На правах рукописи

Трифонов Петр Владимирович

Адаптивное кодирование в многочастотных системах

05.13.01 — Системный анализ, управление и обработка информации (информатика)

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата технических наук

Санкт-Петербург — 2005

Работа выполнена в Государственном образовательном учреждении высшего профессионального образования “Санкт-Петербургский государственный политехнический университет”.

Научный руководитель: доктор технических наук, профессор Крук Евгений Аврамович.

Официальные оппоненты:
доктор технических наук, профессор Колесник Виктор Дмитриевич
кандидат технических наук, доцент Алмазова Вера Сергеевна

Ведущая организация: Санкт-Петербургский институт информатики и автоматизации РАН

Защита состоится 26 мая 2005 г. в 16-00 часов на заседании диссертационного совета Д 212.229.18 ГОУ ВПО “Санкт-Петербургский государственный политехнический университет” по адресу: 195251 Санкт-Петербург, Политехническая ул. 29, 9-й учебный корпус, аудитория 325.

С диссертацией можно ознакомиться в библиотеке ГОУ ВПО “Санкт-Петербургский государственный политехнический университет” по адресу: 195251, г. Санкт-Петербург, Политехническая ул., 29.

Автореферат разослан 25 апреля 2005 г.

Ученый секретарь диссертационного совета В.Н. Шашихин

Общая характеристика работы

Актуальность темы. Бурное развитие микроэлектроники, имевшее место в конце 20 века, создало возможность для реализации сложных высокопроизводительных вычислительных систем, используемых в настоящее время практически во всех отраслях народного хозяйства. Это в свою очередь потребовало организации взаимодействия этих систем, причем с ростом их производительности растут требования к скорости и качеству связи между ними. Для эффективного функционирования подобных систем необходим точный учет текущего состояния среды передачи данных. По мере его изменения необходимо осуществлять подстройку параметров системы связи с целью минимизации мощности передатчика, требуемой для поддержания заданного качества связи. Таким образом, возникает задача управления параметрами передатчика. Несмотря на то, что в теории информации были построены решения для этой задачи, их нельзя признать удовлетворительными с практической точки зрения. Причиной этого является оптимизационный критерий, используемый в подобных теоретико-информационных исследованиях, а именно максимизация суммарной (или взвешенной) пропускной способности всех пользователей системы. Это не позволяет учесть ограничений, связанных как с невозможностью достижения пропускной способности канала с помощью существующих методов передачи информации, так и с необходимостью поддержания определенного качества обслуживания отдельных пользователей системы. В связи с этим возникает необходимость разработки алгоритмов адаптивной передачи, учитывающих вышеприведенные ограничения. При этом использование многочастотного метода передачи, получившего широкое распространение в последние годы, позволяет существенно упростить реализацию соответствующих оптимизационных алгоритмов, а также допускает использование при анализе системы достаточно простых математических моделей.

Построение адаптивной системы передачи данных требует наличия нескольких методов кодирования и модуляции, обеспечивающих различную степень защиты передаваемых данных от помех. При этом особую важность имеет эффективная реализация используемых методов обработки информации, в частности кодирования и декодирования корректирующих кодов. Алгоритмы кодирования и декодирования многих корректирующих кодов включают в себя классические вычислительные примитивы, такие как циклическая свертка, поиск корней многочлена, дискретное преобразование Фурье и т.п. При этом в большинстве случае вычисления производятся в конечных полях. Несмотря на то, что известны быстрые алгоритмы решения указанных задач, во многих случаях их непосредственное использование при реализации алгоритмов кодирования и декодирования оказывается крайне неэффективным как в силу специфики вычислений в конечных полях, так и в силу ограничений, накладываемых структурой алгоритмов кодирования и декодирования. В связи с этим возникает задача эффективной реализации соответствующих вычислительных алгоритмов.

Целью данной диссертационной работы является построение методов оптимизации

параметров кодирования в многочастотных системах, позволяющих снизить мощность передатчика, требуемую для достижения заданного качества работы системы. В рамках работы решаются следующие задачи:

1. Разработка методов настройки параметров помехоустойчивого кодирования, модуляции, разделения канала и распределения мощности в зависимости от текущего состояния физического канала связи.

2. Эффективная реализация соответствующих процедур обработки информации при кодировании и декодировании данных.

Предметом исследования являются оптимизация параметров схемы передачи данных в многочастотных системах, а также алгоритмы обработки информации, применяемые при кодировании и декодировании корректирующих кодов, используемых в подобных системах.

В данной работе используются **методы** теорий цифровой связи, условного экстремума, помехоустойчивого кодирования, чисел и коммутативной алгебры.

Достоверность полученных результатов обеспечена сопоставлением результатов теоретического анализа и имитационного моделирования, а также наличием программной реализации всех предложенных методов.

