На правах рукописи
УДК 519.725

СЕМЕНОВЫХ
Денис Николаевич

О ТЕОРЕТИКО-ЧИСЛОВЫХ ЗАДАЧАХ В ТЕОРИИ КОДИРОВАНИЯ

01.01.06 - математическая логика, алгебра
и теория чисел
01.01.09 - дискретная математика и
математическая кибернетика

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата
физико-математических наук

Москва
2006

Работа выполнена на кафедре теории чисел механико-математического факультета МГУ им. М.В. Ломоносова

Научный руководитель: кандидат физико-математических наук,
доцент Черепнев Михаил Алексеевич

Официальные оппоненты: доктор физико-математических наук
профессор
Сидельников Владимир Михайлович,
кандидат физико-математических наук
Карпунин Григорий Анатольевич

Ведущая организация: Институт проблем передачи информации РАН

Защита диссертации состоится 13 октября 2006 г. в 16 ч. 20 м. на заседании диссертационного совета Д.501.001.84 в Московском государственном университете им. М.В. Ломоносова по адресу: 119992, ГСП-2, Москва, Ленинские горы, МГУ, Механико-математический факультет, ауд. 14-08.

С диссертацией можно ознакомиться в библиотеке
Механико-математического факультета (Главное Здание, 14 этаж).

Автореферат разослан 13 сентября 2006 г.

Ученый секретарь диссертационного
совета Д.501.001.84 в МГУ,
доктор физико-математических
наук, профессор

В.Н. Чубариков

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Диссертация посвящена некоторым теоретико-числовым вопросам, связанным с теорией кодов, исправляющих ошибки. Затрагиваются коды, представляющие собой линейные подпространства в конечномерном линейном пространстве F_q^n над произвольным конечным полем F_q, и потому называемые линейными.

Актуальность темы. Теория линейных кодов, исправляющих ошибки - это область математики, возникшая и получившая бурное развитие сравнительно недавно - во второй половине XX века. Для получения результатов в этой области активно используются алгебраические, теоретико-числовые и, в последнее время, в связи с возникновением алгеброгеометрических кодов, алгеброгеометрические методы. В данной диссертации затрагиваются некоторые теоретико-числовые задачи, возникающие в теории кодирования. Одна из таких задач связана с построением линейных кодов, исправяющих ошибки, на основе вычетов степени n, $n \in \mathbb{N}$, $n \geq 2$ по модулю простого числа p.

В 1963 году и немного позднее Ассмус и Мэттсон опубликовали цикл работ (например [1] [2]), в которых они дали описание конструкции линейных квадратично-вычетных кодов. А именно, рассмотрим p и l - простые числа, такие, что l является квадратичным вычетом по модулю p. Пространством, в котором будет строиться код, является факторкольцо

$$R_p = F_l[x]/(x^p - 1).$$

Обозначим через Q множество квадратичных вычетов, а через N - множество квадратичных невычетов по модулю p. Найдя поле, содержащее поле F_l, в котором многочлен $x^p - 1$ раскладывается на линейные множители и обозначив через α какой-либо элемент, порождающий циклическую группу корней из единицы степени p в этом поле, будем рассматривать следующие многочлены:

$$q(x) = \prod_{r \in Q}(x - \alpha^r) \qquad \text{и} \qquad n(x) = \prod_{n \in N}(x - \alpha^n).$$

Можно показать, что данные многочлены лежат в $F_l[x]$.

Тогда идеалы $\mathfrak{L} = (q(x))$, $\overline{\mathfrak{L}} = ((x-1)q(x))$, а также $\mathfrak{N} = (n(x))$, $\overline{\mathfrak{N}} = ((x-1)n(x))$ в кольце R_p, порожденные, соответственно, многочленами $q(x)$, $(x-1)q(x)$, $n(x)$, $(x-1)n(x)$, называются квадратично - вычетными кодами.

