с фильтрами ФНЧ и без них. Для примера рассмотрим рис. 5, где показаны линии постоянного уровня поверхности, определяемой целевой функцией (20), с нанесенными траекториями поиска оптимума из разных начальных точек. Значения целевой функции на этих линиях уровня соответствуют малоотличающимся по “высоте” сечениям трехмерной поверхности в пространстве $(c, p, \tilde{Q})$ и равны: 1 - $\tilde{Q} = 19,872$ дБ; 2 - $\tilde{Q} = 20,107$ дБ; 3 - $\tilde{Q} = 20,667$ дБ, т.е. значения $\tilde{Q}$ для всех трех сечений различаются менее, чем на 1 дБ. Иными словами, все соответствующие “неровности” отвечают “шуму оценки $\tilde{Q}$ ”.

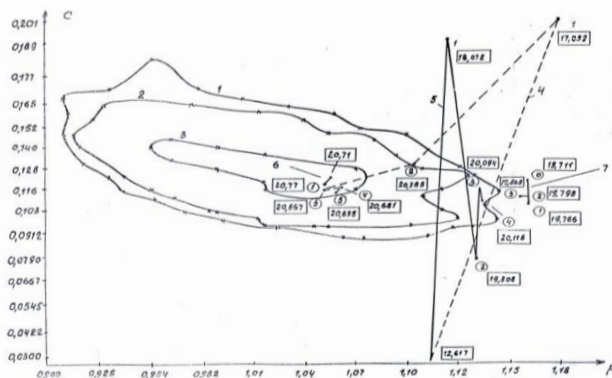


Рис. 5. Линии постоянного уровня поверхности, определяемой целевой функцией (19)

При этом на рис. 5 приняты также следующие обозначения: 5,6,7 - метод Хука-Дживса; 4 - метод наискорейшего спуска; кружками обведены номера итераций, а прямоугольниками - значения $\tilde{Q}$, дБ. Кроме того, $N=10000$, $x=1$, $f_0=48$ МГц, $\alpha=0,25$, система без фильтров. Однако не следует считать, что эта область очень велика. Построение линий постоянного уровня в укрупненном масштабе показало, что, например, уменьшение параметра адаптации p на 0,1 от левой по рис. 5 границы сечения 1 приводит к падению отношения сигнал/шум квантования на 7 дБ. Рассмотрение рис. 5 показывает, что локальные экстремумы $\tilde{Q}(\vec{v})$, найденные

разными методами и при различных начальных значениях $\vec{V}^{(0)}$, весьма мало отличаются друг от друга, коль скоро $\vec{V}^{(0)}$ расположены либо внутри замкнутой линии 1, либо на незначительном удалении от нее (в сторону возрастания p от “правой” границы области).

В третьей главе рассмотрены помехоустойчивое кодирование и коды Рида-Соломона. Проанализированы основные характеристики, свойства и параметры таких важных математических моделей теории кодирования, как группы, кольца и поля (в частности, конечные поля), на основании чего в дальнейшем проведены исследования различных кодов. Кроме того, обобщены практически все известные формы представления элементов конечных полей. Эти и другие результаты анализа, проведенного в диссертации, позволили построить таблицы элементов полей Галуа $GF(2^4)$, $GF(2^5)$ и $GF(2^8)$, а также исследовать ЦК и коды РС.

Главная идея циклических кодов заключается в том, что циклический сдвиг любого кодового слова приводит к новому КС.

Аналитическое описание и преобразования над циклическими кодами удобно осуществлять, представив их в следующей полиномиальной форме [27]:

$$c(x) = c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1}, \quad (23)$$

где x - основание КС (фиктивная переменная); c_i - координаты КС (для двоичных кодов – это 0 и 1); n - его длина.

Циклический сдвиг этого полинома вправо можно получить, умножив его на x . Действительно,

$$xc(x) = c_0x + c_1x^2 + c_2x^3 + \dots + c_{n-2}x^{n-1} + c_{n-1}x^n = c^{(1)}(x). \quad (24)$$

Чтобы степень полинома не превышала $n-1$, необходимо в этом выражении положить $x^n = 1$. Тогда получим циклический сдвиг, например, на один разряд вправо:

$$c^{(1)}(x) = xc(x) = c_{n-1} + c_0x + c_1x^2 + c_2x^3 + \dots + c_{n-2}x^{n-1}. \quad (25)$$

В общем случае при сдвиге на $n-1$ разряд получим

$$c^{(n-1)}(x) = c_1 + c_2x + c_3x^2 + \dots + c_0x^{n-1}. \quad (26)$$

Кодирование и декодирование ЦК можно производить с помощью матриц, а также методом, основанным на понятии генераторного (порождающего, образующего, производящего) полинома.

Сущность представления ЦК с помощью генераторного полинома заключается в том, что кодовый полином $c(x)$ формируется умножением информационного полинома $m(x) = m_0 + m_1x + m_2x^2 + \dots + m_{k-1}x^{k-1}$ длиной k на генераторный полином $g(x) = g_0 + g_1x + g_2x^2 + \dots + g_rx^r$ степени $r = n - k$. Естественно, что при делении КС (т.е. разрешенной комбинации) на генераторный полином мы получим нулевой остаток. Если же кодовое слово исказилось под влиянием ошибок, т.е. образовалась запрещенная комбинация, то результат аналогичного деления даст некоторый остаток, по которому и можно судить о наличии ошибок. Отметим, что в систематических ЦК, в отличие от несистематических, позиции проверочных и информационных символов строго определены. Вначале в КС могут располагаться

проверочные, а затем информационные символы, или наоборот. Для формирования *несистематических* ЦК обычно используется следующее простое выражение:

$$c(x) = m(x) \cdot g(x). \quad (27)$$

Рассмотрим способ построения *систематических* ЦК. Как уже отмечалось ранее, последовательные сдвиги $x^r \cdot c(x)$ кодового слова $c(x)$ образуют также новое КС.

Умножив $m(x)$ на x^r и разделив результат на $g(x)$, получим [15,27]

$$\frac{x^r \cdot m(x)}{g(x)} = \varepsilon(x) + \frac{\rho(x)}{g(x)}, \quad (28)$$

где $\varepsilon(x)$ - частное от деления; $\rho(x)$ - остаток.

Из выражения (28) нетрудно получить

$$\varepsilon(x) \cdot g(x) = x^r \cdot m(x) - \rho(x) = c(x). \quad (29)$$

Поскольку произведение $x^r \cdot m(x)$ осуществляет сдвиг полинома $m(x)$ на r символов, то k позиций кодового слова $c(x)$ занимают информационные символы, а остальные r - проверочные символы, соответствующие остатку. Далее из (29) получим выражение для систематического кода:

$$c(x) = \rho(x) + x^{n-k} m(x) = \rho_0 + \rho_1 x + \dots + \rho_{n-k-1} x^{n-k-1} + m_0 x^{n-k} + m_1 x^{n-k+1} + \dots + m_{k-1} x^{n-1}, \quad (30)$$

которому соответствует КС $C = (\rho_0, \rho_1, \dots, \rho_{n-k-1}, m_0, m_1, \dots, m_{k-1})$ или в общем виде $C = (c_0, c_1, c_2, \dots, c_{n-2}, c_{n-1})$.

Используем приведенные соотношения с целью построения циклического кода ЦК(7,4) для следующих информационных кодовых слов: $m_1(x) = 1 + x + x^2$; $m_2(x) = x + x^3$; $m_3(x) = 1 + x + x^2 + x^3$ и $m_4(x) = x^3$. Здесь имеем $n = 7$, $k = 4$ и $r = 3$. Определим генераторный полином, разложив двучлен $x^n \pm 1 = x^{2^{m-1}} \pm 1$ на неприводимые полиномы. Для нашего случая $m = 3$. Это значит, что сомножителями двучлена $x^7 + 1$ должны быть неприводимые полиномы, степени которых являются делителями числа 3, т.е. это полиномы первой и третьей степеней. Тогда, используя таблицы неприводимых полиномов, получим следующее разложение [27]:

$$x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

Для кода ЦК(7,4) генераторный полином должен иметь степень $r = 3$. Остановим выбор на полиноме $g(x) = 1 + x^2 + x^3$, т.е. кодовый вектор (КВ) равен $G = 1011$. Теперь определим кодовые комбинации для всех заданных информационных кодовых слов, используя формулу (27).

Для $m_1(x) = 1 + x + x^2$ (КВ $M_1 = 1110$) имеем $c_1(x) = (1 + x + x^2)(x^3 + x^2 + 1) = 1 + x + x^5$, т.е. $C_1 = 1100010$.

