Предисловие

Вы держите в руках книгу, посвященную теории алгеброгеометрических кодов — сравнительно молодой области, возникшей в начале восьмидесятых годов прошлого века на стыке нескольких областей математики. С одной стороны здесь выступают такие почтенные, развитые и сложные области как алгебраическая геометрия и алгебраическая теория чисел, с другой — достояние второй половины двадцатого века, теория передачи информации (со своей алгебраической дочкой — теорией корректирующих кодов), а также комбинаторика, конечные геометрии, теория плотных упаковок и так далее.

Связь между этими, на внешний взгляд, далекими группами областей открыл В. Д. Гоппа. В начале 1981 года он рассказал о своем открытии на семинаре кафедры алгебры МГУ, на котором присутствовал Ю. И. Манин, который, в свою очередь, рассказал об этом на своем семинаре. Один из авторов книги (М. А. Цфасман) был на этом семинаре и впервые услышал там о существовании теории кодирования. Еще через несколько месяцев им, другим автором (С. Г. Влэдуцом) и Т. Цинком была написана небольшая работа, улучшавшая асимптотическую границу Варшамова–Гилберта. К огромному удивлению авторов, сомневавшихся, стоит ли вообще публиковать такую работу, мировое математическое сообщество в лице как специалистов по теории кодирования, так и алгебраических геометров, восприняло эту работу очень живо. (Неожиданно для авторов оказалось, что границу Варшамова–Гилберта пытались улучшить уже с четверть века и у многих сложилось мнение об ее окончательности.) Так возникла новая область — алгеброгеометрические коды.

Нас (С. Г. Влэдуца и М. А. Цфасмана) попросили написать книгу, которую могли бы читать и кодировщики, и алгебраические геометры. Книга эта [TV91] вышла в 1991 году в издательстве «Kluwer Academic Publishers» и должна была в том же году выйти на русском языке в издательстве «Наука». Однако судьбы России распорядились иначе, за что мы, впрочем, на эти судьбы отнюдь не в обиде. Следующий раз нам предложили опубликовать эту книгу десять лет спустя. Но к этому времени книга явно устарела, алгеброгеометрические коды стали вдвое старше, и мы решили вместо этого написать новую книгу, на базе старой. Число авторов выросло в полтора раза, а книга превратилась

в две, разделившись на «Основные понятия» и «Дополнительные главы». Первая из них перед Вами.

В предисловии к [TV91] мы писали, что «ближайшее десятилетие принесет множество новых интересных результатов, методов и задач в этой плодотворной области» и выражали надежду, что «книга может оказаться полезной математикам, пожелавшим выбрать эту область в качестве поля своих исследований». Смеем надеяться, что предсказание сбылось и что те же слова можно повторить и в отношении этой книги и ближайшего десятилетия.

Чтобы оживить чтение, мы снабдили книгу множеством упражнений и проблем.[1]

* * * * *

Авторы этой книги — чистые математики, основные научные интересы которых лежат на стыке алгебраической геометрии и теории чисел. Это определяет наше восприятие теории кодирования, зачастую отличающееся от ее восприятия специалистами. Основная цель этой части предисловия — изложить наш взгляд на эту область (точнее говоря, на ту ее часть, которая занимается изучением блоковых кодов, всюду в дальнейшем называемых просто кодами).

Конечномерные векторные пространства над нормированными полями ($\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}_p$ и т. п.) обладают естественной метрикой. Векторные пространства над $\mathbb{Q}$ и другими полями алгебраических чисел и конечномерные свободные $\mathbb{Z}$-модули обладают рядом метрик, связанных с вложениями соответствующего поля или кольца в нормированные. То же самое происходит с глобальными полями конечной характеристики: $\mathbb{F}_q(T)$ и его конечными алгебраическими расширениями.

