Предисловие

Первый том этой книги — «Алгеброгеометрические коды. Основные понятия» — вышел в свет в издательстве МЦНМО в 2003 году. В той книге мы пообещали читателю дополнить ее вторым томом — «Алгеброгеометрические коды. Дополнительные главы». Отчасти в связи с объективными трудностями, отчасти благодаря нашей собственной лени написание второй книги растянулось на два десятилетия.

Для тех, кто успел позабыть содержание первого тома, к этой книге написано приложение, в котором изложены основы теории и вкратце перечислены главные результаты.

Мы старались сделать текст как можно более понятным и независимым от других источников, но хотя этот том и рассчитан на более подготовленного читателя, чем первый, мы никак не можем утверждать, что эта цель вполне достигнута.

К некоторому нашему удивлению нам удалось покрыть почти все темы, которые мы считаем основными в данной теории, и выполнить обещания, данные в предисловии к «Основным понятиям» (за исключением графов без коротких циклов и кодов над кольцами). Разумеется, имеется множество результатов, которые мы не смогли затронуть хоть сколько-либо подробно, как и многочисленные смежные области.

Мы рассматриваем следующие вопросы. Кривые с большим числом $\mathbb{F}_q$-точек, особенно достигающие границы Дринфельда–Влэдуца, а именно модулярные кривые — как классические, так и кривые Дринфельда, — и явные конструкции Элкиса. Теория полей классов и возникающие из нее башни кривых. Границы Остерле для числа точек. Примеры хороших кривых, в частности, кривых малых родов, кривые Делиня–Люстига, рекурсивные башни Гарсии–Штихтенота и т. д. Теория бесконечных глобальных полей, включая основное неравенство и обобщенную теорему Брауэра–Зигеля, примеры башен полей классов и т. д. Декодирование алгеброгеометрических кодов. Плотные упаковки шаров, в особенности асимптотически хорошие, решетки Элкиса–Шиоды, конструкции, основанные на полях классов, и некоторые другие связи между теорией чисел и алгебраической геометрией с одной стороны и упаковками шаров с другой. Затем затрагивается увлекательный сюжет о числе $\mathbb{F}_q$-точек на поверхностях и многомерных многообразиях, о котором известно гораздо

меньше, чем о числе точек на кривых, и конечно, коды, получаемые по этим многообразиям. Помимо этого, есть некоторые приложения либо непосредственно алгеброгеометрических кодов, либо стилистически связанных с ними конструкций к алгоритмам быстрого умножения, криптографии, квантовым кодам и т. п.

Мы надеемся, что эта книга будет полезна как читателям, интересующимся алгебраической геометрией и теорией чисел, так и тем, кому интересно, что из этого может оказаться полезным для теории кодирования и других приложений. Два тома этой книги вместе взятые — это и учебник для аспирантов (и хороших студентов), и пособие для специалистов, и чтение для математиков, специализирующихся в других областях.

* * * * *

Поясним наш выбор рассматриваемой тематики по каждой отдельной главе. Оба тома этой книги написаны для математиков различных специальностей и базового образования. Мы имеем в виду специалистов по теории кодирования, алгебраической геометрии, теории чисел, комбинаторике, геометрии и т.д.

В первом томе глава 1 предлагает введение в теорию кодирования для тех, кто ее не знает, и геометрический взгляд на нее для тех, кто ее знает.

Глава 2 представляет собой сжатый перечень необходимых нам сведений по алгебраической геометрии кривых.

В главе 3 рассматриваются кривые над конечными полями — тема, которая в известном смысле ближе к теории чисел, чем к классической алгебраической геометрии.

В главе 4 мы наконец снимаем сливки, рассказывая о том, что можно получить для кодов благодаря использованию алгебраических кривых.

В этом томе мы восполняем пробелы и выполняем обещания, данные в первом.

Для построения алгеброгеометрических кодов с хорошими параметрами нужны кривые с большим числом точек. Существует несколько типов таких конструкций. Исторически первой и одной из самых красивых является конструкция модулярных кривых (глава 5).

