Preface

The book you hold in your hands is devoted to algebraic geometry codes, a comparatively young domain which emerged in the early 1980s at the meeting-point of several fields of mathematics. On the one side we see such respectable, well-developed, and difficult areas as algebraic geometry and algebraic number theory; on the other is a twentieth-century creation, information transmission theory (with its algebraic daughter, the theory of error-correcting codes), as well as combinatorics, finite geometries, dense sphere packings, and so on.

The relation between the two groups of domains, a priori distant from each other, was discovered by Valery Goppa. At the beginning of 1981 he presented his discovery at the algebra seminar of the Moscow State University; among the listeners there was Yuri Manin, who (being maybe the only one to understand), in turn, related the story at his seminar. One of the authors of this book (Tsfasman) was there and had the first chance in his life to hear the words *error-correcting code*. A couple of months later he, another author (Vlăduţ), and Thomas Zink wrote a small paper improving the asymptotic Gilbert–Varshamov bound. To the great astonishment of the authors, who were in doubt whether it was worth publishing or not, the world mathematical community, represented by both coding theorists and algebraic geometers, expressed lively interest. (All of a sudden, the authors found out that for a quarter of a century the asymptotic Gilbert–Varshamov bound had been attacked in vain, which had led to a widely spread—though not unanimous—opinion of its tightness.) This gave birth to a new domain, the algebraic geometry codes.

We (Tsfasman and Vlăduţ) were asked to write a book that could be of use to both coding specialists and algebraic geometers. The book [TV91] was published in 1991 by Kluwer Academic Publishers, and the Russian edition was scheduled and prepared for publication the same year by a Russian publisher, Nauka. The destiny of Russia was, however, different, which we by no means regret. The next time we were asked to publish the book in Russian came ten years later. By that time the book had become somewhat obsolete—the theory of algebraic geometry codes becoming twice as old—and we decided instead to write a new book in both English and Russian. The number of authors has increased, and the book has become two different books, being divided into *Basic Notions*, which you are reading now, and *Advanced Chapters*, yet to be written.

In the introduction to [TV91] we wrote that "the next decade will witness many new interesting results, methods, and problems in this fruitful area" and hoped for the book "to be of some use for those who choose this area for their own." We dare say that the prediction was correct and that the same words could be applied to this new book and to the decade to come.

To make the reading less tedious, we provide many exercises and problems.[1]

* * * * *

The main interests of the authors of this book lie where algebraic geometry meets number theory. This leads to a point of view on coding theory different from that of an insider. This part of the introduction is to explain this view. (We restrict ourselves to *block codes*, called *codes* from now on.)

A finite-dimensional vector space over a normed field ($\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}_p$, etc.) possesses a natural metric. Vector spaces over $\mathbb{Q}$ and other algebraic number fields, as well as free $\mathbb{Z}$-modules of finite rank, have different possible metrics linked to different embeddings of the corresponding field or ring in a normed one. The same for global fields in finite characteristic: $\mathbb{F}_q(T)$ and its finite algebraic extensions.

How can we introduce a metric space structure on $\mathbb{F}_q^n$, a finite-dimensional space over a finite field? We know no metric that is more natural than the *Hamming metric*:

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

i.e., the distance equals the number of different coordinates, the corresponding norm being

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

This norm has a serious disadvantage: it depends on the choice of a basis, but this is, alas, unavoidable.

Then, $\mathbb{F}_q^n$ being a metric space, we make a direct analogy with the classical problem to construct dense packings of equal spheres in $\mathbb{R}^n$ and get the problem to place in $\mathbb{F}_q^n$ as many balls of a given diameter d as possible so that the packing density be as large as possible (the volume on $\mathbb{F}_q^n$ is much more natural than the metric, the volume of a set being nothing more than its cardinality). An almost equivalent problem is to construct the largest subset $C \subseteq \mathbb{F}_q^n$ such that the distance between any two distinct elements is at least d. Such a subset C is called an $[n,k,d]_q$ *code*,[2] where $k = \log_q |C|$. The question of finding the largest code for given q, n, and d looks like a natural combinatorial problem.