Но каким образом можно ввести структуру метрического пространства на $\mathbb{F}_q^n$ — конечномерном пространстве над конечным полем? Мы не знаем никакой метрики более естественной, чем *метрика Хэмминга*:

$$d(x,y) = |\{i \mid x_i \neq y_i\}|,$$

т. е. расстояние равно числу различающихся координат; соответствующая норма:

$$\|x\| = |\{i \mid x_i \neq 0\}|.$$

[1] Упражнением мы старались называть вопрос, ответ на который нам известен, давая указания к более сложным из них, а проблемами — исследовательские задачи и открытые вопросы. Поучительная история произошла с упражнением 1.3.23. Это упражнение, равно как и аналогичное упражнение для упаковок шаров, было сформулировано в книге [TV91]. Оно оказалось несколько сложнее, чем нам тогда казалось. Будучи спрошен, как же его делать, один из авторов потратил некоторое время, чтобы сообразить, что вероятностные соображения действительно дают искомый результат. Попытка сделать аналогичное упражнение для упаковок шаров также увенчалась успехом: несколько лет работы легко привели к искомому результату (см. [ST01]).

У этой нормы имеется один существенный недостаток — она зависит от выбора базиса, но с этим, увы, ничего не поделаешь.

После того как пространство $\mathbb{F}_q^n$ метризовано, по аналогии с классической задачей о построении плотных упаковок равных шаров в $\mathbb{R}^n$ появляется задача: разместить в $\mathbb{F}_q^n$ возможно больше шаров данного диаметра d так, чтобы плотность упаковки была возможно выше (объем на $\mathbb{F}_q^n$ гораздо естественнее метрики: объем подмножества — это его мощность). Почти эквивалентная задача — построить возможно более мощное подмножество $C \subseteq \mathbb{F}_q^n$, такое что расстояние между любыми двумя его элементами не меньше d. Такое подмножество C называется $[n,k,d]_q$-*кодом*[2], где $k = \log_q |C|$. Вопрос о нахождении наиболее мощного кода при данных q, n, d представляется довольно естественной комбинаторной задачей.

Среди всех кодов органично выделяются *линейные*, т. е. коды $C \subseteq \mathbb{F}_q^n$, являющиеся линейными подпространствами. Причин для особого изучения линейных кодов по меньшей мере три: во-первых, линейные коды являются аналогом решетчатых упаковок шаров в $\mathbb{R}^n$; во-вторых, их легче строить — они доставляют много хороших примеров. Третья же, наиболее существенная для нас причина такова: линейные $[n,k,d]$-коды соответствуют *проективным системам* — системам $\mathcal{P}$ из n определенных над $\mathbb{F}_q$ точек в $(k-1)$-мерном проективном пространстве $\mathbb{P}^{k-1}$ над полем $\mathbb{F}_q$, причем $n-d$ есть максимум числа точек $\mathcal{P}$, лежащих в одной гиперплоскости (подробнее об этом см. в п. 1.1.2, такие $\mathcal{P}$ мы называем *проективными* $[n,k,d]_q$-*системами*). Таким образом, мы пришли к другой задаче: как разместить n точек в $\mathbb{P}^{k-1}$ так, чтобы достаточно большое их число не попадало одновременно ни в какую гиперплоскость (это условие типа общности положения). Заметим, что в этой постановке мы избавились как от базиса, так и от не вполне удовлетворявшей нас метрики.

Прочтя последний абзац, любой алгебраический геометр спросит: а что получится, если в качестве $\mathcal{P}$ взять все или часть $\mathbb{F}_q$-точек какого-нибудь алгебраического многообразия W? В случае кривой ответ довольно прост. Пусть V — алгебраическая кривая, определенная над $\mathbb{F}_q$ вместе со своим проективным вложением $V \hookrightarrow \mathbb{P}^{k-1}$, тогда n не превосходит $|V(\mathbb{F}_q)|$ — числа $\mathbb{F}_q$-точек кривой V, а $n-d$ не превосходит степени кривой $V \subset \mathbb{P}^{k-1}$, и вопрос о возможных соотношениях n, k, d является чисто алгеброгеометрическим. Дальнейшим свойствам таких кодов посвящена важная часть этой книги.

Сказанное во многом определяет наши взгляды на математическую теорию кодирования. Коды над всеми конечными полями $\mathbb{F}_q$ рáвно интересны (несмотря на то, что для приложений удобнее всего двоичные коды, т. е. коды над полем $\mathbb{F}_2$, в крайнем случае, над его расширениями); при этом особый интерес представляют линейные коды. Основной

[2] См. замечание 1.1.2, объясняющее, почему такое подмножество называется кодом.