Научные результаты и их новизна:

1. Построен циклотомический алгоритм быстрого преобразования Фурье (БПФ) над конечными полями, на основе которого разработан метод вычисления вектора синдрома при классическом декодировании кодов Рида-Соломона. Данные алгоритмы обладают наименьшей сложностью среди известных аналогов.

2. Разработан метод оптимизации разделения канала, распределения мощности и скорости передачи в многопользовательских многочастотных системах вещания, позволяющий получить существенный (около 5 дБ) энергетический выигрыш по сравнению с известными методами.

3. Предложен метод адаптивной передачи в многочастотных системах на основе многоуровневого кодирования, позволяющий повысить точность адаптации по сравнению с существующими методами, что приводит к снижению требуемой мощности передатчика на 2 дБ по сравнению с существующими методами.

4. Разработан метод быстрого нахождения корней многочлена локаторов ошибки при классическом декодировании кодов Рида-Соломона, обеспечивающий снижение сложности одного из этапов декодирования в 2 – 6 раз по сравнению со стандартными методами.

5. Предложен метод двумерной интерполяции при списочном декодировании кодов Рида-Соломона, позволяющий построить параллельную реализацию вычислительно наиболее сложного шага алгоритма Гурусвами-Судана.

Практическая ценность работы состоит в разработке методов адаптивной передачи в одно- и многопользовательских системах, позволяющих существенно снизить требуемую мощность передатчика, а также методов декодирования некоторых классов кодов, исправляющих ошибки, со сложностью, существенно меньшей по сравнению со стандартными методами. Предложенный метод адаптивной передачи в однопользовательских

системах при использовании кодов длины 3200 обеспечивает функционирование системы при вероятности ошибки на бит порядка 10^{-7} на отношении сигнал/шум, превышающем предел Шеннона всего на 3 децибела. Данный метод может быть также использован и в многопользовательских системах. Предложенный метод адаптивной передачи в многопользовательских системах на основе кодового разделения позволяет снизить мощность передатчика, требуемую для достижения заданных параметров работы системы, на 5 дБ по сравнению с наилучшим известным автору методом, использующим частотное разделение. Предложенный метод нахождения корней многочленов над конечным полем обладает наименьшей сложностью среди известных аналогов. Предложенный алгоритм БПФ имеет наименьшую сложность среди известных алгоритмов на длине по крайней мере до 512 и позволяет построить алгоритмы вычисления синдрома при классическом декодировании кодов Рида-Соломона, обладающие наименьшей сложностью среди известных методов.

Публикации и апробация работы. Предложенные методы были опубликованы в журналах IEEE Transactions on Communications [6], Проблемы передачи информации [3], European Transactions on Telecommunications [4, 7], Информационно-управляющие системы [1], в трудах конференций IEEE International Symposium on Information Theory [8], IEEE Vehicular Technology Conference [10], International OFDM Workshop [9], XXXI Недели Науки СБбГПУ [2].

Прикладная реализация работы.

По материалам диссертации получен Европейский патент [5].

Материалы диссертационной работы внедрены в учебный процесс кафедры “Распределенные вычисления и компьютерные сети” СПбГПУ и разработки АО ”Институт информационных систем и технологий”. Указанные внедрения подтверждены соответствующими актами.

Структура и объем работы. Диссертация состоит из введения, четырех глав, заключения и списка литературы, включающего 176 наименований. Материал работы изложен на 147 страницах машинописного текста, основное содержание на 130 страницах. Работа содержит 39 рисунков и 7 таблиц.

Содержание работы

Во введении обоснована актуальность темы диссертационной работы; сформулирована цель и поставлены задачи проводимых исследований; определены научная новизна и практическая значимость выполненных изысканий; приведены сведения о публикациях и апробации полученных результатов, структуре диссертации; раскрыто краткое содержание глав работы.

В первой главе приведен обзор некоторых методов передачи и обработки информации на физическом уровне современных телекоммуникационных систем, используемых в последующих главах диссертационной работы. Приведены основные теоретико-информационные результаты, связанные с управлением параметрами передатчиков телекоммуникационных систем, а также описаны некоторые практические приемы реализации адаптивной передачи. В результате их сравнительного анализа выявлены возможности по совершенствованию алгоритмов адаптивной передачи.

Показано, что для эффективного осуществления передачи данных в как в одно-, так и в многопользовательских многочастотных системах необходима адаптация используемой схемы передачи к текущему состоянию частотно-селективного канала. Управление параметрами схемы передачи должно осуществляться на основе классического “правила водонаполнения” или его модификаций на случай многопользовательских систем. Практическая реализация этого правила приводит к необходимости использования дискретных скоростей передачи, что требует некоторого увеличения мощности сигнала по сравнению с идеальным решением оптимизационной задачи. Таким образом, можно ожидать повышения эффективности адаптивной системы в случае использования набора схем кодирования/модуляции с малым шагом скоростей, что может быть реализовано на основе концепции многоуровневого кодирования.