[1] E.F. Assmus, Jr., H.F. Mattson, Jr., Error-correcting codes: An axiomatic approach, Info. and Control, 6 (1963) 315-330

[2] E.F. Assmus, Jr., H.F. Mattson, Jr., On tactical configurations and error-correcting codes, J. Comb. Theory, 2 (1967) 243-257

Помимо основных определений были получены оценки основных параметров таких кодов - блоковой длины, относительной скорости передачи и кодового расстояния. А именно, была доказано, что параметры квадратично - вычетных кодов удовлетворяют следующим условиям:

длина кода	$n = p$	-выбранное ранее простое число;
размерность кода	$k = \frac{p+1}{2}$	- для кодов $\mathfrak{L}$, $\mathfrak{N}$;
	$k = \frac{p-1}{2}$	- для кодов $\overline{\mathfrak{L}}$, $\overline{\mathfrak{N}}$;
кодовое расстояние	$d \geq \sqrt{p}$.	

Подробное доказательство этого результата можно найти также в книге [3].

Позднее были получены многочисленные интересные свойства описанных выше кодов. В частности, Паттерсон выписал порождающие идемпотенты таких кодов, однако, как утверждают Ф. Мак-Вильямс и Н. Слоэн, этот результат остался неопубликованным. При рассмотрении так называемых расширенных квадратично-вычетных кодов, получаемых из обычных кодов путем добавления проверки на четность, была установлена мощная группа автоморфизмов, относительно действия которой на множестве координатных позиций код является инвариантным. Эта группа обозначается $PSL_2(p)$ и является множеством всех подстановок вида

$$y \to \frac{ay+b}{cy+d}, \qquad a,b,c,d \in GF(p), \qquad ad-bc=1.$$

Наличие большой группы автоморфизмов позволяет применять эффективные алгоритмы декодирования (например, перестановочное декодирование, введенное в 1959 году Прэнджем.

Все упомянутые свойства при своем обосновании существенно используют одно важное утверждение, которое было доказано в 1952 году О.Перроном [4]. Это свойство позволяет устанавливать распределение квадратичных вычетов и невычетов в множестве чисел, полученных в результате сложения всех квадратичных вычетов (или, соответственно, невычетов) по модулю простого числа p с одним и тем же числом a, взаимно простым с p.

Актуальность задачи обобщения квадратично-вычетных кодов на случай вычетов более высоких степеней, поставленной перед автором, обусловлена тем, что при наличии довольно хорошей нижней оценки на кодовое расстояние ($d \geq \sqrt{p}$), второй важный параметр - относительная

[3] Ф. Мак-Вильямс, Н. Слоэн Теория кодов, исправляющих ошибки, "Связь", Москва, 1979.

[4] O. Perron Bemerkungen ueber die Verteilung der quadratischen Reste, Mathematische Zeitschrift, Band 56, Heft 2, (1952), S. 123-130

скорость передачи - остается довольно плохим - этот параметр всегда примерно равен $1/2$, независимо от значения простого числа p. Появляется необходимость с помощью изменения степени вычетов изменять значение относительной скорости передачи, естественно, при не сильном ухудшении нижней оценки на кодовое расстояние. Кроме теоретического построения таких кодов актуальной остается задача сохранения применимости таких кодов на практике, что означает сохранение возможности явного вычисления порождающего многочлена и выписывания порождающей матрицы.

Другая теоретико-числовая задача, рассматриваемая в диссертации, связана с гиперэллиптическими кривыми, рассмматриваемыми над конечным полем K характеристики 2. Для фиксированного дивизора D, определенного на данной кривой X, можно рассмотреть пространство Римана-Роха, задаваемое на множестве $\mathbb{F}_q(X)$ рациональных функций, определенных на кривой, следующим образом:

$$L(D) = \{\ f \in \mathbb{F}_q(X)^* \mid (f) + D \geq 0\ \} \cup \{\ 0\ \},$$

В 1981 году в статье [5] В.Д.Гоппа впервые упоминает про алгеброгеометрические коды. Речь идет о следующей конструкции (которая имеет несколько эквивалентных формулировок).