задачей мы считаем задачу о возможных параметрах кода (в идеале их надо не только найти, но и предъявить код, их реализующий). У этой задачи имеется несколько основных постановок. Вот они (поле $\mathbb{F}_q$ всегда фиксировано).

Пусть длина кода n фиксирована. При данном d найти наибольшее $k = K(n,d)$, такое что существует $[n,k,d]_q$-код (соответственно, линейный $[n,k,d]_q$-код). Близкая задача — задача нахождения наибольшего $d = D(n,k)$ при фиксированном k. Заметим, что по $[n,k,d]_q$-коду легко строить $[n+1,k,d]_q$-, $[n,k-1,d]_q$- и $[n,k,d-1]_q$-коды, так что решая указанные задачи, мы одновременно описываем и все возможные значения параметров (а не только наилучшие). Третья близкая задача того же типа: найти наименьшее $n = N(k,d)$ при фиксированных k и d.

Поскольку на сегодняшний день наука не умеет решать эти задачи, проблема разбивается на две части (для простоты мы далее говорим о задаче нахождения $K(n,d)$). С одной стороны, полезно искать условия, которым удовлетворяют параметры любого кода. Такого рода условия ограничивают возможный объем кода сверху: $K(n,d) \leqslant K_{\mathrm{up}}(n,d)$, и называются поэтому *верхними границами*, или *границами возможности*. С другой стороны, хорошо бы указать конкретные коды с достаточно хорошими параметрами, каждый такой код (с заданными n и d) дает оценку снизу: $K_{\mathrm{low}}(n,d) \leqslant K(n,d)$ — *нижнюю границу*, или *границу существования*; естественно, что коды строятся, как правило, не по одиночке, а большими классами. Если для данных n и d верхняя граница совпала с нижней, то мы решили соответствующую задачу.

Основной недостаток указанной постановки состоит в том, что ставится не одна, а сразу очень много задач, и опыт работы над ними показывает, что мы очень далеки от общего решения. Частичным ответом для небольших n являются таблицы $K_{\mathrm{up}}(n,d)$ и $K_{\mathrm{low}}(n,d)$, наличие которых позволяет сравнивать новые способы построения кодов с уже имеющимися (см. таблицы в приложении B.2 в конце книги).

Второй тип задач возникает, когда мы начинаем интересоваться поведением параметров кода с ростом n. Пусть имеется семейство кодов с $n \to \infty$; как могут вести себя k и d? Правильная постановка асимптотических задач всегда зависит от того, как реально ведут себя параметры на бесконечности. В нашем случае естественными являются по меньшей мере три асимптотические задачи (точные постановки см. в § 1.3).

Первая: как ведет себя k в зависимости от n при фиксированном d? Известен характер ответа: положим

$$\varkappa_q(d) = \liminf_{n\to\infty} \left(\frac{n - K(n,d)}{\log_q n} \right),$$

тогда $0 < \varkappa_q(d) < \infty$, и законен вопрос о точном значении или оценке этой величины; оказывается, что $\varkappa_q(d)/(d-1)$ оценивается сверху и снизу

константами, не зависящими от d (грубо говоря, $1/2 \leqslant \varkappa_q(d)/(d-1) \leqslant (q-1)/q$ для всех d).

Вторая: как ведет себя d в зависимости от n при фиксированном k? Характер ответа опять известен; более того, известен и ответ: положим

$$\delta_q(k) = \limsup_{n\to\infty} \left(\frac{D(n,k)}{n} \right),$$

тогда

$$\delta_q(k) = \frac{q^{k-1}(q-1)}{q^k - 1}.$$

Третья задача, на наш взгляд, наиболее интересна, мы называем ее *основной асимптотической задачей*. Пусть $n, k, d \to \infty$, $k/n \to R$, $d/n \to \delta$; как R зависит от δ? Эту задачу удается точно поставить и показать, что зависимость нетривиальна. Этой задаче будет посвящена значительная часть книги. Возможны еще некоторые асимптотические постановки, но они представляются нам более искусственными.