В случае многопользовательских систем вещания обеспечение фиксированной скорости передачи данных для каждого из пользователей может потребовать совместного использования подканалов для передачи данных нескольким абонентам, что требует разработки соответствующих оптимизационных алгоритмов.

Использование корректирующих кодов требует эффективной реализации соответствующих вычислительных алгоритмов. В частности, при классическом декодировании кодов Рида-Соломона наиболее трудоемкими этапами являются вычисление вектора синдрома и поиск корней многочлена локаторов ошибок, а при списочном декодировании с помощью алгоритма Гурусвами-Судана — двумерная интерполяция. Несмотря на то, что известны быстрые алгоритмы решения этих задач в общем случае, они оказываются неэффективны при использовании в декодерах корректирующих кодов как в силу специфики вычислений в конечных полях, так и в силу ограничений, накладываемых алгоритмами декодирования. Таким образом, возникает возможность снижения сложности декодирования путем построения специализированных вычислительных алгоритмов.

В результате проведенного анализа современного состояния области адаптивной пе-

редачи и вычислительных алгоритмов помехоустойчивого кодирования сформулирована цель и поставлены задачи диссертационной работы.

Вторая глава посвящена построению адаптивных методов передачи для однопользовательских и многопользовательских систем.

Рассмотрение проблемы адаптивной передачи начинается со случая однопользовательской многочастотной системы. Как известно, принятый сигнал в многочастотных системах может быть представлен как $r_i = \mu_i s_i + \eta_i, i = 1..N$, где s_i — сигнал, переданный по i-му подканалу, η_i — отсчет аддитивного Гауссовского шума с дисперсией σ^2, μ_i — передаточный коэффициент i-го подканала. Каждый подканал может быть охарактеризован своим отношением канал/шум $\xi_i = |\mu_i|^2/\sigma^2$. В соответствии с результатами анализа, выполненного в первой главе, для повышения точности адаптации в подобной системе необходимо наличие большого семейства схем кодирования и модуляции с малым шагом скоростей. Описывается новый прагматический способ построения семейства многоуровневых кодов с указанными свойствами на основе заданного набора компонентных кодов.

Предлагаемая процедура построения многоуровневого кода, использующего M-ичную амплитудную модуляцию и способного функционировать с заданной вероятностью ошибки P_{target} на заданном отношении сигнал/шум γ, состоит из следующих шагов:

1. Для каждого из компонентных кодов $\mathcal{C}_j$ построить теоретически или путем имитационного моделирования кривую $p_j(\gamma)$ вероятности ошибки в зависимости от отношения сигнал/шум при передаче по аддитивному Гауссовскому каналу.

2. Для каждого из имеющихся компонентных кодов $\mathcal{C}_j$ найти отношение сигнал/шум γ_j, обеспечивающее заданную вероятность ошибки, т.е. решить уравнение $p_j(\gamma) = P_{target}$. Это дает отображение $r_j \leftrightarrow \gamma_j$ или $r_j \leftrightarrow C(\gamma_j)$, которое также может быть аппроксимировано некоторой функцией $r(C)$. Здесь $C(\gamma)$ — пропускная способность аддитивного Гауссовского канала при отношении сигнал/шум γ, Примеры аппроксимирующих функций приведены в четвертой главе.

3. Вычислить пропускные способности $C_i, i = 0..l-1$ эквивалентных подканалов M-ичной амплитудной модуляции с помощью стандартных выражений для пропускной способности эквивалентных подканалов в многоуровневом коде.

4. Для каждого из подканалов i найти скорость кода $r(C_i)$, пригодного для использования в качестве компонентного на данном подканале. Для кодирования данных на i-м уровне многоуровневого кода должен использоваться компонентный код из семейства $\{\mathcal{C}_j\}$ с наибольшей скоростью, не превосходящей $r(C_i)$.

Описанная процедура позволяет выбрать для каждого γ набор компонентных кодов, максимизирующих скорость передачи при заданной вероятности ошибки. Ясно, что если имеется возможность использования сигнальных множеств с различным числом уровней M, то для каждого γ может быть выбрано сигнальное множество, обеспечивающее максимальную скорость передачи.

Данный метод построения многоуровневых кодов может рассматриваться как модификация известного правила равных вероятностей ошибки. Действительно, для каждого компонентного кода вероятность ошибки при передаче по аддитивному Гауссовскому каналу однозначно определяется отношением сигнал/шум. С другой стороны, отношение сигнал/шум однозначно характеризует пропускную способность канала, т.е. пропускная способность канала однозначно определяет вероятность ошибки декодирования. Предлагаемый метод основывается на предположении о том, что при переходе от аддитивному

Гауссовскому каналу к эквивалентным подканалам в многоуровневом коде эта зависимость не претерпевает существенных изменений. Основным достоинством предлагаемого метода является простота процедуры построения многоуровневого кода, которая не требует достаточно сложного анализа вероятности ошибки декодирования. Для многих кодов такой анализ практически неосуществим.