Пусть $P = \{P_1, P_2, \ldots, P_n\}$ - произвольное подмножество точек, лежащих на кривой X. Выберем дивизор $D = \sum m_i P_i$, принадлежащий множеству $Div(F_q)$, так, чтобы выполнялось следующее условие:

$$Supp\ D \cap P = \emptyset,$$

где $Supp\ D = \{\ P_i \mid m_i \neq 0\ \}$.

Рассмотрим следующее отображение:

$$Ev_P : L(D) \to F_q^n, \quad f \mapsto (f(P_1), \ldots, f(P_n)).$$

Образ этого отображения $Ev_P(L(D)$ является линейным кодом. Этот код мы будем обозначать $C = (X, P, D)_L$. Можно также рассматривать код $C^\perp$, двойственный к коду C и являющийся, по определению, ортогональным дополнением к линейному пространству $Ev_P(L(D))$.

Таким образом, для построения данного кода требуется умение явно вычислять базис пространства Римана-Роха. Более того, необходимость явно выписывать такой базис для разных дивизоров возникает также при использовании описанных в литературе алгоритмов кодирования-декодирования [6].

[5] В.Д. Гоппа, Коды на алгебраических кривых, ДАН СССР, Т. 259, №6, с. 1289-1290, 1981

[6] С.Г. Влэдуц, Д.Ю. Ногин, М.А. Цфасман "Алгеброгеметрические коды. Основные понятия.", МЦНМО 2003.

Решаемая автором задача выписывания такого базиса для гиперэллиптических кривых, рассматриваемых над полем характеристики 2, основана на результатах опубликованной в 1996 году статьи [7], согласно которой для так называемого приведенного дивизора $D = \sum m_i P_i$, где $P_i(x_i, y_i)$, можно найти однозначно определенную пару многочленов $a(u)$ и $b(u)$, строящуюся следующим образом.

В качестве многочлена $a(u)$ берется многочлен $a(u) = \prod (u - x_i)^{m_i}$. Тогда, согласно результатам указанной статьи, можно найти единственно определенный многочлен $b(u)$, обладающий свойствами:

1) $deg_u b(u) < deg_u a(u) < g$,

2) $b(x_i) = y_i$,

3) $a(u)$ делит многочлен $N(v - b(u)) = b(u)^2 + b(u)h(u) - f(u)$.

Базис пространства Римана-Роха строится на основе задания полуприведенного дивизора D такой парой многочленов.

Цель работы. В процессе написания настоящей диссертационной работы преследовались две основные цели.

1) Построение новых кодов, исправляющих ошибки, на основе обобщения уже известных на сегодняшний день квадратично-вычетных кодов. Главной задачей при этом было улучшение нижних границ относительной скорости передачи, которая, как уже говорилось, в случае квадратично-вычетных кодов приблизительно равняется $\frac{1}{2}$. При этом, разумеется, важно было преимущественно не ухудшить нижние оценки кодового расстояния. Представляло также интерес эффективное построение многочлена, порождающего эти коды, так как задание такого многочлена в явном виде позволяет бы выписать порождающую матрицу, и, тем самым, полностью описать код и построить эффективные алгоритмы кодирования и декодирования.

2) Явное построение совокупности рациональных функций, составляющих базис пространства Римана-Роха на гладких гиперэллиптических кривых. Основной задачей при рассмотрении этого вопроса было применить при поиске базиса известное представление полуприведенных и приведенных дивизоров, определенных на гладких гиперэллиптических кривых, парой многочленов. Такой способ задания дивизоров помогает явным образом находить в произвольной точке порядок функций, лежащих в соответствующем пространстве Римана-Роха.

Научная новизна результатов диссертации.

В настоящей работе построены коды, основанные на вычетах степени n по модулю простого числа. Получены оценки на кодовое расстояние

[7] Alfred J. Menezes, Yi-Hong Wu, Robert J. Zuccherato, "An elementary introduction to hyperelliptic curves", Technical Report COORR 96-19, department of CO, University of Waterloo, Ontario, November 1996.

и относительную скорость передачи таких кодов. При этом последняя оценка оказывается лучше, чем в известных аналогичных случаях, и с возрастанием числа n она стремится к 1.