Далее $m_2(x) = x + x^3$ (КВ $M_2 = 0101$). Аналогично:

$$c_2(x) = (x + x^3)(x^3 + x^2 + 1) = x + x^4 + x^5 + x^6, \text{ т.е. } C_2 = 0100111.$$

Следующий код для $m_3(x) = 1 + x + x^2 + x^3$ (КВ $M_3 = 1111$) имеет вид

$$c_3(x) = (1+x+x^2+x^3)(x^3+x^2+1) = 1+x+x^3+x^6, \text{ т.е. } C_3 = 1101001.$$

И, наконец, для $m_4(x) = x^3$ (КВ $M_4 = 0001$) имеем

$$c_4(x) = x^3(x^3+x^2+1) = x^3+x^5+x^6, \text{ т.е. } C_4 = 0001011.$$

Обратив внимание на структуру полученных КС, можно заметить, что здесь ни первые k позиций, ни последние не занимают информационные кодовые слова, а это значит, что полученный код *несистематический*.

Заметим, что если мы будем записывать все полиномы в виде $f(x) = f_1x^{n-1} + f_2x^{n-2} + \dots + f_n$, т.е. по убывающим степеням переменной X , то в результате получим кодовые слова, инверсные тем, что получены нами.

Теперь построим одно кодовое слово для *систематического* кода ЦК(7,4), используя предыдущий генераторный полином. Пусть $m_1(x) = 1+x+x^2$ или $M_1 = 1110$. Тогда $x^3 \cdot m_1(x) = x^3 \cdot (1+x+x^2) = x^3+x^4+x^5$. Разделив этот результат на $g(x)$ в соответствии с формулой (27), получим КС по формуле (28)

$$c_1(x) = \rho_1(x) + x^r \cdot m_1(x) = 1+x^3+x^4+x^5, \text{ т.е. } C_1 = 1001110.$$

Как уже отмечалось, существует различное представление полиномов, а именно, по возрастающим или убывающим степеням переменной x . Рассмотрим теперь предыдущий пример для случая убывания степеней X . Для этого построим одно КС для систематического кода ЦК(7,4), используя для генераторного и информационного полиномов соответственно записи $g(x) = x^3+x^2+1$ и $m_1(x) = x^2+x+1$ (т.е. $M_1 = 0111$).

Тогда, умножив $m_1(x)$ на x^3 и произведя деление на $g(x)$, окончательно имеем $c_1(x) = x^5+x^4+x^3+1 \rightarrow 0111001$, т.е. первые $k=4$ позиции занимает информационный вектор, а следующие $r=3$ – проверочный вектор (остаток), причем, что очень важно, кодовые слова инверсны друг другу!

Техническая реализация ЦК основана на использовании обычных сдвигающих регистров, сумматоров и умножителей, как это показано на рис. 6 для случая несистематического ЦК [15].

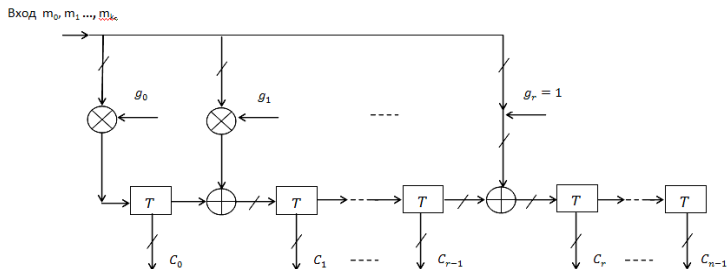


Рис. 6. Структурная схема несистематического циклического кодера:

$\otimes$ - умножители; $\oplus$ - сумматоры; T - сдвигающие регистры;
 $g_0, g_1, g_2, \dots, g_r$ - коэффициенты генераторного полинома.

В последние годы среди многообразных циклических кодов большое распространение во многих системах и устройствах получили недвоичные коды РС,

которые характеризуются генераторным полиномом следующего вида:

$$g(x) = (x + \alpha^\lambda)(x + \alpha^{\lambda+1})(x + \alpha^{\lambda+2}) \dots (x + \alpha^{\lambda+r-1}) = \prod_{i=0}^{r-1} (x + \alpha^{\lambda+i}), \quad (31)$$

где λ - любое положительное целое число, включая и нуль; α - элемент из $GF(2^m)$, являющийся корнем примитивного полинома, который выбран для построения генераторного полинома и всего кода в целом [25, 27, 28].

Код $RS(n, k)$ определяется следующими параметрами с символами из $GF(2^m)$: $n = 2^m - 1$ - число m битовых символов в коде; $k = n - 2\nu = n - r$ - число m битовых информационных символов; $n - k = r = 2\nu$ - число m битовых проверочных символов; ν - максимальное количество m битовых исправляемых символов.

Выбор величины λ сильно влияет на структуру кода и служит предметом отдельного исследования. Например, для некоторых систем асимметричных цифровых абонентских линий (ADSL), где используется код $RS(255, 239)$, выбрано $\lambda = 0$. В стандарте CCSDS использовано $\lambda = 11$, что привело к снижению сложности аппаратуры. Однако наиболее распространенным является выбор $\lambda = 1$, и коды РС тогда называются кодами в узком смысле (*narrow-sense*). Для этого случая получим

$$g(x) = (x + \alpha)(x + \alpha^2) \dots (x + \alpha^r) = \prod_{i=0}^{r-1} (x + \alpha^{i+1}) = \prod_{i=1}^r (x + \alpha^i). \quad (32)$$

С другой стороны

$$g(x) = g_0 + g_1x + g_2x^2 + \dots + g_rx^r = \sum_{i=0}^r g_ix^i = \sum_{i=1}^{r+1} g_{i-1}x^{i-1}. \quad (33)$$

Тогда можем записать

$$g(x) = \prod_{i=1}^r (x + \alpha^i) = \prod_{i=0}^{r-1} (x + \alpha^{i+1}) = \sum_{i=0}^r g_ix^i = \sum_{i=1}^{r+1} g_{i-1}x^{i-1}. \quad (34)$$

Анализ этих выражений показывает, что, во-первых, в генераторном полиноме кода РС всегда присутствуют все его члены. Поэтому структурная схема кодера РС должна содержать все коэффициенты полинома $g(x)$, т.е. $g_0, g_1, g_2, \dots, g_r$, причем всегда $g_r = 1$. Во-вторых, степень генераторного полинома всегда равна r . В-третьих, всегда присутствует свободный член g_0 генераторного полинома [25].

С учетом сказанного на рис. 7 представлена общая блок-схема систематического кодера $RS(n, k)$ над полем $GF(2^m)$.

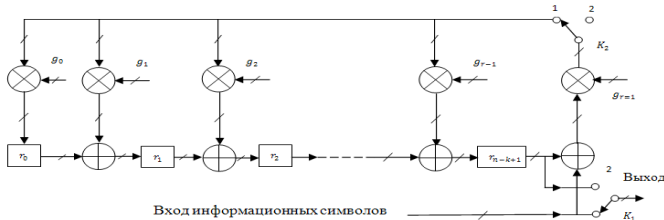


Рис. 7. Структура кодера $RS(n, k)$ над полем $GF(2^m)$

Здесь $\boxed{r_i}$ - m битовые сдвигающие регистры на один разряд, $\oplus$ - m битовые сумматоры; $\otimes$ - m битовые умножители; $g_0, g_1, g_2, \dots, g_r$ - m битовые коэффициенты генераторного полинома; K_1, K_2 - переключатели.

В настоящее время существуют следующие основные методы (алгоритмы), используемые при декодировании кодов Рида Соломона:

1. Питерсона-Горенштейна-Цирлера (Peterson-Gorenstein-Zierler - PGZ).
2. Процедура Чена (Chien search).
3. Берлекампа-Питерсона-Мессе (Berlekamp-Peterson-Massey).
4. На основе Быстрого Преобразования Фурье (FFT).
5. Евклида (Euclidean).
6. Прямое декодирование без использования итеративных алгоритмов.
7. Декодирование по алгоритму Гурсурами-Судана за пределами кодового расстояния, т.е. когда число ошибок больше $(d-1)/2$.

Общая идея декодирования кодов РС такая же, как и для циклических кодов. Первым шагом декодирования является вычисление полинома ошибок $e(x)$ по принятому на входе полиному $y(x)$. Эта процедура начинается с определения синдромного полинома $S(x)$, куда входят величина X_1 , часто называемая локатором ошибок и определяющая позицию ошибок, и величина Y_1 , которая дает значение ошибки (часто говорят: значение, амплитуда или магнитуда). Определение X_1 и Y_1 осуществляется вычислением полинома локатора ошибок $\Lambda(x)$.

Кратко рассмотрим эти этапы декодирования, которые более подробно исследованы в диссертации.

Для вычисления синдрома возможно применение следующих двух подходов:

- прямая подстановка корней $\alpha^1, \alpha^2, \alpha^3, \alpha^4, \dots, \alpha^r$ генераторного полинома в принятый кодовый полином $y(x)$;
- путем деления $y(x)$ на полином вида $h(x) = (x + \alpha^j)$, где $j = 1, 2, 3, \dots, r-1$.