Для построения семейства многоуровневых кодов описанная процедура должна быть выполнена для набора значений γ с некоторым достаточно малым шагом Δ. Это позволяет построить большое число многоуровневых кодов на основе сравнительно небольшого семейства компонентных кодов.

Построенное семейство многоуровневых кодов может быть использовано для организации адаптивной передачи на основе классического правила "водонаполнения", используемого во многих известных адаптивных алгоритмах. Новизна предлагаемого метода состоит в использовании большого семейства многоуровневых кодов, обеспечивающего более точную подстройку параметров каждого подканала. При этом большое семейство многоуровневых кодов может быть построено с помощью сравнительно небольшого набора компонентных кодов. В работе рассматривается также способ снижения времени задержки сообщения и сложности оптимизации, состоящий в группировке подканалов с близкими характеристиками в одну подполосу (группу) и отображении каждого кодового слова многоуровневого кода на несколько подканалов, входящих в соответствующую подполосу.

Описывается новый метод аналитического исследования поведения адаптивных многочастотных систем в условиях стохастического канала. Во многих случаях оказывается, что ξ_i являются случайными величинами с некоторым распределением. Наиболее распространенный способ анализа поведения подобных систем состоит в выполнении имитационного моделирования. В работе показано, что переупорядочение подканалов в соответствии с их отношениями канал/шум ξ_i не влияет на характеристики адаптивной системы, но позволяет заменить при анализе случайные величины ξ_i на математические ожидания порядковых статистик $\xi_{i:N}$ для почти всех i. Для систем с большим числом подканалов оказывается, что дисперсия порядковых статистик достаточно мала, вследствие чего погрешность, связанная с такой заменой, незначительна. Для многих практически важных распределений величин ξ_i выражения для математического ожидания порядковых статистик сравнительно просты, что позволяет существенно упростить анализ адаптивных систем. Кроме того, данный метод позволяет исследовать их поведение в области малых отношений сигнал/шум, что соответствует случаю неполного использования ресурсов однопользовательской системы. Приводится пример анализа системы, функционирующей в условиях релеевского канала с независимыми замираниями. Эти результаты используются в дальнейшем при анализе характеристик многопользовательской системы.

Далее в работе рассматривается адаптивная передача в многопользовательских системах. Формулируется задача условной минимизации мощности передатчика в многопользовательской многочастотной системе вещания. Параметрами оптимизационной задачи являются скорости кодирования и модуляции пользователей по отдельным подканалам, коэффициенты усиления сигналов, предназначенных для отдельных пользователей, и параметры разделения каналов. Предполагается, что каждый подканал может одновременно использоваться для передачи данных нескольким пользователям, а их разделение осуществляется во временной или в кодовой области. В случае использования кодового разделения предполагается использование ортогональных расширяющих последовательностей с однопользовательским детектированием. Это позволяет рассматривать временное и кодовое разделение с одинаковых позиций. Кроме того, накладывается требование поддержания фиксированных скоростей передачи данных для отдельных пользователей.

Используется предположение о том, что отношение сигнал/шум, необходимое для передачи данных со скоростью c с использованием имеющегося семейства методов кодирования/модуляции, может быть вычислено с помощью некоторой функции $f(c)$. На функцию накладывается требование выпуклости, монотонного возрастания, а также $f(c) = 0, c \leq 0$. Использование этой функции позволяет найти коэффициент усиления V_{ki} для символов, передаваемых k-му пользователю по i-му подканалу со скоростью c_{ki}, как

$$V_{ki} = \sqrt{f(c_{ki})/\xi_{ki}}, i = 1..N, k = 1..K. \tag{1}$$

Таким образом, оптимизационная задача может быть сформулирована как

$$\min_{c_{ki},\rho_{ki}} \sum_{i=1}^{N} \sum_{k=1}^{K} \frac{\rho_{ki} f(c_{ki})}{\xi_{ki}} \tag{2}$$

с ограничениями

$$R_k = \sum_{i=1}^{N} \rho_{ki} c_{ki} \tag{3}$$

$$1 = \sum_{k=1}^{K} \rho_{ki} \tag{4}$$

$$0 \leq \rho_{ki}. \tag{5}$$

Показывается, что решение оптимизационной задачи должно удовлетворять следующей системе уравнений и неравенств:

$$0 = \left(\beta_i^{(k)} - \beta_i\right) \rho_{ki} \tag{6}$$

$$R_k = \textstyle\sum_{i=1}^{N} \rho_{ki} f'^{-1}(\lambda_k \xi_{ki}) \tag{7}$$

$$1 = \textstyle\sum_{k=1}^{K} \rho_{ki} \tag{8}$$

$$\beta_i \leq \beta_i^{(k)} = \frac{f(f'^{-1}(\lambda_k \xi_{ki})) - \lambda_k \xi_{ki} f'^{-1}(\lambda_k \xi_{ki})}{\xi_{ki}}. \tag{9}$$