Для случая вычетов третьей и четвертой степеней в явном виде выписан порождающий идемпотент соответствующих кодов, что решает задачу явного нахождения порождающей и проверочной матрицы. Стоит отметить, что этот результат получен новым методом с применением симметрических многочленов, который может быть в дальнейшем распространен на вычеты более высоких степеней.

Для произвольного дивизора, определенного на гладкой гиперэллиптической кривой над полем характеристики 2 выписан в явном виде базис пространства Римана-Роха над этим полем, состоящий из рациональных функций.

Практическая значимость работы.

Для построенных в настоящей работе кодов относительная скорость передачи может быть приближена к 1 сколь угодно близко.

Для кодов на основе вычетов третьей и четвертой степеней явно выписан порождающий идемпотент и порождающая матрица.

Построенный в явном виде базис пространства Римана-Роха позволяет выписать проверочную матрицу соответствующего кода, и, кроме того, может быть использован в основном алгоритме декодирования кодов, рассматриваемых на гладких гиперэллиптических кривых.

Публикации. Оба результата настоящей диссертации опубликованы в двух статьях, одна их которых депонирована в ВИНИТИ РАН.

Структура и объем диссертации. Диссертация состоит из списка обозначений, введения, обсуждения результатов, вычислительного приложения и списка цитируемой литературы. Работа изложена на 80 страницах машинописного текста.

Методы исследования. В работе используются результаты теории кодирования и алгебраической теории чисел, а также применяются алгебраические и алгеброгеометрические методы.

СОДЕРЖАНИЕ РАБОТЫ

В первой главе приведен краткий обзор исследований, связанных с содержанием данной диссертации. Даются основные определения и вводятся основные объекты, связанные с теорией кодирования - линейные коды, их порождающие и проверочные матрицы, параметры (блоковая длина, относительная скорость передачи и минимальное кодовое расстояние). Большую роль в теории кодирования играет изучение границ, накладывающих различные ограничения на возможные значения параметров кодов, поэтому в обзоре приводятся некоторые известные на сегодняшний день оценки параметров линейных кодов (границы Синглтона, Хемминга, Плоткина, линейного программирования и достаточное условие существования кода - условие Варшамова-Гилберта). Упоминается основная асимптотическая задача теории кодирования, связанная с существованием так называемых асимптотически хороших семейств кодов, описывается в связи с этим граница Варшамова-Гилберта, обладающая интересными статистическими свойствами.

Одним из основных объектов диссертации являются квадратично-вычетные коды, которые являются циклическими кодами, поэтому в первой главе также даны основные определения и результаты, связанные с циклическими кодами. Более подробно рассмотрен важный частный случай циклических кодов - БЧХ-коды.

Другой основной объект диссертации - пространство Римана-Роха $L(D)$, являющееся линейным подпространством в пространстве рациональных функций, рассматриваемых на алгебраических кривых. С пространством Римана-Роха тесно связаны алгеброгеометрические коды, определение которых, оценки параметров, а также основной метод декодирования также приведены в первой главе.

Во второй главе диссертации исследуются линейные коды, основанные на квадратичных вычетах по модулю простого числа p. Эти коды являются циклическими. Известно, что такие коды имеют довольно хорошую нижнюю оценку одного из важнейших параметров - кодового расстояния, а именно оценку $d \geq \sqrt{p}$. Однако у них есть существенный недостаток, связанный с тем, что другой важный параметр - относительная скорость передачи кода - независимо от блоковой длины всегда равен $1/2$, что делает затруднительным применение таких кодов на практике. Исходя из этих соображений, в диссертации строится обобщение таких кодов на случай вычетов более высоких степеней по модулю простого числа p, что позвояет улучшить значение этого параметра.