Among all the codes, there is an organic subset of *linear codes*, i.e., codes $C \subseteq \mathbb{F}_q^n$ that are linear subspaces. There are at least three reasons to study linear codes. First, they are natural analogues of lattice sphere packings in $\mathbb{R}^n$. Next, they are easier to construct and give many good examples. The third reason—most important for us—is that linear $[n,k,d]$ codes correspond to *projective systems*, i.e., systems $\mathcal{P}$ of n points defined over $\mathbb{F}_q$ in the $(k-1)$-dimensional projective space $\mathbb{P}^{k-1}$ over $\mathbb{F}_q$. Moreover, $n-d$ equals the maximal number of points in $\mathcal{P}$ lying in a hyperplane (details are given in Sec. 1.1.2; such $\mathcal{P}$ are called *projective*

[1] We tried to follow the distinction, calling a question that we know the answer to an EXERCISE, sometimes giving hints to more difficult ones, and reserving the word PROBLEM for research problems and open questions. A rather instructive story happened with Exercise 1.3.23. This exercise—and its analogue for sphere packings—was given in [TV91]. It happened to be slightly more difficult than we thought it to be. Being asked how to solve it, one of the authors took some time to understand that probabilistic arguments do give the necessary result. The attempt to do the same exercise for sphere packing was also successful, several years of reflection easily providing the solution ([ST01]; see also [Bli05]).

[2] See Remark 1.1.2, explaining why it is called a code.

$[n,k,d]_q$-*systems*). We have thus arrived at another problem: how to place n points in $\mathbb{P}^{k-1}$ so that there are many of them outside any hyperplane (this is a general position type condition). Note that here we have gotten rid of both the basis in the ambient space and the metric we were not quite content with.

Having read the last paragraph, each algebraic geometer will ask, what if for $\mathcal{P}$ we take (a part of) $\mathbb{F}_q$-points of some algebraic variety W? If we take a curve, the answer is almost obvious. Let V be an algebraic curve defined over $\mathbb{F}_q$ together with its projective embedding $V \hookrightarrow \mathbb{P}^{k-1}$; then n is at most $|V(\mathbb{F}_q)|$, the number of $\mathbb{F}_q$-points of the curve V, and $n-d$ is at most the degree of the curve $V \subset \mathbb{P}^{k-1}$. The question of possible relations between n, k, and d becomes that of sheer algebraic geometry. The most important part of this book treats further properties of such codes.

The latter remark determines our view of mathematical coding theory. Codes over any finite field $\mathbb{F}_q$ are equally interesting for us (in spite of the fact that for applications one mostly uses binary codes, i.e., those over the field $\mathbb{F}_2$ or at least over its extension). Linear codes are of special interest. The main problem for us is that of finding possible parameters of a code (ideally, not only should one find them out but also produce a code having these particular parameters). This problem has several main forms. Here is the list (the field $\mathbb{F}_q$ is always fixed).

Let the code length n be fixed. For a given d, find the maximal $k = K(n,d)$ such that there exists an $[n,k,d]_q$ code (respectively, a linear $[n,k,d]_q$ code). A close problem is to find the maximal $d = D(n,k)$ for a fixed k. Note that, given an $[n,k,d]_q$ code, we easily construct $[n+1,k,d]_q$, $[n,k-1,d]_q$, and $[n,k,d-1]_q$ codes, so that solving these problems, we get not just the best possible parameters but also all possible parameters. The third problem of the same kind is to find the minimal $n = N(k,d)$ for given k and d.

Being unable to solve these problems completely, we cut the problem into two (for simplicity, let us consider the problem, say, to find $K(n,d)$). On the one hand, it is useful to look for some conditions to restrict parameters of any code. Such conditions would give an *upper bound* for the cardinality of a code, $K(n,d) \le K_{\mathrm{up}}(n,d)$; they are also called *possibility bounds*. On the other hand, it would be nice to produce explicit codes enjoying good parameters. Each of such codes (with given n and d) gives a *lower bound* $K_{\mathrm{low}}(n,d) \le K(n,d)$, also called an *existence bound*; it is natural that codes are usually constructed not individually but by vast classes. If for given n and d the upper bound equals the lower one, the problem is solved.

The main disadvantage of putting the problem this way is that we have not one problem but an infinite series of problems, and experience shows that we are extremely far from the general solution. As a partial answer for small values of n, one has tables of values of $K_{\mathrm{up}}(n,d)$ and $K_{\mathrm{low}}(n,d)$ (see [Bro] for online versions of such tables, maintained and regularly updated by A.E. Brouwer). These tables are good to compare new methods of code constriction with existing ones.

Another type of problem arises when we start to get interested in the behaviour of code parameters as n grows. Consider a family of codes with $n \to \infty$; how can k and d vary? A reasonable statement of an asymptotic problem always depends on certain knowledge of the actual behaviour of parameters at infinity. In our case, at least three asymptotic problems look natural (see precise statements in Sec. 1.3).