Здесь ρ_{ki} — доля i-го подканала, используемая k-м пользователем, R_k — скорость передачи данных k-м пользователем, ξ_{ki} — отношение канал/шум, наблюдаемое k-му пользователю на i-м подканале, λ_k и β_i являются множителями Лагранжа. При этом должно учитываться дополнительное ограничение $\rho_{ki} \in \{0, \frac{1}{S}, \ldots, \frac{S}{S}\}$, где S — длина расширяющей последовательности в случае кодового разделения. Таким образом, $\rho_{ki} S$ задает число расширяющих последовательностей, используемых для передачи данных k-го пользователя на i-м подканале. Ясно, что увеличение S приводит к повышению точности аппроксимации дискретных величин ρ_{ki} непрерывными, принимающими значения из множества $[0; 1]$. Следовательно, точность решения рассматриваемой оптимизационной задачи, получаемого с помощью стандартных методов вариационного исчисления, также будет повышаться с ростом S.

Исследование свойств вышеприведенной системы уравнений и неравенств показывает, что она имеет большое число различных решений. Это приводит к существованию точек в пространстве параметров задачи, в которых матрица Якоби системы уравнений вырождена или плохо обусловлена, что затрудняет использование для ее решения стандартных методов численного анализа. В работе описывается специализированный оптимизационный алгоритм, позволяющий построить приближенное решение описанной задачи:

1. Сформировать начальный набор $\{\rho_{ki}\}$.

2. Вычислить λ_k из (7) и подставить это значение в (9), получив $\beta_i^{(k)}$.

3. Найти наихудший подканал и наихудшего пользователя, назначенного на этот подканал $(i_w, k_w) = \arg\max\limits_{i,k:\rho_{ki}>0}(\beta_i^{(k)} - \beta_i)$, а также наилучшего пользователя $k_b = \arg\min\limits_{k} \beta_{i_w}^{(k)}$.

4. Уменьшить долю ρ_{k_w,i_w} подканала i_w, занимаемую пользователем k_w, на $1/S$ и увеличить долю ρ_{k_b,i_w}, занимаемую пользователем k_b, на эту же величину.

5. Повторять шаги 2 — 4 заданное число раз. Вычисления могут быть прекращены досрочно, если в течение нескольких шагов не происходит уменьшение величины $\Delta = \max\limits_{i,k:\rho_{ki}>0}(\beta_i^{(k)} - \beta_i)$

6. Воспользоваться каким-либо алгоритмом оптимизации однопользовательских многочастотных систем для нахождения распределения мощности передаваемого сигнала и скоростей передачи по подканалам, выделенным каждому из пользователей.

Анализ характеристик описанной многопользовательской многочастотной адаптивной системы существенно более сложен, чем в однопользовательском случае. Рассматривается приближенный метод анализа, основанный на предположении о том, что в оптимизированной системе передача данных каждому из пользователей осуществляется по наилучшим подканалам. При этом допустимость совместного использования подканалов позволяет игнорировать возможность совпадения наилучших подканалов нескольких пользователей. Таким образом, задача анализа многопользовательской системы сводится к анализу однопользовательских систем, что может быть выполнено с привлечением аппарата порядковых статистик (см. выше).

Рассматривается также возможность объединения смежных подканалов в группы (подполосы) размером $S_f : 1 \le S_f \le S, S = S_f S_t$. Показывается, что это приводит к существенному снижению сложности оптимизации и объема передаваемой служебной информации. Но с другой стороны, увеличение S_f приводит к снижению возможностей по адаптации схемы передачи.

Анализируется структура служебной информации, которая должна широковещательно передаваться базовой станцией с целью обеспечения функционирования адаптивного протокола. Показывается, что при наличии достаточно точных оценок состояния канала все пользователи могут восстановить величины V_{ki} с помощью выражения (1). Следовательно, передача величин V_{ki} не требуется. Величины ρ_{ki} могут быть преобразованы в списки подканалов, используемых каждым из пользователей, с указанием числа расширяющих последовательностей, используемых на каждом подканале. Показывается, что объем служебной информации может быть существенно снижен путем использования комбинации дельта-кодирования, кодирования длины пробегов и кодов Хаффмана. При этом использование статических кодов Хаффмана требует также передачи дерева кодирования, которое оказывается сопоставимо по объему с собственно сжатой служебной информацией. Одним из возможных решений данной проблемы является использование заранее построенных деревьев Хаффмана. Однако оказывается, что статистические свойства служебной информации существенно зависят как от параметров канала, так и от параметров системы (числа активных пользователей и их требований к скорости передачи), что приводит к снижению коэффициента сжатия служебной информации. Данная проблема может быть решена

путем использования динамических кодов Хаффмана. Однако их применение связано с определенными сложностями:

1. Объем служебных данных на начальном этапе может существенно превышать средний.