На этом кончается важнейший, на наш взгляд, сюжет математической теории кодирования — *проблема параметров*.

Ко второму сюжету мы подходим уже с опытом, накопленным при разработке первого. Нам известен ряд верхних границ; существуют ли коды, параметры которых лежат на этих границах? Как правило, эти коды характеризуются каким-либо хорошим свойством, таковы, например, совершенные и эквидистантные коды. Кроме этого, нам известен уже целый ряд конкретных классов кодов, и можно задавать вопрос о возможных параметрах кодов из данного класса (хороший пример — вопросы о параметрах циклических кодов, самодвойственных кодов, МДР-кодов и т. д.). Полезно также знать свойства этих конкретных кодов: их весовые спектры (см. п. 1.1.3), их группы автоморфизмов, их поведение относительно естественной двойственности и т. п. Этот сюжет можно назвать *проблемой свойств и структуры*, задачи здесь также очень важны и весьма разнообразны.

Нам бы хотелось не только уметь определять наилучшие возможные параметры кода, но и уметь в сколько-нибудь явном виде строить коды с такими параметрами. Для конечного фиксированного n построить код — это предъявить алгоритм его построения (например, для линейного кода — построить его порождающую матрицу). Конечно, имеется «глупый» универсальный алгоритм: перебрать все подмножества или линейные подпространства $\mathbb{F}_q^n$; хотелось бы исключить такие решения. Теория сложности алгоритмов дает возможность это сделать при постановке асимптотических задач: потребуем, чтобы алгоритмы построения полиномиально зависели от n (точные постановки см. в п. 1.3.3). Сегодня это единственная строгая постановка задачи о явном

построении кодов, поэтому мы ее и придерживаемся. Это — третий сюжет: *проблема конструктивности*, ею мы также будем много заниматься.

Имеется еще четвертый, почти не затрагиваемый в этой части нашей книги сюжет: коды, хорошие с точки зрения их практического применения. Вспомним, что коды способны исправлять ошибки, возникающие при передаче искажаемой случайными помехами информации по каналу связи определенного типа. Коды для практического применения должны быть, как правило, двоичными или 2^m-ичными с небольшим m; достаточно, но не чрезвычайно длинными; с простым и быстрым, а не просто полиномиальным алгоритмом построения; наконец, с простым и быстрым алгоритмом декодирования. Это — *проблема практической применимости*. С этим сюжетом также связан ряд интересных алгеброгеометрических задач; алгеброгеометрические коды уже привели к существенному прогрессу и в этом направлении.

Наконец, имеется еще один сюжет, который можно назвать *проблемой аналогов*. Мы считаем, что эта тема во многом определяет место теории кодирования в здании современной математики. Оказывается, что имеется красивая аналогия между линейными кодами и решетками в евклидовом пространстве, согласованная с едва ли не самой фундаментальной в современной математике аналогией между алгебраическими кривыми и числовыми полями. Надежда на прояснение этой аналогии во многом обуславливает интерес авторов к теории кодирования.

И наконец, теория алгеброгеометрических кодов породила много новых задач и методов в материнских областях, в том числе в алгебраической геометрии и теории чисел. Обо всем этом мы надеемся поговорить в «Дополнительных главах».

Мы думаем, что возможности алгеброгеометрических кодов далеко не исчерпаны, и надеемся, что эта книга послужит притоку новых сил в эту область.

* * * * *

Книга рассчитана на математика. Читатель может быть, а может и не быть знакомым с основными понятиями теории кодирования и алгебраической геометрии.

Две первые главы — вводные. Первая глава содержит основы теории кодирования, алгебраическая геометрия в ней явно не фигурирует, хотя подбор материала и многие результаты мотивированы алгеброгеометрическими кодами. По сравнению с классическими учебниками по теории корректирующих кодов, новых результатов в ней немного. Основные особенности: во-первых, мы почти всегда говорим о кодах над произвольным конечным полем (не ограничиваясь двоичными кодами). Во-вторых, мы все время проповедуем геометрический подход. Для этого мы вводим

проективные системы, разбираем мотивированные этими системами выражения для спектров и так далее. В связи с этим мы сразу же обращаем внимание на высшие веса — очень естественные геометрические инварианты конфигурации точек.