В первом случае компоненты синдрома равны

$$S_j = \sum_{i=1}^{\gamma} e_{i_l} (\alpha^j)^{i_l} = \sum_{i=1}^{\gamma} e_{i_l} (\alpha^{i_l})^j, \quad j = 1, 2, 3, \dots, r. \quad (35)$$

Здесь $e(x) = e_{i_1} x^{i_1} + e_{i_2} x^{i_2} + \dots + e_{i_\gamma} x^{i_\gamma} = \sum_{i=1}^{\gamma} e_{i_l} x^{i_l}$ - полином ошибок, $i = 1, 2, \dots, n$; i_l - индекс i при e_{i_l} показывает расположение ошибки, а индекс l - номер ошибки. Позиции ошибок γ , которые произошли на самом деле, обозначены через $i_1, i_2, \dots, i_\gamma$, где $0 \leq \gamma \leq v$.

Во втором случае компоненты синдрома равны остатку от деления $y(x)$ на $h(x)$, т.е. $S_j = \rho_j(\alpha^j)$.

Для нахождения полинома локатора ошибок введем новые, более простые обозначения: $X_l = \alpha^{i_l}$ - локаторы ошибок, которые являются элементами поля $GF(2^m)$

и указывают позиции $i_1, i_2, \dots, i_v$, где действительно произошли ошибки; $Y_l = e_{i_l}$ - величины ошибок.

Тогда с учетом этих обозначений уравнения для синдрома можно представить в виде следующей системы:

$$\begin{cases} S_1 = Y_1 X_1^1 + Y_2 X_2^1 + \dots + Y_v X_v^1, \\ S_2 = Y_1 X_1^2 + Y_2 X_2^2 + \dots + Y_v X_v^2, \\ \vdots \\ S_j = Y_1 X_1^j + Y_2 X_2^j + \dots + Y_v X_v^j, \\ \vdots \\ S_r = Y_1 X_1^r + Y_2 X_2^r + \dots + Y_v X_v^r. \end{cases} \quad (36)$$

Таким образом, имеем систему нелинейных уравнений с неизвестными X_l, Y_l , где $l = 1, \dots, \gamma$. Эта система имеет единственное решение при $0 \leq \gamma \leq v$, хотя в "лоб" ее решить невозможно. Поэтому для решения системы (36) ее линеаризуют с помощью вспомогательных полиномов. Часто для этой цели используется специальный, так называемый, полином локаторов ошибок вида

$$\Lambda(x) = \Lambda_0 + \Lambda_1 x + \Lambda_2 x^2 + \dots + \Lambda_\gamma x^\gamma, \quad (37)$$

причем всегда полагают $\Lambda_0 = 1$, а корни этого полинома являются инверсными величинам локаторов ошибок, т.е. равны X_l^{-1} , при $l = 1, \dots, \gamma$, следовательно количество ошибок равно степени этого полинома.

Тогда $\Lambda(x)$, как и любой другой полином, можно представить в виде

$$\Lambda(x) = (1 - X_1 x)(1 - X_2 x) \dots (1 - X_\gamma x) = \prod_{i=1}^{\gamma} (1 - X_i x). \quad (38)$$

Компоненты синдрома с коэффициентами многочлена $\Lambda(x)$ связывает следующая система:

$$\begin{cases} \Lambda_1 S_\gamma + \Lambda_2 S_{\gamma-1} + \dots + \Lambda_{\gamma-1} S_2 + \Lambda_\gamma S_1 = -S_{\gamma+1}, \\ \Lambda_1 S_{\gamma+1} + \Lambda_2 S_\gamma + \dots + \Lambda_{\gamma-1} S_3 + \Lambda_\gamma S_2 = -S_{\gamma+2}, \\ \vdots \\ \Lambda_1 S_{2\gamma-2} + \Lambda_2 S_{2\gamma-3} + \dots + \Lambda_{\gamma-1} S_\gamma + \Lambda_\gamma S_{\gamma-1} = -S_{2\gamma-1}, \\ \Lambda_1 S_{2\gamma-1} + \Lambda_2 S_{2\gamma-2} + \dots + \Lambda_{\gamma-1} S_{\gamma+1} + \Lambda_\gamma S_\gamma = -S_{2\gamma}. \end{cases} \quad (39)$$

Эта система линейных уравнений часто называется тождествами Ньютона.

Данная система может быть представлена и в краткой матричной форме

$$\Lambda = M^{-1} \cdot S, \quad (40)$$

где Λ - матрица коэффициентов полинома локатора ошибок; S - матрица компонент полинома синдрома из правой части (40); M^{-1} - матрица, обратная матрице компонент полинома синдрома из левой части (40).

Решение матричного уравнения (38) для нахождения коэффициентов полинома $\Lambda(x)$ производится по алгоритму PGZ и требует двукратной инверсии матриц, при которой в случае $v > 7$ объем вычислений становится чрезмерным, и поэтому приходится использовать другие методы. Один из таких методов носит имя Берлекампа-Мессис (Б-М) с использованием итеративной процедуры вычисления корней полинома $\Lambda(x)$, которая легко осуществима посредством регистров сдвига с обратными связями (LFSR- Linear Feedback Shift-Register).

Следующий этап декодирования - нахождение позиций ошибок, например, с использованием процедуры Ченя, при которой осуществляется подстановка элементов α^{-j} в $\Lambda(x)$ с дальнейшей проверкой полученных значений равенству нулю:

$$\Lambda(\alpha^{i_1}) = \sum_{j=0}^v \Lambda_j \alpha^{j \cdot i_1} = 0, \quad i_1 = 0, 1, \dots, n-1. \quad (41)$$

Итак, последний этап декодирования - определение значений ошибок. Удобным способом вычисления значений ошибок Y_i является алгоритм Форни. Существует два способа представления этого алгоритма: с помощью формальных производных и через ряды. Рассмотрим первый способ. Зададим полином значений ошибок в виде следующего ключевого уравнения (key equation):

$$\Lambda(x) \cdot S(x) = \Omega(x) \bmod x^{2v}. \quad (42)$$

Решение этого уравнения имеет вид:

$$Y_i = e_{i_1} = \frac{-X_i \Omega(X_i^{-1})}{\Lambda'(X_i^{-1})}, \quad (43)$$

где $\Lambda'(x)$ - формальная производная, а X_i^{-1} - корни полинома $\Lambda(x)$.

Покажем все этапы декодирования на примере кода RS(7,3) при $\lambda=0$, $v=2$.

Тогда $g(x) = (x+1)(x+\alpha)(x+\alpha^2)(x+\alpha^3) = \alpha^6 + \alpha^{78}x + \alpha^{249}x^2 + \alpha^{75}x^3 + x^4$.

Пусть на входе декодера принято ошибочное КС:

$$y(x) = 1 + \alpha^9x + \alpha^{81}x^2 + \alpha^{252}x^3 + \alpha^{78}x^4 + \alpha^{51}x^5.$$

Рассчитав коэффициенты $S(x)$ прямой подстановкой элементов α^j в $y(x)$, получим

$$S(x) = \alpha^{25} + \alpha^{191}x + \alpha^{245}x^2 + \alpha^{145}x^3.$$

Итак, $S_1 = \alpha^{25}$; $S_2 = \alpha^{191}$; $S_3 = \alpha^{245}$; $S_4 = \alpha^{145}$. Расчет полинома локаторов ошибок по алгоритму Б-М приведен в таблице, где принято $S_0 = 0$.

Таблица

Расчет $\Lambda(x)$ по алгоритму Б-М

k	S_k	$\Delta^{(k)}$	$\Lambda^{(k)}(x)$	L	$B(x)$
0	0	0	1	0	x
1	α^{25}	$S_1 - 1 \cdot 0 = S_1 = \alpha^{25}$	$\Lambda^{(0)}(x) - \Delta^{(1)}(x) \cdot B(x) = 1 + \alpha^{25}x = 1 + \Lambda_1^{(1)}x$	1	$\frac{1}{\alpha^{25} \cdot x} = \alpha^{-25} = \alpha^{230}$
2	α^{191}	$S_2 - \Lambda_1^{(1)} \cdot S_1 = \alpha^{191} + \alpha^{25} = \alpha^{191}$	$\Lambda^{(1)}(x) - \Delta^{(2)}(x) \cdot B(x) = 1 + \alpha^{25}x + \alpha^{191}x^2 = 1 + \alpha^{25}x + \alpha^{332}x = (\alpha^{25} + \alpha^{77})x + 1 + \alpha^{166}x$	1	$\alpha^{230} \cdot x$
3	α^{245}	$S_3 - \Lambda_1^{(2)} \cdot S_2 = \alpha^{245} + \alpha^{191} \cdot \alpha^{191} = \alpha^{245} + \alpha^{102} = \alpha^{232}$	$1 + \alpha^{166}x + \alpha^{227}x^2 + \alpha^{73}(\alpha^{33}x + \alpha^{169}x^2) = 1 + \alpha^{166}x + \alpha^{227}x^2 + \alpha^{76}x + \alpha^{242}x^2 = 1 + (\alpha^{166} + \alpha^{76})x + (\alpha^{227} + \alpha^{242})x^2 = 1 + \alpha^{138}x + \alpha^5x^2$	2	$\frac{1 + \alpha^{138}x}{\alpha^{232}} = \alpha^{-232} + \alpha^{-88}x = \alpha^7 + \alpha^{189}x^2$

4	α^{145}	$S_4 - [\Lambda_1^{(3)} \cdot S_3 + \Lambda_2^{(3)} \cdot S_2] =$ $\alpha^{145} + \alpha^{166} \cdot \alpha^{245} +$ $\alpha^{227} \cdot \alpha^{191} = \alpha^{145} + \alpha^{156} +$ $\alpha^{163} = \alpha^{73}$	$1 + \alpha^{166}x + \alpha^{227}x^2 +$ $\alpha^{73}(\alpha^3x + \alpha^{169}x^2) = 1 +$ $\alpha^{166}x + \alpha^{227}x^2 + \alpha^{76}x +$ $\alpha^{242}x^2 = 1 + (\alpha^{166} +$ $\alpha^{76})x + (\alpha^{227} + \alpha^{242})x^2 =$ $1 + \alpha^{138}x + \alpha^5x^2$	-	-
---	----------------	--	---	---	---

Отсюда $\Lambda(x) = 1 + \alpha^{138}x + \alpha^5x^2$. Тогда $\Lambda'(x) = \alpha^{138}$.