К сожалению, модулярные кривые не годятся для конечных полей, мощность которых не является квадратом, а соответствующие аналоги для числовых полей нам не известны. Конструкция, которая работает в этих случаях, основана на башнях полей классов (глава 6).

В главе 7 рассматриваются некоторые другие вопросы, касающиеся кривых с большим числом точек, в частности, вопрос о том, как строить модулярные кривые с помощью явных уравнений.

Одной из наиболее увлекательных сторон рассматриваемой теории и в определенной степени смыслом ее существования является параллелизм между полями функций на кривых над конечными полями с одной

стороны и числовыми полями с другой. В совокупности эти два типа полей называются *глобальными полями*, и их теория очень красива и хорошо развита. Мы стараемся продвинуться еще дальше. Изначально руководствуясь вопросами асимптотического поведения параметров кода, а значит, и асимптотического поведения числа точек на кривых в башнях и семействах, в главе 8 мы излагаем теорию бесконечных глобальных полей и их дзета-функций, что составляет крайне интересную часть общей теории.

Глава 9 посвящена декодированию алгеброгеометрических кодов — предмету, который имеет первостепенное значение для приложений, а также ставит ряд интересных вопросов перед алгебраическими геометрами.

Давняя замечательная геометрическая задача о плотной упаковке шаров (глава 10) оказывается связанной как с кодами, так и с числовыми и функциональными полями. Излагаемые нами конструкции близки по духу к конструкциям алгеброгеометрических кодов.

Многомерные многообразия над конечными полями изучены гораздо меньше, чем кривые. В главе 11 мы излагаем то, что о них известно, и строим коды на их основе.

В заключительной главе 12 описаны некоторые другие приложения и аналоги алгеброгеометрических кодов, такие как быстрое умножение в больших конечных полях, криптография, квантовые коды и т. д.

Поскольку первый том был опубликован уже достаточно давно, для удобства читателя в приложении мы приводим сводку его основных положений.

* * * * *

Позволим себе дать читателю несколько советов в отношении отдельных глав настоящего тома.

Если вы интересуетесь теорией кодирования, то вам пригодятся конструкции хороших кодов, их параметры, кодирование и декодирование. Тогда вы можете прочитать главу 9 (Декодирование алгеброгеометрических кодов), главу 11 (Коды по многомерным многообразиям; она требует более глубоких познаний в алгебраической геометрии), и наконец, глава 12 также может представлять для вас интерес. Что касается остальных глав, то они составляют алгеброгеометрическую и теоретико-числовую основу для изучаемых объектов и раскрывают их глубинную природу; соответственно, необходимые для этого знания алгебраической геометрии и арифметики более широки.

Если вас интересует в основном арифметическая геометрия, то вам подойдут главы 6, 7 и особенно глава 8. В главе 10 описано красивое приложение к упаковкам шаров.

Для алгебраического геометра наибольший интерес может представлять глава 11, однако, вероятно, лучше прочитать ее после глав 5 и 7.

Если вы интересуетесь теорией чисел, прочитайте главы 6 и 8.

Те же, кому нравятся все эти области, возможно, захотят прочитать всю книгу целиком.

* * * * *

Особый интерес для нас представляют связи и взаимопроникновения различных разделов математики, которые постоянно прослеживаются в данной области. Перечислим некоторые из этих точек соприкосновения.

1. *Коды и алгебраические многообразия над конечными полями*. Это основной сюжет первого тома [ВНЦ03], особенно в случае кривых (см. приложение). Линейный код эквивалентен мультимножеству точек в $\mathbb{P}^{k-1}$ — см. раздел П.1. Тогда естественно рассмотреть коды, соответствующие $\mathbb{F}_q$-точкам алгебраических многообразий, в частности, кривых. Это приводит к многочисленным вопросам о кривых (но также и о многомерных многообразиях) над конечными полями.