Вторая глава содержит введение в теорию алгебраических кривых, коды в ней не упоминаются, но выбор материала главы отчасти определен запросами теории кодирования. В этой главе мы в основном работаем над алгебраически замкнутым полем. От основных понятий мы доходим до теоремы Римана–Роха, более подробно разбираем теорию эллиптических кривых. Наконец, мы переходим к алгебраически незамкнутому полю и вводим язык функциональных полей.

Геометрии над конечным полем посвящена третья глава. Мы сразу же начинаем работать с дзета-функцией и не скрываем нашего интереса к асимптотическим задачам. В этой главе много примеров. Относительно новыми являются асимптотические границы для числа точек на кривой и ее якобиане, подсчет числа дивизоров с заданными свойствами, теорема о структуре группы точек на эллиптической кривой над конечным полем, башни кривых с большим количеством точек. Теория глобальных полей и связанные с ней асимптотические дзета-функции отложены до «Дополнительных глав».

В четвертой главе описаны конструкции алгеброгеометрических кодов, их спектры, различные примеры, коды малых родов, двойственность и самодвойственность, и так далее. Кроме этого, мы говорим о задаче характеризации алгеброгеометрических кодов. Затем мы подробно разбираем различные асимптотические нижние границы алгеброгеометрического происхождения — эти границы особенно ярко демонстрируют силу алгеброгеометрических методов.

В конце книги в качестве приложения даны уравнения и таблицы асимптотических границ, таблицы параметров некоторых классов кодов и кодовых конструкций, таблица параметров двоичных кодов, построенных по алгеброгеометрическим, таблицы максимального числа точек на кривых заданного рода, а также таблицы параметров линейных кодов.

* * * * *

Теперь скажем два слова о самом интересном — о том, чего в этой книге нет. В «Дополнительных главах» мы хотели бы затронуть следующие темы, многие из которых возникли совсем недавно.

Во-первых, нельзя не коснуться декодирования алгеброгеометрических кодов, темы не только потенциально важной для приложений, но и порождающей небезынтересные геометрические задачи.

Во-вторых, куда более подробное изучение кривых с большим количеством точек, в том числе модулярных кривых и кривых Делиня–Люстига.

В-третьих, хотелось бы коснуться других задач, связанных с алгебро-геометрическими кодами общей идеологией. Таковы метрики Розенблюма–Цфасмана и их приложения к задачам планирования эксперимента и равномерным последовательностям, алгоритмы быстрого умножения в конечных полях, использующие модулярные кривые, аутентификационные коды, квантовые коды, коды над кольцами, графы без коротких циклов и многое другое.

В-четвертых, очень важный аналог кодов — решетки и упаковки шаров в евклидовых пространствах. Тут необходимо рассказать о типичном поведении случайных упаковок, об аддитивных и мультипликативных конструкциях плотных упаковок по полям алгебраических чисел, о нелинейных кодах Ленстры, о конструкции Элкиса–Шиоды упаковок по эллиптическим кривым над глобальными полями.

Пятый сюжет — многомерные многообразия над конечными полями и связанные с ними коды. Здесь естественно было бы подробнее поговорить о высших весах, об обобщениях кодов Рида–Маллера, о кодах по многообразиям Грассмана и Шуберта. Очень интересен вопрос о числе точек на поверхностях над конечным полем, как в плане границ, так и примеров. С теорией абелевых многообразий над конечными полями связаны такие темы как вопросы о структуре группы их точек, о статистике числа точек, о поведении собственных значений оператора Фробениуса.

И наконец, очень близкая нам тема — асимптотическая теория числовых и функциональных полей, башни полей и бесконечные расширения $\mathbb{Q}$ и $\mathbb{F}_q(t)$, их дзета-функции, обобщенная теорема Брауэра–Зигеля и многое другое.

Нам ясно, что даже при самом благоприятном развитии событий включить все перечисленное в «Дополнительные главы» никак не удастся. Но если бы нам удалось охватить хотя бы часть перечисленных тем, мы были бы уже очень довольны.