Пусть n - натуральное число, $n \geq 2$, а простое число p выбрано так, что число 2 является вычетом степени n по модулю p. Будем строить

двоичные коды, определив предварительно следующие $h = (n, p-1)$ классов:

$$Q_i = \{r \in F_p^* | r = g^k, k \in \mathbb{Z}, 0 \le k \le p-2, k \equiv i \pmod{h}\}, \quad i = 0, \ldots, h-1,$$

где g - произвольный порождающий элемент группы F_p^*. Далее зафиксируем кольцо $R_p = F_2[x]/(x^p - 1)$, произвольный идеал которого является циклическим кодом [8]. Обозначив через α произвольный примитивный корень степени p из единицы, лежащий в некотором расширении поля F_2, введем в рассмотрение следующие h многочленов:

$$q_i(x) = \prod_{r \in Q_i} (x - \alpha^r), \qquad i = 0, \ldots, h-1.$$

В диссертации показывается, что данные многочлены принадлежат кольцу $F_2[x]$. Поэтому для каждого числа $i = 0, \ldots, h-1$ можно рассмотреть идеалы $\mathfrak{L}_i$ в кольце R_p, порождающим многочленом которых служат, соответственно, многочлены $q_i(x)$. Заметим, что данные порождающие многочлены задаются лишь своими корнями; для эффективного же задания таких многочленов требуется проводить вычисления их коэффициентов в конечном поле F_2. Для того, чтобы избежать этих вычислений, далее для каждого кода будет найден другой многочлен, порождающий этот код, с помощью которого задача эффективного описания кода становится более простой.

Для полученных таким образом кодов доказывается следующая теорема.

Теорема 1

1) *Длина кода (длина каждого кодового слова) равна* p.
2) *Размерность кода равна* $p - deg\ q_i(x) = p - \frac{p-1}{h}$, *а относительная скорость передачи* $1 - \frac{1}{h} + \frac{1}{ph}$;
3) *Все коды* $\mathfrak{L}_i$ *эквивалентны друг другу и получаются друг из друга некоторой перестановкой координатных позиций.*
4) *Кодовое расстояние* d *удовлетворяет неравенству* $d \ge \sqrt[h]{p}$.

Таким образом, нижняя граница относительной скорости передачи таких кодов улучшается и возрастает в зависимости от степени рассматриваемых вычетов по модулю простого числа p, правда, при некотором ухудшении нижней оценки на кодовое расстояние.

[8] С.Г. Влэдуц, Д.Ю. Ногин, М.А. Цфасман "Алгеброгеметрические коды. Основные понятия."МЦНМО 2003, стр. 66

Если сравнивать параметры полученных кодов с параметрами другого широко известного класса циклических кодов - БЧХ-кодами, то нижние границы параметров примитивных БЧХ-кодов имеют несколько лучшую асимптотику (имеются в виду случаи, в которых сравниваются коды над полем F_2, построенные с помощью вычетов степени n блоковой длины p, где p - простое число, и примитивные БЧХ-коды такой же блоковой длины, то есть случаи, когда число p имеет вид $p = 2^m - 1$). Однако у БЧХ-кодов имеется один существенный недостаток, связанный со сложностью построения в явном виде порождающего многочлена, который, по определению, является многочленом наименьшей степени, имеющий своими корнями $\alpha, \alpha^2, \ldots, \alpha^{\delta-1}$ для некоторого натурального числа δ, где α - примитивный элемент поля F_{2^m}. В рассматриваемых нами кодах, обобщающих квадратично-вычетные коды, в случае вычетов третьей и четвертой степеней в явном виде построен многочлен, порождающий код, для выписывания коэффициентов которого достаточно указать все вычеты третьей и четвертой степени соответственно по модулю простого числа p.

Введем некоторые определения, требующиеся для формулировки полученных результатов.

Определение 1 *Многочлен $E(x) \in R_p$ - идемпотент, если в R_p выполнено равенство $E^2(x) = E(x)$.*

Рассмотрим также следующие многочлены: $T_i(x) = \sum\limits_{r \in Q_i} x^r,\ i = \overline{0, h-1}$.

Определение 2 *Скажем, что семейство кодов $\mathfrak{L}_i$ имеет распределение $(a_0, a_1, \ldots, a_{h-1})$, $a_i \in \{0, 1\}$, если для некоторого α - примитивного корня из 1 степени p - справедливы равенства:*

$$T_0(\alpha) = a_0,\ T_1(\alpha) = a_1,\ \ldots,\ T_{h-1}(\alpha) = a_{h-1}.$$

Для случаев $h = 3$ и $h = 4$ доказаны следующие теоремы.