2. Ошибка декодирования служебного блока данных может привести к рассинхронизации таблиц кодера и декодера, что сделает невозможной дальнейшую работу приемника.

3. Подключение нового пользователя к системе затруднено ввиду необходимости синхронизации его таблицы декодирования.

Эти проблемы могут быть решены путем использования комбинации универсальных кодов Хаффмана, а также периодической реинициализации кодера базовой станции и декодеров всех пользователей.

Приведен анализ поведения адаптивной системы в случае наличия стохастических временных изменений состояния канала, характеризуемых моделью Джейкса. Полученные результаты позволяют выбрать длительность временного интервала, в течение которого может использоваться одна и та же оптимизированная схема передачи.

Третья глава посвящена вопросам построения эффективных вычислительных алгоритмов декодирования корректирующих кодов. Проблема рассматривается с точки зрения задачи декодирования кодов Рида-Соломона, заданных над полем $GF(2^m)$, но полученные результаты могут быть применены и для других кодов, использующих аналогичные процедуры декодирования.

Согласно результатам первой главы, наиболее трудоемкими операциями при классическом декодировании кодов Рида-Соломона являются вычисление синдромного многочлена и поиск корней многочлена локаторов ошибок. Обе операции сводятся к вычислению значений некоторого многочлена в наборе точек. Показано, что использование факта существования линеаризованных и аффинных многочленов над полем $GF(2^m)$ позволяет существенно упростить вычисления.

В частности, доказано, что всякий многочлен $f(x) = \sum_{i=0}^{t} f_i x^i, f_i \in GF(2^m)$, может быть разложен на сумму многочленов, кратных аффинным:

$$f(x) = f_3 x^3 + \sum_{i=0}^{\lceil (t-4)/5 \rceil} x^{5i}(f_{5i} + L_i(x)), \tag{10}$$

где $L_i(x) = \sum_{j=0}^{3} f_{5i+2^j} x^{2^j}$ — линеаризованные многочлены, $f_j = 0$ для всех $j > t$. Таким образом, для вычисления значений многочлена во всех точках конечного поля может использоваться следующий алгоритм:

1. Построить таблицы значений линеаризованных многочленов из разложения (10): $L_i^{(k)} = L_i(\alpha^k)$, $k = [0; m-1]$, $i \in [0; \lceil (t-4)/5 \rceil]$, где α — примитивный элемент конечного поля;

2. Произвести инициализацию $A_i^{(0)} = f_{5i}$;

3. Упорядочив все элементы поля $x_j \in GF(2^m)$, $j \in [0; 2^m - 1]$, разложенные в стандартном базисе, в соответствии с кодом Грея, вычислить $A_i^{(j)} = A_i^{(j-1)} + L_i^{(\delta(x_j, x_{j-1}))}, j \in [1; 2^m - 1]$, где $\delta(x_j, x_{j-1})$ указывает координату, в которой x_j отличается от x_{j-1};

4. Вычислить $f(x_j) = f_3 x_j^3 + \sum_{i=0}^{\lceil (t-4)/5 \rceil} x_j^{5i} A_i^{(j)}, j \in [0; 2^m - 1]$. Если $f(x_j) = 0$, x_j является корнем многочлена.

Сложность данного алгоритма равна

$$W_{aff} = m \left\lceil \frac{t+1}{5} \right\rceil (4C_{mul} + 3C_{add}) + \left(\left\lceil \frac{t+1}{5} \right\rceil (2C_{add} + C_{mul}) + 2C_{exp} \right) W, \qquad (11)$$

где W — число обращений к вышеописанной процедуре вычисления значений многочлена, C_{add} — сложность одной операции сложения над конечным полем, C_{mul} — сложность одной операции умножения над конечным полем. Предложены также специализированные разложения многочленов степени 8 и 17, позволяющие несколько снизить требуемое число арифметических операций над конечным полем. Описан гибридный алгоритм поиска корней многочленов над конечным полем, состоящий в последовательном понижении степени многочлена $f(x)$ путем его деления на $(x - x_i)$ для каждого найденного корня x_i. После получения многочлена степени 4 или ниже может быть использован аналитический метод поиска корней. Применение предложенной модификации процедуры Ченя позволяет снизить сложность поиска корней многочленов над конечным полем $GF(2^m)$ в 2 – 6 раз.