Не следует также забывать, что в то время как мы пишем эту книгу, многие математики, среди которых и Вы, читатель, получают или готовятся получить новые красивые результаты. Вряд ли можно надеяться, что мы за Вами успеем.

* * * * *

Мы (С. Влэдуц и М. Цфасман) глубоко благодарны нашему учителю Ю. И. Манину (привлекшему наше внимание к этой тематике), В. Г. Дринфельду (объяснившему нам свою теорию), Г. Л. Кацману (научившему нас теории кодирования), Л. А. Бассалыго (прояснившему для нас многие тонкости этой науки), Ж. Лашо (за многолетнее плодотворное сотрудничество и гостеприимство, благодаря которому мы имели возможность в течение ряда лет работать над материалом этой книги), А. М. Баргу (сделавшему

ряд ценных замечаний и предоставившему нам материалы, использованные в таблицах асимптотических границ), С. И. Гельфанду (уговорившему нас опубликовать работу об улучшении границы Варшамова–Гилберта), Г. А. Кабатянскому (сделавшему много ценных замечаний по тексту этой книги), С. Н. Лицыну (обратившему наше внимание на упаковки шаров в $\mathbb{R}^n$), М. Ю. Розенблюму (занимавшемуся с нами проблемой аналогов), А. Н. Скоробогатову (с которым обсуждались многие вопросы), А. Брауэру, Х. Ван дер Хееру и М. Ван дер Флюгту (написавшим приложения к этой книге) и многим другим математикам за их дружбу и помощь в работе над книгой.

Д. Ногин, кроме всех вышеназванных математиков, выражает благодарность своим соавторам, привлекшим его к этой работе.

Мы глубоко благодарны нашим родителям за их заботу о нас и нашим женам за их нежную к нам любовь.

Наши научные исследования во время работы над книгой были поддержаны грантами РФФИ 99-01-01204, 02-01-01041 и 02-01-22005. Электронные адреса авторов: vladut@iml.univ-mrs.fr, nogin@iitp.ru, tsfasman@iml.univ-mrs.fr.

Советы читателю

Цель этой книги — рассказ об алгеброгеометрических кодах, от введения до самых последних достижений. Не следует думать, что эта цель достигнута. Напротив того, поскольку область эта имеет уже почти четвертьвековую историю и насчитывает многие сотни работ, полный рассказ обо всех ее достижениях попросту невозможен. Поэтому мы ограничились созданием учебника, рассчитанного на читателя, работающего или собирающегося работать в этой или смежных областях. При этом мы не считали себя вправе рассчитывать на то, что читатель хорошо знаком с алгебраической геометрией или же с теорией корректирующих кодов. Поэтому в первых двух главах мы кратко излагаем необходимые нам далее результаты. Эти главы не призваны быть учебником по кодам или по алгебраической геометрии, хотя мы надеемся, что читатель, не знакомый с одной из этих дисциплин (или с обеими), запасшись долей трудолюбия, сможет получить некоторое представление о них, которое позволит ему работать в избранном им направлении.

В связи с упоминанием о трудолюбии уместно отметить особую роль упражнений, помещенных в книге: их много, и они составляют органичную часть текста. Их формулировки следует читать и осознавать наравне с остальными утверждениями книги. Если у читателя не возникло желания решить упражнение, то надо воспринимать его формулировку как предложение, даваемое без доказательства. Желательно все же хотя бы попытаться решить некоторое количество упражнений, поскольку это, несомненно, необходимо для твердого усвоения излагаемого материала. Большинство упражнений вполне доступны и для не слишком искушенного читателя.

Авторы льстят себя надеждой, что они умеют решать все упражнения. Те же упражнения, которые авторы решать не умеют, названы проблемами. (См., однако, сноску на стр. 8.)

Книга рассчитана на несколько различных категорий читателей.