First: what is the asymptotic behaviour of k with respect to n for a fixed d? Here, the character of the answer is known. Put

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

then $0 < \varkappa_q(d) < \infty$, and the question of the exact value of or bounds for $\varkappa_q(d)$ is quite legitimate. It so happens that $\varkappa_q(d)/(d-1)$ is bounded from above and below by constants independent of d (roughly speaking, $1/2 \le \varkappa_q(d)/(d-1) \le (q-1)/q$ for any d).

Second: what is the behaviour of d with respect to n for a fixed k? The character of the answer is again known; moreover, the answer itself is known. Let

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

then

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

The third problem is, we feel, the most interesting. We call it the *main asymptotic problem*. Let $n, k, d \to \infty$, $k/n \to R$, $d/n \to \delta$; what is the dependence between R and δ? The question can be stated rigorously and happens to be highly nontrivial. The core of the book treats this problem. There are other asymptotic questions to ask, which, however, look more artificial.

This ends the first and most important (as we see it) subject of mathematical coding theory, the *parameter problem*.

We approach the second subject equipped with the experience of the first one. We know several upper bounds; do there exist codes whose parameters reach these bounds? Usually, these codes are characterized by a nice property, such as, for example, perfect and equidistant codes. Then we know many classes of codes, and we can ask what are possible parameters of codes in a given class (good examples are cyclic codes, self-dual ones, MDS codes, etc.). Properties of specific codes are also of interest: their weight spectra (see Sec. 1.1.3), their automorphism groups, their behaviour under a natural duality, and so on. This subject can be called the *property and structure problem*; questions here are various and very important.

We would like not only to be able to find out the best parameters but also to construct codes with given parameters more or less explicitly. To construct a code for a fixed n is to produce a construction algorithm (for example, for a linear code this means to produce its generator matrix). Of course, there always exists a "stupid" universal algorithm: sorting out all subsets or all linear subspaces of $\mathbb{F}_q^n$; we would like to exclude such solutions. A way to do it in the asymptotic setting is given by the algorithm complexity theory: let us demand the construction algorithms be polynomial in n (see Sec. 1.3.3 for details). As of today, it is the only rigorous setting of the problem of explicit construction of codes, and we stick to it. This is the third subject, the *constructiveness problem*.

There is a fourth subject, almost totally ignored in this book: codes good from the practical point of view. Here we should admit that codes are able to correct errors that occur while transmitting information distorted by random noise in a transmission channel of a certain type. Codes for practical use should mostly be binary or at least 2^m-ary for a small m; they need to be rather long, but not too

much; they must have not just a polynomial but a really simple and fast construction algorithm; and, not the least, they must enjoy a fast and simple decoding algorithm. This is a specific *problem of practical use*. This subject also puts forth interesting algebraic geometry problems; algebraic geometry codes have already led to significant progress in this direction.

And last, there is a subject that we may call the *problem of analogues*. We consider this problem to be the cornerstone for the role of coding theory in the whole building of modern mathematics. There is a beautiful analogy between linear codes and lattices in Euclidean spaces, corresponding to what is maybe the most fundamental analogy in mathematics, that between algebraic curves and number fields. Our interest in coding theory is due to a hope we can clarify this analogy.

The theory of algebraic geometry codes gave birth to many new problems in mother domains, including algebraic geometry and number theory. We hope to discuss all this in *Advanced Chapters*.

We believe that the possibilities of algebraic geometry codes are far from being exhausted and that this book will help to attract new forces to it.

* * * * *

The book is designed for mathematicians. The reader may or may not be acquainted with the main notions of coding theory and algebraic geometry.

The first two chapters are introductory. Chapter 1 is devoted to the basics of coding theory; algebraic geometry does not appear here explicitly, though in fact algebraic geometry codes determine the choice of material and results. There are few new results with respect to classical textbooks in coding theory. The main feature is that, first, we always work over an arbitrary finite field. Next, we profess the geometric approach whenever possible. To this end, we introduce projective systems, discuss spectra expressions motivated by these systems, and so on. This immediately attracts our attention to higher weights of codes, which are natural invariants of point configurations.

The second chapter provides an introduction to algebraic curves; codes are never mentioned, but the choice of topics is often determined by needs of coding theory. In this chapter we mostly work over an algebraically closed field. Starting from the very basics, we go as far as the Riemann–Roch theorem, discussing in some detail the theory of elliptic curves. At the end we pass to a nonclosed field and introduce the language of function fields.