Корни $\Lambda(x)$ определим согласно процедуре Ченя подстановкой величин $x = \alpha^{-i}$, $i = 0, \dots, n-1$:

$$\begin{aligned} \Lambda(1) &= 1 + 1 + \alpha^5 + \alpha^5 = 0; & \Lambda(\alpha^{-1}) &= 1 + \alpha + \alpha^2 + \alpha^4 + \alpha^7 \neq 0; \\ \Lambda(\alpha^{-2}) &= \alpha^2 + \alpha^3 + \alpha^6 \neq 0; & \Lambda(\alpha^{-3}) &= \alpha + \alpha^2 + \alpha^5 \neq 0; & \Lambda(\alpha^{-4}) &= \alpha + \alpha^2 + \alpha^5 \neq 0; \\ \Lambda(\alpha^{-5}) &= 1 + \alpha^{133} + \alpha^{250} = 0; & \Lambda(\alpha^{-6}) &= \alpha + \alpha^5 + \alpha^7 \neq 0. \end{aligned}$$

Таким образом, $X_0 = 1$; $X_5^{-1} = \alpha^{-5}$, т.е. $X_5 = \alpha^5$, следовательно, ошибки произошли на нулевой и пятой позициях кодового слова.

Определим

$$\Omega(x) = \Lambda(x) \cdot S_1(x) \bmod x^4 = (1 + \alpha^{138} \cdot x + \alpha^5 \cdot x^2)(\alpha^{25} + \alpha^{191} \cdot x + \alpha^{245} \cdot x^2 + \alpha^{145} \cdot x^3) \bmod x^4 = \alpha^{25} + \alpha^{101}x.$$

Тогда из (43) имеем

$$Y_i = \frac{X_i \cdot \Omega(X_i^{-1})}{\Lambda'(X_i^{-1})} = \frac{X_i(\alpha^{25} + \alpha^{101} \cdot X_i^{-1})}{\alpha^{138}} = (X_i \alpha^{25} + \alpha^{101}) \cdot \alpha^{-138} = \alpha^{142} \cdot X_i + \alpha^{218}.$$

Величины $Y_0 = \alpha^{142} \cdot 1 + \alpha^{218} = 1$; $Y_5 = \alpha^{142} \cdot \alpha^5 + \alpha^{218} = \alpha^{147} + \alpha^{218} = \alpha!$ равны. Тогда полином ошибок $e(x) = 1 + \alpha x^5$.

Найдем правильно переданный кодовый полином, т.е. исправим ошибку:

$$\begin{aligned} c(x) &= y(x) + e(x) = 1 + \alpha^9x + \alpha^{81}x^2 + \alpha^{252}x^3 + \alpha^{78}x^4 + \alpha^{51}x^5 + 1 + \alpha x^5 = \\ &= \alpha^9x + \alpha^{81}x^2 + \alpha^{252}x^3 + \alpha^{78}x^4 + \alpha^3x^5 \end{aligned}$$

Проверим полученный результат на нулевой остаток делением $c(x)$ на $g(x)$

$$\begin{array}{r} \alpha^9x + \alpha^{81}x^2 + \alpha^{252}x^3 + \alpha^{78}x^4 + \alpha^3x^5 \\ \alpha^9x + \alpha^{81}x^2 + \alpha^{252}x^3 + \alpha^{78}x^4 + \alpha^3x^5 \\ \hline 0 \end{array} \quad \begin{array}{r} \alpha^6 + \alpha^{78}x + \alpha^{249}x^2 + \alpha^{75}x^3 + x^4 \\ \alpha^3x \\ \hline \end{array}.$$

Итак, обобщив ранее изложенное, можем представить схему декодера, показанную на рис. 8.

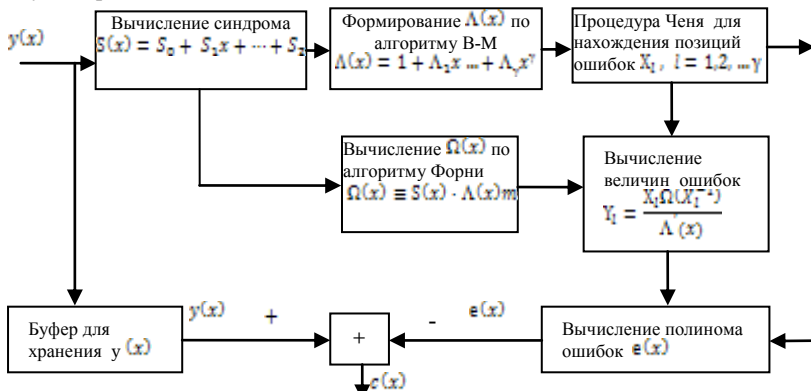


Рис. 8. Модель декодера Рида-Соломона

Как видно из схемы, приведенной на рис.8, при декодировании производится большое количество различных математических операций в конечном поле, из которых наиболее сложной операцией является умножение. В диссертации выведены формулы для двух типов умножителей с помощью соответствующих таблиц в полях $GF(2^3)$ и $GF(2^8)$, на основе которых разработаны их принципиальные схемы [16].

В четвертой главе рассмотрены остальные компоненты сложной кодирующей системы, а именно, - вокодеры, шифраторы, перемежители и коды передачи.

Традиционно устройства сжатия (компрессии) речевых сигналов называются вокодерами, которые осуществляют различные преобразования над сигналами. В зависимости от методов таких преобразований вокодеры можно разделить на аналоговые и цифровые.

В классических аналоговых вокодерах, называемых также и параметрическими системами сжатия, по каналу связи вместо речевого сигнала передаются сигналы, соответствующие его структурным параметрам, которые выделяются на передающей стороне. Так как объем всех структурных сигналов-параметров намного меньше объема самого речевого сигнала, то уменьшается и объем передаваемой информации, т.е. происходит компрессия.

Все эти системы основаны на идее линейного предсказания, которое может рассматриваться как частный случай метода рекуррентно-разностных уравнений, описанного формулой (1).

В настоящее время параметрические вокодеры в отдельности не нашли широкого применения из-за ухудшения натуральности звучания речи и чувствительности к фоновому шуму. Поэтому более широко используются гибридные методы, в которых объединены линейные предсказатели, параметрические компрессоры и кодеры формы волны. В последние годы разработаны весьма эффективные стандарты и системы компрессии нового поколения для цифровой передачи ТВ сигнала. Это три основных стандарта сжатия цифрового ТВ сигнала MPEG-1, MPEG-2, MPEG-4.

Цифровой сигнал после компрессии в кодере источника подвергается дополнительному кодированию в различных устройствах с целью защиты системы от несанкционированного доступа. Устройства защиты информации по степени стойкости условно можно разделить на следующие виды: маскираторы для защиты от случайного подслушивания; скремблеры (перемешиватели), позволяющие защищать информацию от профессионалов в течение ограниченного периода времени (сутки, месяцы); шифраторы – устройства гарантированной стойкости с защитой на длительный период времени (десятилетия).

Шифраторы - наиболее сложные системы, в которых в настоящее время применяют два различных метода: преобразования аналоговых параметров сигнала и цифровые преобразования. Основопологающей работой в этой области можно считать известную работу К. Шеннона, где изложены математическая структура и алгебра секретных систем, теоретические и практические вопросы обеспечения секретности передаваемой информации. В дальнейшем появилось огромное количество работ и разработанных устройств, посвященных этой проблеме. С целью унификации многочисленного количества предложенных алгоритмов, методов и

устройств во многих странах были приняты национальные стандарты шифрования, например, ГОСТ 28147-89 (Россия) или DES (США) и др.

В соответствии с обобщенной моделью системы в кодер канала включены перемежитель и кодер передачи (уровни 5 и 6 на рис. 2). С целью разбиения пачек одинаковых символов на одиночные разработаны специальные устройства перемежения – деперемежения, которые в общем случае, подобно кодам, можно подразделить на блочные и сверточные. Идея перемежения заключается в следующем: на передающей стороне перемежитель переставляет (перемешивает) символы исходной последовательности некоторым образом в соответствии с выбранным алгоритмом. Далее в приемном устройстве деперемежитель производит перестановку в обратном порядке, в результате чего восстанавливается исходная последовательность.