Если Вы — специалист по кодам, заинтересованный в первую очередь в быстром ознакомлении с алгеброгеометрическими кодами, то мы рекомендуем начать с очень беглого чтения §§ 1.1 и 1.2, чтобы привыкнуть к нашей, не всегда стандартной, терминологии. При этом п. 1.1.2 мы рекомендуем изучить более тщательно. Далее следует прочесть пп. 2.1.1–2.1.3,

2.2.1, 2.2.2 и § 2.5. Затем попробуйте хотя бы частично прочесть §§ 2.4 и 3.3 и пп. 3.4.1 и 3.4.2. После этого можно переходить к четвертой главе, т. е. собственно к алгеброгеометрическим кодам. Вы заведомо сможете прочесть § 4.1 (кроме материала о самодвойственных кодах в п. 4.1.2) и § 4.5 (кроме п. 4.5.2). Для понимания материала о самодвойственных кодах в п. 4.1.2 необходимо прочесть п. 2.1.4, для понимания пункта 4.4.2 — пп. 2.4.1, 2.4.2 и часть § 3.3; перед прочтением пункта 4.5.2 следует прочесть пп. 2.1.4 и 3.2.4. Изучение этого материала при сравнительно небольших затратах дает довольно основательное знакомство с алгеброгеометрическими кодами. После этого советуем Вам бегло прочесть остальную часть книги.

Если Вы — специалист по кодам, интересующийся в первую очередь асимптотическими задачами теории кодирования, то Вам целесообразно начать с беглого чтения §§ 1.1 и 1.2 и более внимательного изучения § 1.3, содержащего материал, который обычно остается несколько в тени в монографиях по теории кодирования. Затем следует прочесть пункты 2.1.1–2.1.3, 2.2.1 и 2.2.2 и § 3.2. Теперь можно переходить к чтению § 4.5 (для чтения п. 4.5.2 необходимо прочесть еще пп. 2.1.4 и 3.2.4). Изучение этого материала дает хорошее представление об асимптотических возможностях алгеброгеометрических кодов. Затем мы советуем бегло прочесть все остальное.

Алгебраическому геометру, интересующемуся алгеброгеометрическими кодами как новой областью приложения алгебраической геометрии, мы советуем внимательно прочесть главу 1, а затем, просмотрев пункты 2.1.1–2.1.3, 2.2.1 и 2.2.2, изучить те из них, материалом которых Вы владеете не вполне свободно. Затем можно приступить к чтению главы 4, которое необходимо начинать с п. 4.1.1, после чего следует читать главу согласно одному из приведенных выше сценариев, в зависимости от Ваших интересов.

Если Вы — алгебраический геометр, желающий найти в алгеброгеометрических кодах новые алгеброгеометрические задачи, то после изучения главы 1 мы советуем Вам просмотреть главу 2, останавливаясь на тех разделах, с материалом которых Вы недостаточно знакомы. После этого внимательно изучите главу 3. Затем прочтите §§ 4.1 и 4.3 и переходите к §§ 4.5 и 4.6.

Если коды не интересуют Вас совсем, бегло просмотрев главу 2, Вы можете внимательно изучить главу 3. Таким образом, книга превращается в учебник алгебраической геометрии над конечным полем.

Теперь следует обратиться к наиболее многочисленной категории читателей. Если Вы не являетесь специалистом ни по кодам, ни по алгебраической геометрии и хотите возможно скорее освоиться в зоне их взаимодействия, мы рекомендуем Вам такую последовательность чтения: пункты 1.1.1, 1.1.2, 1.2.1, затем пункты 2.1.1–2.1.3, 2.2.1, 2.2.2, §§ 3.1 и 3.4.

В четвертой главе надо в первую очередь прочесть пункты 4.1.1, 4.1.2, 4.3.1, 4.4.2, 4.4.3. После этого Вы уже будете ориентироваться в алгебро-геометрических кодах. Затем можно читать остальной материал главы 4, обращаясь по мере необходимости к тем разделам глав 1 и 2, которые понадобятся по ходу чтения.

Наконец, если Вы — специалист по алгеброгеометрическим кодам, начните с оглавления, — в остальном Вы разберетесь сами. Не забудьте про историко-библиографические замечания.

Всем читателям мы еще раз горячо советуем пробовать решать хотя бы часть упражнений.

Можно еще посоветовать активно пользоваться таблицами и диаграммами, собранными в приложении, а также указателями обозначений и терминов.

Схема зависимости глав.