Задача вычисления синдрома принятого вектора может рассматриваться как вычисление неполного дискретного преобразования Фурье над конечным полем. Применение свойств линеаризованных многочленов над полем $GF(2^m)$ позволяет построить разложение произвольного многочлена степени $2^m - 1$ на сумму линеаризованных:

$$f(x) = \sum_{i=0}^{l} L_i(x^{k_i}), \quad L_i(y) = \sum_{j=0}^{m_i - 1} f_{k_i 2^j \bmod n} y^{2^j}. \qquad (12)$$

Это дает возможность представить компоненты дискретного преобразования Фурье как $F_j = f(\alpha^j) = \sum_{i=0}^{l} L_i(\alpha^{jk_i})$. Разлагая величины $\beta^j, \beta = \alpha^{k_i}$ в подходящих базисах $\mathcal{B}_i$, можно получить следующее выражение для ДПФ над конечным полем $GF(2^m)$:

$$F = ALf, \qquad (13)$$

где f — переставленный вектор коэффициентов исходного многочлена $f(x)$, L — блочно-диагональная матрица, соответствующая базисам $\mathcal{B}_i$, A — некоторая двоичная матрица. Показано, что выбор в качестве $\mathcal{B}_i$ нормальных базисов подполей $GF(2^m)$ позволяет свести задачу умножения на блоки матрицы L к задаче вычисления набора коротких циклических сверток.

Показана возможность сведения задачи умножения на двоичную матрицы A к задаче декодирования линейного кода с проверочной матрицей $H = (I|A)$. Предложен вычислительный алгоритм, осуществляющий построение разреженного представления матрицы H. Разреженное представление этой матрицы может быть использовано для нахождения произведения $y = Ax$ с помощью итеративного алгоритма декодирования низкоплотностных кодов в двоичном канале со стираниями. Описанный метод позволяет получить весьма эффективные алгоритмы умножения вектора на двоичную матрицу, но оценить их сложность в общем случае не удалось.

В таблице 1 представлена сложность (число умножений и сложений) алгоритма быстрого преобразования Фурье над конечным полем, полученного описанным методом, а также сложность наилучшего известного аналога.

Выражение (13) может быть преобразовано к виду $f = L^{-1}A^{-1}F$. В силу симметрии прямого и обратного ДПФ, это выражение также задает алгоритм быстрого преобразования Фурье, который удобно использовать при вычислении неполного ДПФ. Применение

Таблица 1: Сложность некоторых алгоритмов БПФ

	Метод Захаровой		Предлагаемый метод	
n	N_{mul}	N_{add}	N_{mul}	N_{add}
7	6	26	6	25
15	16	100	16	77
31	60	388	54	315
63	97	952	97	805
127	468	3737	216	2780
255	646	35503	586	7919
511	—	—	1014	26643

этого метода позволило построить алгоритм вычисления синдромного многочлена со сложностью в 8 раз меньшей, чем у стандартного метода, основанного на схеме Горнера.

Была показана возможность преобразования алгоритма вычисления синдрома в разреженный фактор-граф, задающий соответствующий код Рида-Соломона. Это может быть использовано для его мягкого декодирования.

Предложенные вычислительные методы могут быть использованы не только в классическом, но и в списочном декодировании кодов Рида-Соломона. В работе предложен также специализированный вычислительный алгоритм для списочного декодирования кодов Рида-Соломона. Показано, что вычислительно наиболее сложный интерполяционный шаг алгоритма Гурусвами-Судана списочного декодирования кодов Рида-Соломона состоит в нахождении базиса полиномиального модуля, образованного интерполяционными многочленами от двух переменных. Предложен новый алгоритм, состоящий в разбиении множества интерполяционных точек на непересекающиеся подмножества, независимом построении модулей интерполяционных многочленов для этих подможеств и их последующем пересечении. Показана связь операции пересечения полученных таким образом модулей и операции нахождения наименьшего общего кратного матричных полиномов. Показана возможность нахождения пересечения таких модулей с помощью более простого алгоритма перемножения полиномиальных идеалов. Введено понятие производящей функции базиса полиномиального идеала, использование которой позволяет свести задачу перемножения двух нульмерных взаимно простых полиномиальных идеалов к перемножению их производящих функций, что в свою очередь может быть выполнено с помощью классических алгоритмов быстрой линейной свертки многочленов. Применение описанных методов позволяет параллелизовать вычислительно наиболее сложный шаг алгоритма Гурусвами-Судана.

В четвертой главе рассматривается применение предложенных методов адаптивной передачи в широкополосных системах кабельной и радиосвязи. Приводится описание используемых математических моделей стационарного в широком смысле радиоканала с некоррелированными рассеяниями и кабельного канала на основе неэкранированной витой пары.

Приводятся характеристики семейства многоуровневых кодов, построенных на основе низкоплотностных (LDPC) кодов с помощью метода, предложенного во второй главе. Показывается, что использование большого семейства кодов с малым шагом скоростей (82

кода на основе КАМ с диапазоном скоростей от 0,05 до 10) позволяет снизить мощность, требуемую для достижения заданной скорости передачи данных в однопользовательской системе, на 2 дБ по сравнению с системой, использующей только 12 кодов. Исследуется влияние группировки подканалов на качество работы адаптивной системы. Показано, что предложенный метод анализа адаптивных многочастотных систем позволяет получить адекватные результаты даже при наличии статистической зависимости характеристик отдельных подканалов.