В диссертации рассмотрены структура и характеристики некоторых типов перемежителей, а именно, псевдослучайного, сверточного и блочного (матричный и диагональный), которые были использованы при исследованиях предложенной модели.

Для повышения эффективности и качества цифровых систем передачи важным является выбор соответствующего линейного сигнала (кода передачи), к которому в общем случае предъявляются следующие основные требования [10]: независимость от источника информации и однозначность декодирования, т.е. возможность передачи любого типа сообщений (речь, музыка, телевидение, данные и т.д.); возможность обнаружения и исправления ошибок; наличие информации о синхросигнале; оптимальный энергетический спектр для согласования характеристик сигнала с линией связи. При этом спектр сигнала должен иметь незначительную низкочастотную составляющую для уменьшения межсимвольных искажений; низкую мощность высокочастотной составляющей, т.е. более узкую полосу частот сигнала; и не иметь постоянную составляющую.

В современных информационных технологиях большое распространение получили различные коды передачи [10,11,24]. В простейшем случае электрические сигналы в линии связи или линейные сигналы, соответствующие кодам передачи в виде логических единиц и нулей, представляют собой однополярные или двуполярные импульсы. С другой стороны, часто эти сигналы носят название кодов с возвратом к нулю (ВН-Return to Zero-RZ) или без возврата к нулю (БВН-Non RZ). На основе методов ВН и БВН построено большое разнообразие кодов [10].

Приведем результаты моделирования следующих кодов: манчестерский, ВН, БВН и ЧПИ, которые показаны на рис. 9. [24].

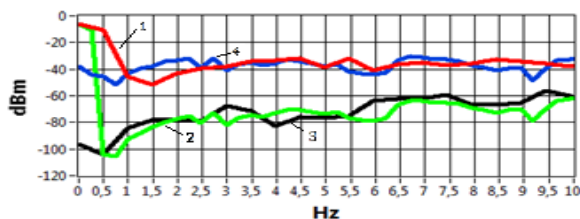


Рис.9. Спектры кодов БВН, манчестерского, ЧПИ и ВН

Исследования осуществлены с помощью пакета LabVIEW, в котором составлена программа для моделирования кодов, а вычисление их спектров производится с помощью встроенной программы Быстрого Преобразования Фурье. Анализ спектров этих четырех кодов показывает, что коды БВН-NRZ (1) и манчестерский-Manchester (2) содержат постоянную составляющую, а ЧПИ-AMI (3) и ВН-RZ (4) её не имеют.

В пятой главе разработана компьютерная модель новой сложной системы связи и приведены результаты моделирования предложенной каскадной конструкции. Модель состоит из следующих уровней: 1 - АЦП; 4 – помехоустойчивый кодер; 5 - перемежитель; 7 - модулятор и 8 - канал связи. Эта конструкция отличается следующими новшествами: во-первых, в качестве внешнего кодера (АЦП) использована дельта-модуляция; во-вторых, внутренним кодером служит кодер Рида-Соломона; и в-третьих, перемежитель включен после помехоустойчивого кодера, как это показано на базовом рис. 10 [18].

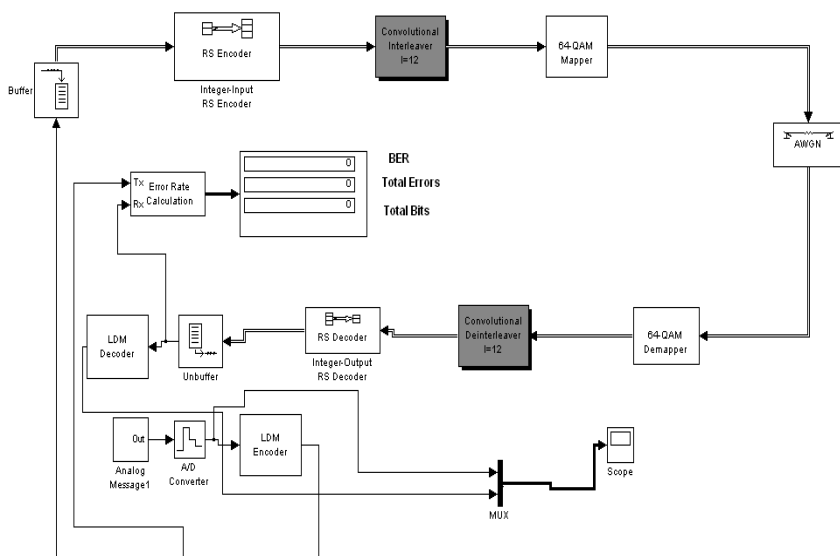


Рис. 10. Базовая модель разработанной конструкции

Здесь приведены кодеки линейной ДМ (LDM Encoder/Decoder) и Рида Соломона (RS Encoder/Decoder), сверточный перемежитель (Convolutional Interleaver I=12/Deinterleaver I=12), модем с квадратурной амплитудной модуляцией (64QAM Mapper/Demapper), а также канал с АГБШ (AWGN).

В дальнейшем эта модель была усложнена введением блока Find Delay с целью определения задержки сигнала после прохождения нескольких блоков. Кроме того, в модель включен и блок Running Sum для контроля числа исправленных ошибок [20,23].

В результате разработана усложненная и универсальная компьютерная модель конструкции, приведенная на рис. 11.

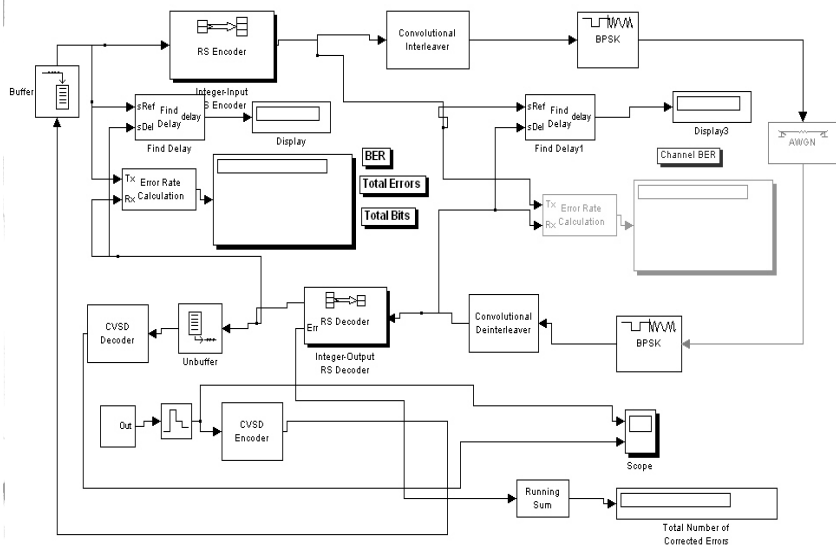


Рис. 11. Универсальная модель сложной системы связи

В этой модели простой заменой нужных блоков можно проводить исследования для любых случаев, что и осуществлено в диссертации.

Здесь отметим, что в этой главе обоснован выбор ДМ по критерию вероятности появления пачек импульсов [7,29].

Приведем некоторые результаты моделирования. Отметим, что кодер Рида Соломона и канал связи оставались без изменений.

Моделирование конструкции с ЛДМ, 2ФМн и пятью типами перемежителей показало, что применение сверточного интерливера позволяет получить выигрыш отношения E_b/N_0 (энергии бита E_b к спектральной плотности шума N_0) примерно в 1,5 дБ по сравнению с другими перемежителями при вероятности битовой ошибки $BER=10^{-6}$.

Остальные типы перемежителей обеспечивают примерно равные показатели. Кроме того, в предложенной кодовой конструкции вероятность появления ошибочных битов в 10^{-6} достигается при отношении E_b/N_0 , равном примерно 6...7 дБ. На рис. 12 для сравнения и оценки эффективности рассмотренной каскадной схемы приведены зависимости BER от отношения E_b/N_0 для кодов Хэмминга и алгоритма Витерби со сверточным кодированием (СК) вне состава конструкции [19,21,22].

Как видно из рис.12, предложенная модель обладает более лучшими характеристиками.

На следующем этапе произведена замена ЛДМ на АДМ и исследованы те же зависимости для разных перемежителей, показанные на рис. 13.

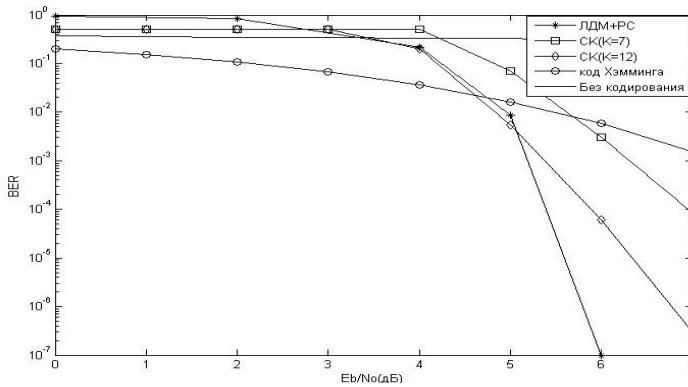


Рис. 12. Сравнение характеристик различных методов кодирования при 2ФМн

Исследования показали, что применение АДМ незначительно улучшает характеристики каскадного кода по сравнению с ЛДМ. Однако, как и в случае линейной ДМ, при использовании АДМ сверточный перемежитель оказывается более помехоустойчивым по сравнению с другими.