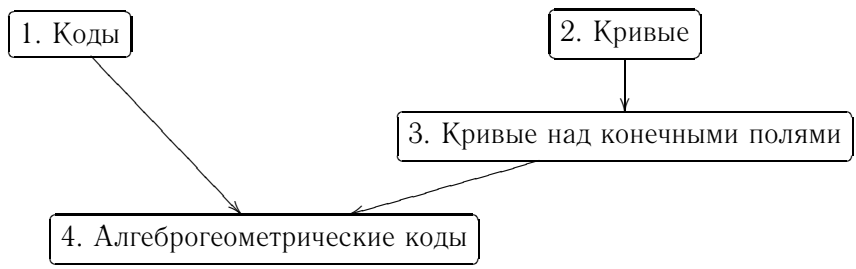
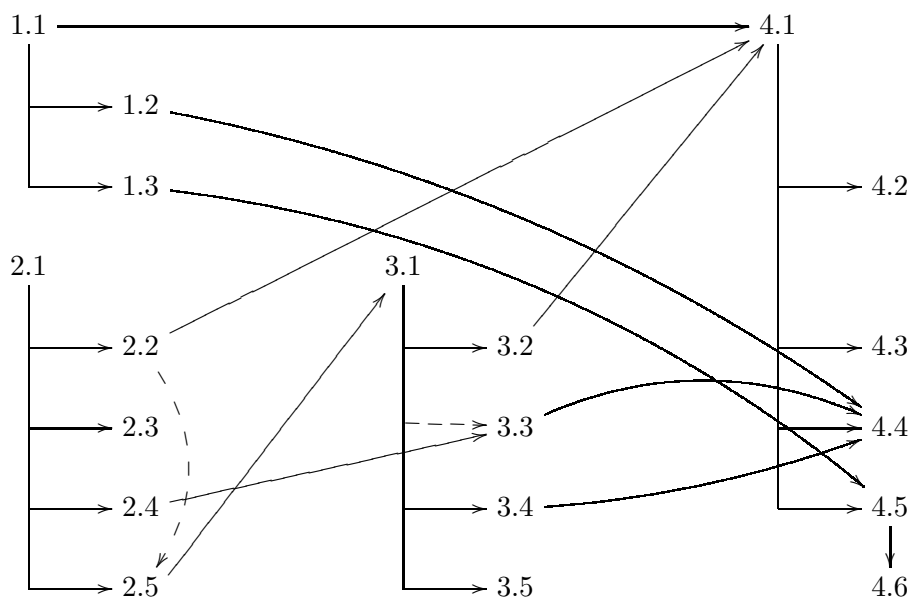


Схема зависимости параграфов.



Мы хотели бы также, во избежание недоразумений, отметить, что некоторые термины и обозначения, используемые в этой книге, иногда употребляются в несколько нестандартном смысле. В частности, всюду далее:

- запись $A \subset B$ означает, что A является *собственным* подмножеством B, то есть $A \neq B$, если же возможность $A = B$ не исключается, то мы пишем $A \subseteq B$; разность множеств обозначается $A \setminus B$;
- $[n, k, d]_q$-код может быть как линейным, так и нелинейным, в последнем случае k не обязательно целое, см. п. 1.1.1;
- для *алгеброгеометрических кодов* используются обозначения $(X, \mathcal{P}, D)_L$, $(X, \mathcal{P}, D)_\Omega$, и т. д., в то время как во многих работах они обозначаются, соответственно, $C(G, D)$ и $C^*(G, D)$, см. п. 4.1.1;
- через $\Omega(D)$ обозначается пространство
$$\Omega(D) = \{\omega \in \Omega(X)^* \mid (\omega) + D \geqslant 0\} \cup \{0\},$$
которое во многих работах обозначается $\Omega(-D)$, см. п. 2.1.1;
- при определении семейств кодов и кодовых конструкций мы, в основном сохраняя общеупотребительный смысл термина, иногда в деталях несколько отступаем от него, см. пп. 1.2.2 и 1.2.3;
- через $\lfloor x \rfloor$ обозначается целая часть числа $x \in \mathbb{R}$, то есть $\lfloor x \rfloor \in \mathbb{Z}$, $\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1$; а $\lceil x \rceil$ — целое число, такое что $x \leqslant \lceil x \rceil < x + 1$.