2. *Коды и упаковки*. Хороший код, исправляющий ошибки, представляет собой плотную упаковку равных шаров в пространстве Хэмминга $\mathbb{F}_q^n$. Таким образом, мы не можем не рассмотреть задачу упаковки шаров и в других пространствах, в частности, в евклидовом пространстве $\mathbb{R}^n$. В такой постановке линейный код соответствует решетчатой упаковке, и существует множество способов построения довольно плотных упаковок по кодам с хорошими параметрами (см. главу 10).

3. *Числовые поля, кривые и упаковки шаров*. Естественные конструкции решеток по числовым полям, известные на протяжении уже двух столетий, можно обобщить до конструкций решеток по кривым. Как оказывается, и те, и другие приводят к плотным упаковкам шаров (см. главу 10).

4. *Алгебраические кривые над конечными полями и числовые поля*. Основной вопрос, стоящий здесь перед нами, заключается в определении числа точек кривой над основным полем и его конечными расширениями. Эти вопросы собраны воедино в понятии дзета-функции кривой. Благодаря этому понятию наряду с алгеброй и геометрией в общей картине появляется математический анализ. При взгляде на теорию кривых с алгебраической точки зрения становится заметна одна из главных жемчужин современной математики — параллелизм между кривыми над конечными полями и числовыми полями, т.е. конечными расширениями поля $\mathbb{Q}$. Мы наблюдаем это в гл. 6 и 8, но имеем в виду всегда.

5. *Кривые с большим числом точек и модулярные функции*. Эта же самая теория приводит нас к модулярным кривым, предоставляя примеры кривых большого рода с большим числом точек (см. главу 5). На геометрическом языке это часть еще одной жемчужины и самой сердцевины современной математики — теории пространств модулей. Отметим,

что в недавно полученном решении задачи о плотнейшей упаковке шаров в размерностях 8 и 24 также использовались модулярные функции.

6. *Кривые, многообразия и теория групп*. Теория групп, а также теория алгебраических групп, появляются при рассмотрении башен полей классов (глава 6) и при поиске многообразий с большим числом точек (многообразия Делиня–Люстига, грассманианы и т.д.); группы автоморфизмов многообразий, особенно кривых, также иногда важны для приложений.

7. *Асимптотические параметры семейств кодов и предельные дзета-функции*. Для поиска и изучения кодов большой длины рассматриваются асимптотические вопросы: что происходит при стремлении параметров к бесконечности? Это соответствует асимптотическому изучению дзета-функций семейств алгебраических многообразий и числовых полей при стремлении рода кривой (дискриминанта поля) к бесконечности. В настоящий момент мы располагаем красивой, хотя и весьма неполной теорией предельных дзета-функций (см. главу 8). Поскольку дзета-функция характеризуется множеством своих нулей, в пределе мы получаем меру на критической прямой, и изучение таких мер добавляет нашим геометрическим и арифметическим объектам еще один аналитический оттенок.

* * * * *

По-видимому, целесообразно указать на взаимозависимость этих сюжетов. Грубо говоря, первые четыре главы этого тома (гл. 5–8; мы используем сплошную нумерацию глав по обоим томам книги) упорядочены линейно, т.е. в каждой главе используется та или иная информация из предыдущих. Напротив того, главы 9–12 по существу независимы как друг от друга, так и от глав 5–8.

С. Г. Влэдуц
Aix Marseille Université, CNRS, Centrale Marseille, I2M UMR 7373, Marseille, France
serge.vladuts@univ-amu.fr

Д. Ю. Ногин
Институт проблем передачи информации им. А. А. Харкевича РАН, Б. Каретный пер. 19, Москва;
Высшая школа современной математики, Московский физико-технический институт, Климентовский пер. 1, Москва
nogin@iitp.ru

М. А. Цфасман
Высшая школа современной математики, Московский физико-технический институт, Климентовский пер. 1, Москва
mtsfasman@yandex.ru