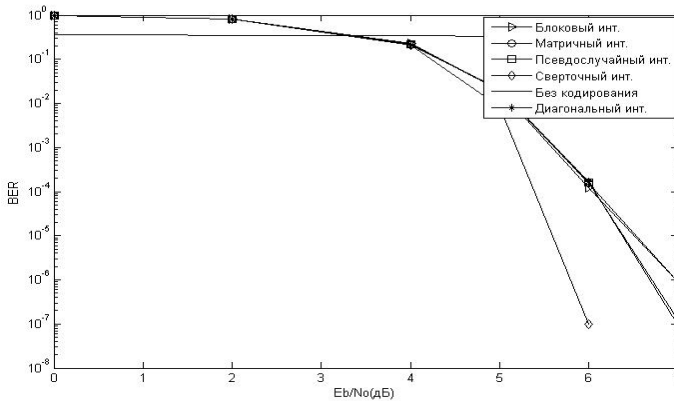


Рис.13. Зависимости BER для АДМ, 2ФМн с различными перемежителями

Дальнейшие исследования уже с КАМ-64 показали, что BER при 2ФМн меньше, чем при КАМ-64. Это следовало ожидать, поскольку при многопозиционной модуляции помехозащищенность хуже, чем при двухпозиционной. Только сверточный перемежитель обеспечивает BER, сравнимую с 2ФМн.

Для сравнения различных методов при КАМ-64 получены аналогичные зависимости, приведенные на рис. 14.

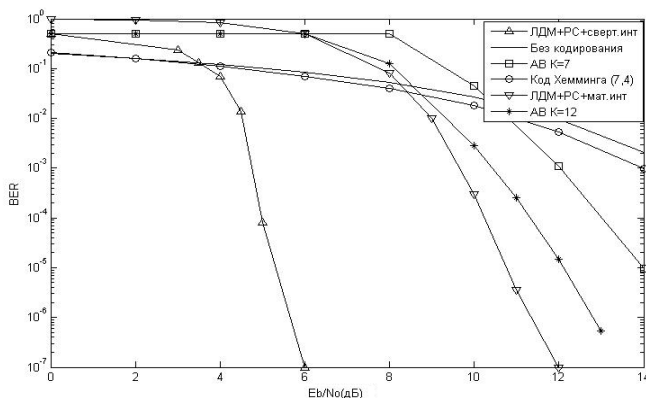


Рис. 14. Сравнение различных методов кодирования при КАМ-64

Из сопоставления графиков на рис. 14 следует, что даже при использовании матричного перемежителя, разработанная кодовая конструкция дает выигрыш почти в 3 дБ при вероятности появления ошибочных битов 10^{-6} по сравнению со сверточным кодом с конструктивной длиной $K=7$ (вне схемы), а также выигрыш в 1 дБ по сравнению со сверточным кодом с $K=12$ (вне схемы). Отметим, что на рис. 14 конструкция “ЛДМ+РС+сверт. интерливер” оказывается гораздо эффективнее других методов, однако это достигается при глубине перемежения большей 12, что не всегда приемлемо, поскольку это усложняет кодовую конструкцию.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ ДИССЕРТАЦИОННОЙ РАБОТЫ

1. Разработана новая модель многоуровневого кодирования, позволяющая существенно повысить эффективность систем обработки информации и являющаяся на сегодняшний день наиболее полной из всех существующих [13,14,17-20,26].

2. Получены рекуррентные соотношения для моделей телевизионных и речевых сигналов, рассмотренных с единой точки зрения теории линейного предсказания. Выведены формулы для моделирования дельта-модулятора, представленного в виде нелинейной импульсной системы с обратной связью. Получены соотношения для синтеза цифровых фильтров нижних частот с переменными частотами среза и дискретизации [1-5,9,12].

3. Установлено, что погрешность среднего значения при формировании гауссовского стационарного случайного процесса наиболее распространенными методами составляет два и более порядка [6].

4. С помощью выведенных уравнений проведен расчет необходимого объема выборки при моделировании для речевого и телевизионного сигналов. Расчеты показали, что при различных заданных точностях моделирования и частотах дискретизации необходимые объемы выборки для этих сигналов изменяются от нескольких тысяч до сотен тысяч [9].

5. Получены такие вероятностные характеристики сигналов в различных точках систем с дельта-модуляцией, как корреляционные функции и распределения пачек символов дельта-потока для стационарного и нестационарного речевого сигнала, что дает возможность учитывать влияние помех в канале связи [7,29].

6. Показано, что методы уменьшения дисперсии с дополняющей переменной сокращают затраты машинного времени от двух до четырех раз и увеличивают точность результатов расчета параметров системы с дельта-модуляцией [8].

7. Установлено, что в процессе машинной оптимизации систем связи с адаптивной дельта-модуляцией необходимо учитывать случайный характер целевой функции, обусловленный использованием метода статистических испытаний [8].

8. Обобщены методика и особенности построения циклических кодов, основанные на их полиномиальном представлении. Рассмотрены этапы технической реализации систематических и несистематических кодеров и составлены их общие функциональные схемы [15,27].

9. Дано математическое описание процедуры кодирования-декодирования кодов Рида-Соломона, на основании чего предложена обобщенная функциональная схема декодера, где показаны все этапы декодирования. Развита способ проверки безошибочного декодирования кодов Рида-Соломона [25, 28].

10. Выведены уравнения для двух типов умножителей в конечных полях, на основе которых разработаны их принципиальные схемы, обеспечивающие снижение сложности реализации [16].

11. Разработаны программы моделирования в среде LabVIEW, с помощью которых исследованы коды Без Возврата к Нулю, с Возвратом к Нулю, с Чередуемостью Полярностей Импульсов, манчестерские, что дает возможность выбора соответствующего кода для системы обработки информации [10,11,24].

12. Создана компьютерная модель предложенной кодовой конструкции, с помощью которой исследованы два вида дельта модуляции, кодер Рида-Соломона, пять типов перемежителей, два типа цифровых модуляторов и канал связи с Аддитивным Гауссовским Белым Шумом, на основании чего получены следующие результаты [18-23]:

- применение сверточного перемежителя в составе каскадной конструкции позволяет получить выигрыш отношения E_b/N_0 примерно в 1,5 дБ по сравнению с другими перемежителями при $BER=10^{-6}$, что при сегодняшних жестких требованиях к мощности передаваемого сигнала является осязаемым результатом. Однако это достигается при глубине перемежения более 12, что не всегда приемлемо и усложняет кодовую конструкцию;

- блочный, матричный и диагональный блочный перемежители несколько уступают сверточному. Однако, если учесть сложность реализации, то эти перемежители можно также рекомендовать для предложенной кодовой конструкции;

- псевдослучайный перемежитель намного сложнее предыдущих, однако его характеристики в каскадной конструкции не уступают блочному перемежителю.

13. Выявлено, что даже при использовании матричного перемежителя разработанная кодовая конструкция дает выигрыш почти в 3 дБ при $BER=10^{-6}$ по сравнению со сверточным кодом с $K=7$ (вне каскадной схемы), а также выигрыш в 1 дБ по сравнению со сверточным кодом с $K=12$ (вне сложной схемы). Разработанная

кодированная конструкция эффективнее декодера для самоортогонального кода и дает выигрыш в отношении сигнал/шум на бит 2 дБ [22].

14. Показано, что в предложенной кодовой конструкции вероятность ошибочных битов в 10^{-6} достигается при отношении E_b/N_0 , равном примерно 6...7 дБ, что сопоставимо с многопороговым декодером самоортогонального кода с кодовой скоростью $r = 1/3$, который в последние годы считается одним из эффективных [22].