В случае адаптивной многопользовательской системы вещания показано, что за счет совместного использования подканалов может быть получен выигрыш до 5 дБ по сравнению с аналогичной системой, в которой каждый подканал используется ровно одним пользователем. Показано, что группировка подканалов в группы (подполосы) приводит к незначительному снижению эффективности адаптивной передачи в случае сильной частотной селективности канала. Показано, что выигрыш от совместного использования подканалов растет с ростом числа одновременно активных пользователей в системе. Сопоставление результатов приближенного анализа, выполненного на основе предложенного метода порядковых статистик, и результатов имитационного моделирования позволяет сделать вывод о том, что ошибка метод порядковых статистик не превышает 1-2 дБ.

Приводятся результаты имитационного моделирования, характеризующие чувствительность предложенного метода адаптивной передачи к неточности оценивания состояния канала. Показано, что выбор $S = S_f$ минимизирует связанное с этим ухудшение характеристик адаптивной системы. Приводятся оценки объема служебной информации после сжатия. Показано, что для системы с 512 подканалами, полосой сигнала 20 МГц и 32 пользователями, осуществляющими передачу со скоростью 160 бит/OFDM символ (т.е. примерно 6,2 Мбит/с) ее объем не превосходит 50 бит на одного пользователя. Из сопоставления этой величины со скоростью передачи пользовательских данных следует, что вся служебная информация может быть передана в рамках одного OFDM-символа.

Основные результаты работы

Основными результатами диссертационной работы являются:

1. Метод поиска корней многочленов над конечным полем, позволяющий снизить сложность соответствующего этапа декодирования кодов Рида-Соломона в 2–6 раз.

2. Метод вычисления быстрого преобразования Фурье над конечным полем, обладающей наименьшей сложностью среди известных аналогов на длинах по крайней мере до 512.

3. Метод построения разреженных фактор-графов линейных кодов и его применение в задаче быстрого умножения матрицы на вектор в полях характеристики два.

4. Метод вычисления синдромного многочлена при декодировании кодов Рида-Соломона, обладающий наименьшей сложностью среди известных аналогичных методов для кодов на длине по крайней мере до 255.

5. Метод вычисления произведения нульмерных взаимно простых полиномиальных идеалов и основывающийся на нем алгоритм интерполяции при списочном декодировании кодов Рида-Соломона.

6. Метод адаптивной передачи с использованием многоуровневого кодирования в многочастотных системах.

7. Метод оценивания пропускной способности векторного Гауссовского канала с независимыми случайными передаточными коэффициентами.

8. Метод адаптивного распределения мощности, скорости и разделения канала в многопользовательских многочастотных системах.

Публикации

[1] *Трифонов П. В.* Адаптивная передача в многопользовательских многочастотных системах вещания // *Информационно-управляющие системы*. — 2005. — Т. 1, № 14. — С. 41–45.

[2] *Трифонов П. В., Федоренко С. В.* Быстрый алгоритм вычисления синдромного многочлена при декодировании кодов Рида-Соломона // XXXI неделя науки СПбГПУ. — Т. 3. — 2002. — С. 189–191.

[3] *Трифонов П. В., Федоренко С. В.* Метод быстрого вычисления преобразования Фурье над конечным полем // *Проблемы передачи информации*. — 2003. — Т. 39, № 3. — С. 3–10.

[4] *Costa E., Fedorenko S. V., Trifonov P. V.* On computing the syndrome polynomial in Reed-Solomon decoder // *European Transactions on Telecommunications*. — 2004. — May/June. — Vol. 15, no. 4. — Pp. 337–342.

[5] *E. Costa, M. Lott, E. Schultz, S. Fedorenko, P. Trifonov, E. Krouk*. Method and device for a communication system for finding roots of an error locator polynomial. — 2003. — European patent EP1367727.

[6] *Fedorenko S. V., Trifonov P. V.* Finding roots of polynomials over finite fields // *IEEE Transactions on Communications*. — 2002. — Vol. 50, no. 11. — Pp. 1709–1711.

[7] *Fedorenko S. V., Trifonov P. V., Costa E.* Improved hybrid algorithm for finding roots of error-locator polynomials // *European Transactions on Telecommunications*. — 2003. — Vol. 14, no. 5.

[8] *Ma J., Trifonov P., Vardy A.* Divide-and-conquer interpolation for list decoding of Reed-Solomon codes // Proceedings of IEEE International Symposium on Information Theory. — 2004. — P. 386.

[9] *Trifonov P., Costa E., Schulz E.* Adaptive user allocation, bit and power loading in multicarrier systems // Proceedings of the 9th International OFDM-Workshop. — 2004.

[10] *Trifonov P., Costa E., Schulz E.* Adaptive multilevel coding in OFDM systems // Proceedings of IEEE Vehicular Technology Conference — Spring 2005. — 2005.