Теорема 2 (Случай кубических вычетов) *При $h = 3$ элемент α - примитивный корень степени p из единицы - можно выбрать таким образом, что порождающими идемпотентами $E_i(x)$ кодов $\mathfrak{L}_i$ и порождающими идемпотентами $\overline{E_i(x)}$ кодов $\overline{\mathfrak{L}_i}$ будут являться, соответственно, многочлены:*

$$E_i(x) = T_{3-i}(x) + 1, \qquad \overline{E_i(x)} = \sum_{j \neq 3-i} T_j(x).$$

Теорема 3 (Случай биквадратичных вычетов) *При $h = 4$ элемент α - примитивный корень степени p из единицы - можно выбрать таким образом, что*

1) *В случае $p \equiv 1 \pmod{16}$ код $\mathfrak{L}_i$ имеет распределение $(1, 0, 0, 0)$ и идемпотенты $E_i(x) = T_{4-i}(x) + 1$, $\overline{E_i(x)} = \sum_{j \neq 4-i} T_j(x)$.*

2) *В случае $p \equiv 9 \pmod{16}$ код $\mathfrak{L}_i$ имеет распределение $(0, 1, 1, 1)$ и идемпотенты $E_i(x) = \sum_{j \neq 4-i} T_j(x) + 1$, $\overline{E_i(x)} = T_{4-i}(x)$.*

Теоремы 2 и 3 позволяют эффективно выписывать многочлены, порождающие соответствующие коды (правда, они уже не являются многочленами наименьшей степени, порождающими код). Действительно, для выписывания таких многочленов достаточно лишь, зная число p, воспользоваться таблицами вычетов третьей и четвертой степени по модулю этого числа p.

Построение в явном виде порождающего многочлена позволяет эффективно строить порождающую матрицу, то есть позволяет полностью описать код.

Третья глава диссертации посвящена рассмотрению гладких гиперэллиптических кривых над конечным полем K характеристики 2 и алгеброгеометрических кодов, построенных по таким кривым.

Пусть K - конечное поле характеристики 2, $\overline{K}$ - его алгебраическое замыкание. Рассмотрим гиперэллиптическую кривую X над полем K рода g, заданную уравнением

$$v^2 + h(u)v = f(u), \tag{1}$$

где $h(u) \in K[u]$ - многочлен степени не выше g, $f(u) \in K[u]$ - многочлен степени $2g + 1$. Дополнительно будем предполагать выполненным условие гладкости рассматриваемой гиперэллиптической кривой, которое заключается в отсутствии решений $(u, v) \in \overline{K} \times \overline{K}$ следующей системы уравнений [9]:

$$\begin{cases} v^2 + h(u)v = f(u), \\ 2v + h(u) = 0, \\ h'(u)v - f'(u) = 0. \end{cases}$$

Для каждой точки $P = P(x, y)$ будем рассматривать сопряженную к ней точку $\tilde{P} = P(x, -y - h(x))$.

[9] Alfred J. Menezes, Yi-Hong Wu, Robert J. Zuccherato, "An elementary introduction to hyperelliptic curves", Technical Report COORR 96-19, department of CO, University of Waterloo, Ontario, November 1996.

Зафиксируем произвольный дивизор D, определенный на кривой: $D = \sum m_P P + s\infty$. Одним из основных объектов, тесно связанных с алгеброгеометрическими кодами, построенными по таким кривым, является пространство Римана-Роха, имеющее в литературе стандартное обозначение $L(D)$:

$$L(D) = \{\ f \in \mathbb{F}_q(X)^* \mid (f) + D \geq 0\ \} \cup \{\ 0\ \}.$$

Известно, что пространство Римана-Роха является конечномерным линейным подпространством в пространстве рациональных функций на кривой. В диссертации предлагается построение базиса данного линейного пространства над полем K для приведенного дивизора D.