Содержание диссертации отражено в следующих работах:

1. Гомцян О.А. Вопросы моделирования систем с дельта-модуляцией // Техника средств связи. Сер. ТРС. -1979. - Вып.1. - С. 34-41.
2. Гомцян О.А. Машинное исследование некоторых характеристик линейной дельта-модуляции // В кн: Дистанционные и информационно-измерительные системы. - М.: Атомиздат, 1980. - С. 294-303.
3. А.с. №853660 (СССР). Устройство для магнитной записи цифровой информации/ М.В.Гитлиц, Ю.В.Скалин, О.А.Гомцян. - Заявл.12.12.79; опубл. 07.08.81 в "Бюллетене изобретений и товарных знаков". - 1981. - №29. - С. 234.
4. А.с. №853659 (СССР). Устройство для воспроизведения с носителя магнитной записи/ М.В.Гитлиц, Ю.В.Скалин, О.А. Гомцян. - Заявл.12.12.79; опубл. 07.08.81 в "Бюллетене изобретений и товарных знаков". - 1981. - №29. - С. 234.
5. Гомцян О.А, Енгибарян Г.Н. Синтез цифровых фильтров для обработки речевых сигналов // В кн: Автоматическое распознавание слуховых образов. АРСО-11. - Ереван, 1980. - С. 105-107.
6. Гомцян О.А, Ризкин И.Х. К оценке погрешности цифрового моделирования сигналов и шумов в радиотехнических системах // Радиотехника и электроника. - 1982.- Т.27, №7. - С.1428-1431.
7. Венедиктов М.Д., Гомцян О.А., Златкин Б.Ш., Монастырский В.Л. Моделирование структуры двоичного ДМЦИК сигнала // Техника средств связи. Сер. ТРС. - 1983.- Вып. 1.- С. 3-20.
8. Вольнский В.А., Гомцян О.А., Буравин А.Е., Ризкин И.Х. Опыт машинной оптимизации систем связи с адаптивной дельта-модуляцией // Электронное моделирование. - 1984.- Т.6, №6.- С. 27-31.
9. Гомцян О.А., Харченко Л.И. Объем выборки при моделировании цифровых систем передачи // Сборник научных трудов учебных институтов связи.- Л.: ЛЭИС, 1985. - С. 37-44.
10. Багдасарян О.В., Гомцян О.А., Мегаворян Д.М. Кодирование линейных сигналов цифровых волоконно-оптических систем связи // Известия НАН РА и ГИУА. Сер. ТН. -1998.- Т.51, №2. - С. 216-221.
11. Багдасарян О.В., Гомцян О.А., Мегаворян Д.М. Современные методы кодового разделения каналов в системах волоконно-оптической связи // Известия НАН РА и ГИУА. Сер. ТН. - 1998. - Т.51, №1. - С. 93-98.
12. Багдасарян О.В., Гомцян О.А., Мегаворян Д.М. Компьютерная модель системы МДКР с адаптивной дельта-модуляцией // Известия НАН РА и ГИУА. Сер. ТН. - 1999.- Т.52, №2. - С. 229-232.

13. Gomtsyan H.A. Computer simulation of cascade codes for CDMA systems // Proceedings of the Second International Symposium of Trans Black Sea. Region on Applied Electromagnetism. - Xanti, Greece. - June 2000. - P.105.
14. Gomtsyan H.A. Encoding Methods for the Fiber Optical Communication and Storage Systems // 5th International Conference on Transparent Optical Networks -ICTON 2003, June 29-July 3, Conference Proceedings.- Poland, 2003.- We.P.13.- P. 133 - 136.
15. Гомцян О.А. Техническая реализация циклических кодов // Годичная научная конференция ГИУА: Сборник материалов. – Ереван, 2004. - Т.2. - С. 541-545.
16. Gomtsyan H.A. Combinational logic multiplier in $GF(2^8)$ // Труды Международного конгресса “Коммуникационные технологии и сети. - М, 2004. - С. 139-142.
17. Գոմցյան Հ.Ա., Բադալյան Բ.Ֆ. Կասկադային կոդավորող համակարգ // ՀՊՃՀ տարեկան գիտաժողով: Նյութերի ժողովածու.-Երևան, 2006.- Հ.2. - էջ 530-532:
18. Գոմցյան Հ.Ա., Բադալյան Բ.Ֆ. Կասկադային կոդեր // ՀՊՃՀ Լրաբեր-75: Գիտական և մեթոդական հոդվածների ժողովածու. - Երևան, 2008.- Հ.2. - էջ 522-525:
19. Гомцян О.А., Бадалян Б.Ф. Сложные кодирующие системы // Известия НАН РА и ГИУА. Серия ТН.- 2009.- Т.62, №4.- С. 451-455.
20. Гомцян О.А, Бадалян Б.Ф. Об одном способе построения составного кода // Вестник ГИУА: Сборник научных и методических статей. - 2010. - Т.2, №1. - С. 194-198.
21. Бадалян Б.Ф., Гомцян О.А. Эффективность каскадных и итеративных методов коррекции ошибок // Вестник ГИУА: Сборник научных и методических статей. - 2011.- Т.3, №1. - С. 200-203.
22. Бадалян Б.Ф., Гомцян О.А. Эффективные системы помехоустойчивого кодирования для цифровой связи // Вестник ГИУА: Сборник научных статей. - 2012.- Ч.1. - С. 216-220.
23. Гомцян О.А., Бадалян Б.Ф. О вычислительной сложности некоторых алгоритмов помехоустойчивого кодирования // Вестник ГИУА: Сборник научных статей. -2013.- Ч.1. - С. 303-308.
24. Գոմցյան Հ.Ա., Բադյան Բ.Ս. Թվային կապի համակարգերի գծային կոդերի մոդելավորում // Հայ-Ռուսական (Սլավոնական) Համալսարանի Ութերորդ տարեկան գիտաժողով. Գիտական հոդվածների ժողովածու. - Երևան, 2014. - էջ 43-46:
25. Гомцян О.А. Об одном методе проверки безошибочного декодирования кодов Рид-Соломона // Вестник Инженерной академии Армении: Сборник научно-технических статей. - 2015. - Т.12, №4.- С. 723-729.
26. Гомцян О.А. Обобщенная концепция каскадного кодирования в цифровых системах обработки информации // Известия НАН РА и ГИУА. Сер. ТН.- 2016.- Т.69, №1.- С. 42-47.
27. Гомцян О.А. Методы формирования блочных циклических кодов // Вестник НПАУ. Сер. “Информационные технологии, электроника, радиотехника”.- 2016.- №1.- С. 85-93.
28. Арзуманян А.Г., Севоян О.Ж., Гомцян О.А. Синхронная система обработки и передачи данных с привязкой к шкале единого мирового времени // Известия вузов России. Радиоэлектроника.- СПб.,СПбГЭТУ “ЛЭТИ”.- 2016.- Вып. 1.- С. 3-7.

29. Гомцяи О.А. Моделирование распределения числа символов двоичного сигнала дельта-модуляции // Известия вузов России. Радиоэлектроника.- СПб., СПбГЭТУ “ЛЭТИ”.- 2016.- Вып. 4. - С. 7-10.

ԱՄՓՈՓԱԳԻՐ

1. Մշակվել է բազմակասկադ կողավորման նոր մոդել, որը հնարավորություն է տալիս էապես բարձրացնել ինֆորմացիայի մշակման համակարգերի արդյունավետությունը և հանդիսանում է այժմ գոյություն ունեցողներից ամենաամբողջականը [13,14,17-20,26]:

2. Ստացվել են հեռուստատեսային և ձայնային ազդանշանների մոդելների համար ռեկուրենտ հարաբերակցություններ՝ դիտարկված գծային կանխատեսման տեսության միասնական տեսանկյունից: Դուրս են բերվել բանաձևեր դելտա-մոդուլյարարի մոդելավորման համար, որը ներկայացվել է հետադարձ կապով ոչ գծային իմպուլսային համակարգի տեսքով: Ստացվել են ցածր հաճախականությունների թվային գոյիչների դիսկրետացման և կտրման փոփոխական հաճախականություններով սինթեզի հարաբերակցություններ [1-5,9,12]:

3. Հաստատվել է, որ Գաուսյան ստացիոնար պատահական պրոցեսի ձևավորման ժամանակ միջին արժեքի սխալանքը ամենաշատ տարածված մեթոդներով կազմում է երկու կարգ և ավելին [6]:

4. Դուրս բերված հավասարումների միջոցով կատարվել է ձայնային և հեռուստատեսային ազդանշանների համար ընտրանքի անհրաժեշտ ծավալի հաշվարկ: Հաշվարկները ցույց են տվել, որ մոդելավորման տրված տարբեր ճշտությունների և դիսկրետացման հաճախականությունների դեպքում այդ ազդանշանների համար ընտրանքի անհրաժեշտ ծավալը փոփոխվում է մի քանի հազարից մինչև հարյուր հազարներ [9]:

5. Ստացվել են դելտա-մոդուլացմամբ համակարգի տարբեր կետերում ազդանշանների այնպիսի հավանականային բնութագրեր, ինչպիսիք են կոռելյացիոն ֆունկցիաները և սիմվոլների փաթեթների դելտա-հոսքի բաշխումը ստացիոնար և ոչ ստացիոնար ձայնային ազդանշանների դեպքում, որը հնարավորություն է տալիս հաշվի առնել աղմուկների ազդեցությունը կապուղում [7,29]:

6. Ցույց է տրվել, որ լրացուցիչ փոփոխականով դիսպերսիայի նվազեցման մեթոդների դեպքում մեքենայական ժամանակը կրճատվում է երկուսից մինչև չորս անգամ, և մեծանում է դելտա-մոդուլացմամբ համակարգի պարամետրերի հաշվարկի արդյունքների ճշտությունը [8]:

7. Հաստատվել է, որ աղապստիվ դելտա-մոդուլացմամբ կապի համակարգի մեքենայական օպտիմալացման ընթացքում անհրաժեշտ է հաշվի առնել նպատակային ֆունկցիայի բնույթը՝ պայմանավորված վիճակագրական փորձարկումների մեթոդի կիրառմամբ [8]:

8. Ընդհանրացվել են ցիկլային կոդերի կառուցման մեթոդիկան և առանձնահատկությունները՝ հիմնված դրանց բազմանդամային ներկայացման

վրա: Դիտարկվել են ցիկլային սիստեմատիկ և ոչ սիստեմատիկ կոդերների տեխնիկական իրականացման փուլերը և կազմվել են դրանց ընդհանուր ֆունկցիոնալ սխեմաները [15,27]:

9. Տրվել են Ռիդ Սոլոմոն կոդերի կոդավորման-ապակոդավորման գործընթացի մաթեմատիկական նկարագրությունը, դրա հիման վրա առաջարկվել է դեկոդերի ընդհանրացված ֆունկցիոնալ սխեմա, որտեղ ցույց են տրվել ապակոդավորման բոլոր փուլերը: Գարգացվել են Ռիդ Սոլոմոն կոդերի անսխալ ապակոդավորման ստուգման միջոցները [25,28]:

10. Դուրս են բերվել հավասարումներ վերջավոր դաշտերում երկու տիպի բազմապատկիչների համար, որոնց հիման վրա մշակվել են այդ բազմապատկիչների պարզ սկզբունքային սխեմաներ՝ ապահովելով իրականացման դժվարությունների նվազեցում [16]:

11. Մշակվել են LabView միջավայրում մոդելավորման ծրագրեր, որոնց օգնությամբ ուսումնասիրվել են BBH (առանց զրոյի վերադարձի), BH (զրոյի վերադարձով), ЧПН (իմպուլսների բևեռականության հերթափոխությամբ), մանչեստերական կոդերը, ինչը հնարավորություն է տալիս ընտրել համապատասխան կոդը ինֆորմացիայի մշակման համակարգի համար [10,11,24]:

12. Ստեղծվել է առաջարկվող կոդային կառուցվածքի համակարգչային մոդելը, ինչի օգնությամբ հետազոտվել են դելտա-մոդուլացման երկու տեսակ, Ռիդ Սոլոմոն կոդավորիչներ, կոդախառնիչների հինգ տիպ, թվային մոդուլարարների երկու տեսակ և ադիտիվ Գաուսյան սպիտակ աղմուկներով կապուղի, որոնց հիման վրա ստացվել են հետևյալ արդյունքները. [18-23]

- փաթեթային կոդախառնիչի կիրառությունը կասկադային կառուցվածքում $BER=10^{-6}$ դեպքում հնարավորություն է տալիս ստանալ E_b/N_0 հարաբերության շահում մոտավորապես 1,5դԲ՝ ուրիշ կոդախառնիչների համեմատ, որը հաղորդվող ազդանշանի հզորության նկատմամբ ժամանակակից կոշտ պահանջների դեպքում կարևոր արդյունք է: Սակայն դա ստացվում է կոդախառնումների ավելի քան 12 խորության դեպքում, որը ոչ միշտ է ընդունելի և բարդացնում է կոդային կառուցվածքը,

- բլոկային, մատրիցային և անկյունագծային բլոկային կոդախառնիչները որոշ չափով զիջում են փաթեթայինին: Սակայն եթե հաշվի առնենք իրականացման բարդությունը, այդպիսի կոդախառնիչներ կարելի է առաջարկել նաև նշված կոդային կառուցվածքի համար,

- կեղծ պատահական կոդախառնիչը շատ ավելի բարդ է նախորդներից, սակայն կասկադային կառուցվածքում նրա բնութագրերը չեն զիջում բլոկային կոդախառնիչի բնութագրերին:

13. Բացահայտվել է, որ նույնիսկ մատրիցային կոդախառնիչի օգտագործման դեպքում մշակված կոդային կառուցվածքը տալիս է մինչև 3դԲ շահում՝սխալ բիթեր հայտնվելու 10^{-6} հավանականության դեպքում $K=7$ (կասկադային

սխեմայից դուրս) կառուցվածքային փաթեթային կողի համեմատությամբ, 1դԲ լավացում՝ $K=12$ (բարդ սխեմայից դուրս) փաթեթային կողի համեմատ: Մշակված կողային կառուցվածքն ավելի արդյունավետ է ինքնաօրթոգոնալ կողի ապակողավորիչից և հնարավորություն է տալիս ազդանշան/աղմուկ հարաբերությունում շահել 2դԲ ամեն բիթի համար [22]:

14. Ցույց է տրվել, որ առաջարկվող կողային կառուցվածքում սխալ բիթեր հայտնվելու 10^{-6} հավանականությունը ստացվում է E_b/N_0 հարաբերության մոտ 6...7դԲ արժեքի դեպքում և համեմատելի է $r=1/3$ կողային արագություն ունեցող ինքնաօրթոգոնալ կողի բազմաշեմային ապակողավորիչի հետ, որը վերջին տարիներին համարվում է ամենաարդյունավետներից մեկը [22]:

HOVHANNES AVAG GOMTSYAN

MODELS AND METHODS OF CASCADE CODING CONSTRUCTIONS AND MODULATION IN INFORMATION PROCESSING DIGITAL SYSTEMS

SUMMARY

1. A new model of multi-level encoding is developed, which greatly improve the efficiency of information processing systems, and which is the most complete of all the existing ones at present [13,14,17-20,26].
2. The recurrence relations for models of television and speech signals, are considered from a unified point of view of the linear prediction theory. The formulas for the delta- modulator simulation presented in the form of the nonlinear pulse systems with a feedback are derived. Relations for the synthesis of digital low-pass filters with variable cut-off and sampling frequencies are obtained [1-5,9,12].
3. It is determined that the error of the mean value at the formation of a Gaussian stationary random process, using the most common methods is two orders and more [6].
4. Using the obtained equations, the calculation of the required sample volume in modeling for voice and television signals is held. Calculations have shown that for a given different accuracy of modelling and sampling rates necessary sample volume for these signals vary from a few thousand to hundreds of thousands [9].
5. Probabilistic characteristics of the signals in various points of systems with delta modulation (DM) such as correlation functions and distribution of symbol packets of delta stream for stationary and nonstationary speech signals are obtained, that gives an opportunity to consider the impact of noises in communication channel [7,29].
6. It is shown that the methods of reducing the dispersion with a complementary variable reduce the calculation time from two to four times, and increase the accuracy of the calculation results of the system parameters with a delta modulation [8].
7. It is determined that during computer optimization of the adaptive DM communication systems, it is necessary to consider the random nature of the objective function conditioned by the use of the statistical testing method [8].
8. The method and design features of cyclic codes based on their polynomial representation are generalized. The stages of the technical implementation of systematic and non-systematic encoders are considered and their common functional schemes are compiled [15,27].

9. The mathematical description of the Reed Solomon code encoding-decoding procedure is given, based on which, a generalized functional diagram of a decoder, showing all steps of decoding. A way of verifying an error-free decoding of RS codes is developed [25,28].

10. Equations for two types of multipliers in finite fields are derived based on which, the principle schemes of those multipliers are developed that provide reduced complexity of implementation [16].

11. Simulation programs in the LabVIEW environment are developed through which the NRZ, RZ, AMI, Manchester codes are investigated, which gives the possibility of selecting the appropriate code for the information processing system [10,11,24].

12. A computer model of the proposed code structure with which two types of DM, the RS coder, five types of interleavers, two types of digital modulators and a communication channel with Additive Gaussian White Noise are investigated, whereby the following results were obtained [18-23]:

- the application of a convolutional interleaver as a part of cascade construction provides a gain in the E_b/N_0 ratio about 1.5 dB compared with other interleavers at $BER = 10^{-6}$, which in case of today's stringent requirements set the power of the transmitted signal is a tangible result. However, this result is achieved at interleaving the depth of more than 12, which is not always acceptable and complicates the code construction;
- block, matrix and diagonal matrix interleavers are somewhat inferior to the convolutional one. However, given the complexity of the implementation, these interleavers may also be recommended for the design of the proposed code construction;
- the pseudo-random interleaver more complex than the previous ones, but its characteristics are not inferior to the block interleaver in the cascade construction.

13. It is revealed that even when using a matrix code, the developed code construction gives a gain of almost 3 dB at a probability of bit-error rates of 10^{-6} compared to the convolutional code with a constraint length $K=7$ (outside the cascade scheme), as well as a the gain in 1 dB compared to the convolutional code with $K=12$ (outside the complex scheme). The developed code construction is much more efficient than the decoder for the self-orthogonal code and allows to win 2 dB in the signal/noise ratio [22].

14. It is shown that in the proposed code construction the $BER=10^{-6}$ is achieved when the ratio E_b/N_0 is nearly equal to 6.7 dB, which is comparable to a self-orthogonal code decoder with a code rate $r=1/3$ which is one of the effective ones in recent years [22].