Метод, с помощью которого строится такой базис, основан на задании приведенных (и полуприведенных) дивизоров, определенных на рассматриваемой гиперэллиптической кривой, парой многочленов. В настоящее время в литературе имеются работы, использующие такой способ задания дивизоров для построения эффективных вычислительных алгоритмов в группе классов идеалов кольца $K[x, y]$, целозамкнутого в своем поле частных $K(x, y)$, где $K(x, y)$ - поле рациональных функций на гиперэллиптической кривой. В данной диссертации продемонстрировано, каким образом можно применять такое задание приведенного дивизора для определения порядка произвольной функции, принадлежащей пространству $L(D)$, соответствующему данному дивизору D, и, тем самым, для построения базиса этого пространства. Линейно независимые функции, принадлежащие множеству $L(D)$, строятся с помощью удобного критерия, основанного на разложении функций в ряд по степеням локального параметра. С помощью этого же критерия исследуется полнота полученной системы функций.

Итак, найдем для приведенного дивизора $D = \sum m_P P + s\infty$ однозначно определенную связанную с ним пару многочленов $a(u)$ и $b(u)$, лежащих в пространстве $K[u]$. Метод нахождения такой пары многочленов указан, например, в работе [10].

Рассмотрим далее вспомогательное пространство

$$(L(D))_u = \{f \in K(u, v)^* \mid \nu_P(f) \geq -\nu_P(D) \text{ для всех конечных точек } P\} \cup \{0\}.$$

Пусть теперь $\tilde{D} = \sum m_i \tilde{P}_i$. Найдем для данного дивизора соответствующую ему пару многочленов точно также, как это делалось для дивизора D. Для дивизора $\tilde{D}$ многочлен $a(u)$ будет в точности совпадать

[10] Alfred J. Menezes, Yi-Hong Wu, Robert J. Zuccherato, "An elementary introduction to hyperelliptic curves", Technical Report COORR 96-19, department of CO, University of Waterloo, Ontario, November 1996.

с соответствующим многочленом для дивизора D. Второй же многочлен будет отличаться от многочлена $b(u)$, найденного для дивизора D. Обозначим этот многочлен через $\tilde{b}(u)$.

В диссертации доказывается следующая теорема.

Теорема 4 *Функции*

$$\omega_1 = \frac{v - \tilde{b}(u)}{a(u)} \qquad u \qquad \omega_2 = 1$$

образуют базис пространства $(L(D))_u$ *над кольцом* $K[u]$.

Доказательство данной теоремы существенным образом опирается на результаты статьи [11], в частности, использован критерий принадлежности рассматриваемому линейному пространству, а также критерий линейной независимости произвольного набора рациональных функций, определенных на кривой.

Пусть $A = \nu_\infty(\omega_1) = 2\sum m_P - 2g - 1$ - порядок функции ω_1 в бесконечно удаленной точке. Далее доказывается теорема о структуре базиса пространства $L(D)$.

Теорема 5 *Пусть* $D = \sum m_P P + s\infty$ *- приведенный дивизор, для которого* $A + s \geq 0$. *Тогда базис пространства* $L(D)$ *над полем* K *задается следующими функциями:*

$$\{u^i\omega_1\}, \quad \{u^j\omega_2 = u^j\}, \quad 0 \leq i \leq \left[\frac{A+s}{2}\right], \quad 0 \leq j \leq \left[\frac{s}{2}\right].$$

Построение в явном виде такого базиса решает задачу явного описания алгеброгеометрического кода на гиперэллиптических кривых, так как позволяет строить порождающую и проверочную матрицы таких кодов, а также может применяться в основном алгоритме декодирования, в котором требуется неоднократный поиск базиса пространства $L(D)$ для разных дивизоров D.

Работы автора по теме диссертации

1. Семеновых Д.Н. Обобщение квадратично-вычетных кодов на случаи вычетов третьей и четвертой степени Дискретная математика, т.17, 2005, №4, с. 143-149

2. Семеновых Д.Н. Построение базиса пространства Римана-Роха на гиперэллиптических кривых. Рукопись деп. в ВИНИТИ 13.12.2005 № 1653-В2005

[11] J. Coates "Construction of rational functions on a curve", Proc. Camb. Soc., 1970, 68, 105