Geometry over a finite field is the subject of the third chapter. We start to work with the zeta function from the very beginning and do not hide our interest in asymptotic problems. We give lots of examples. Relatively new are asymptotic bounds for the number of points on a curve and on its Jacobian, calculation of the number of divisors with prescribed properties, a theorem on the structure of the group of points of an elliptic curve over a finite field, and towers of curves with many points. We postpone the theory of infinite global fields and that of the asymptotic zeta functions to *Advanced Chapters*.

In the fourth chapter we discuss constructions of algebraic geometry codes, their spectra, many examples, codes of small genera, duality and self-duality, and so forth. We also consider the problem of characterization of algebraic geometry codes. Then we discuss in detail asymptotic lower bounds of algebraic geometry

origin; these bounds are most prominent to show the power of algebraic geometry methods.

As an appendix, we give equations and tables of asymptotic bounds, tables of parameters of different classes of codes and of various coding constructions, and bounds for some classes of linear codes.

* * * * *

Now let us give a brief list of the most interesting topics you are not going to find in this book. In *Advanced Chapters* we would like to discuss the following topics, many of which have emerged quite recently.

First of all, we cannot abstain from briefly touching on the decoding of algebraic geometry codes, a topic not only very important for applications but also attracting our attention to new algebraic geometry questions. We shall also discuss relations of algebraic geometry codes to other types of error-correcting codes such as LDPC (low-density parity-check) codes and expander codes.

Next, we shall consider in more detail curves with many points, including modular curves and Deligne–Lusztig curves.

Third, we would like to discuss other problems linked with algebraic geometry codes by the same ideology. Such are the Rosenbloom–Tsfasman metrics and their applications to experimental design and uniform sequences, fast multiplication algorithms in finite fields using modular curves, authentication codes, quantum codes, codes over rings, graphs without short cycles, and many others.

Fourth, there is a very important analogue of codes, lattices, and sphere packings in Euclidean spaces. Here one should relate typical properties of random lattices, additive and multiplicative constructions of dense packings from algebraic number fields, nonlinear Lenstra codes, and Elkies–Shioda constructions of packings related to elliptic curves over global fields.

The fifth topic is multi-dimensional varieties over finite fields and related codes. Here it would be natural to discuss higher weights, generalized Reed–Muller codes, and codes from Grassmann and Schubert varieties. There is a very interesting question of the number of points on a surface over a finite field, both bounds and examples. Then there is the theory of abelian varieties over a finite field, especially such topics as the structure of the set of their points, statistics for the number of points, and behaviour of the eigenvalues of the Frobenius operator.

And the last topic, dear to us, is the asymptotic theory of number and function fields, towers of global fields and infinite extensions of $\mathbb{Q}$ and $\mathbb{F}_q(t)$, their zeta functions, the generalized Brauer–Siegel theorem, and other "infinite" properties.

It is clear that, even in the best circumstances, the attempt to include all the above in *Advanced Chapters* is bound to fail. We shall be happy if we manage to discuss at least some of these subjects.

One should not forget that while we are writing these books, many mathematicians—to start with you, dear reader—are getting or preparing to get new, beautiful results. There is no hope that we can catch up with you.

* * * * *

We (Serge Vlăduţ and Michael Tsfasman) are deeply grateful to our teacher Yuri Ivanovich Manin (who attracted our attention to the topic); Vladimir Drinfeld

(for many interesting discussions of elliptic modules and modular curves); Gregory Katsman (who taught us coding theory); Leonid Bassalygo (who explained to us many coding subtleties); Gilles Lachaud (for many years of fruitful cooperation and hospitality, which helped us to write many chapters of the book); Alexander Barg (for many fruitful remarks and for the first version of tables of asymptotic bounds); Sergei Gelfand (for inducing us to publish our first paper improving the Gilbert–Varshamov bound); Gregory Kabatiansky (who made lots of valuable remarks reading the text of this book); Simon Litsyn (who attracted our attention to sphere packings in $\mathbb{R}^n$); Michael Rosenbloom (who worked with us on the problem of analogues); Alexei Skorobogatov (for many discussions); Andries Brouwer, Gerard van der Geer, and Marcel van der Vlught (who wrote appendices to the Russian edition of this book); members of the coding theory seminar and our colleagues from the Institute for Information Transmission Problems; and many other mathematicians for their friendship and help.

Dmitry Nogin thanks not only the above-named mathematicians but also his co-authors, who attracted him to undertake this work.

We are deeply grateful to our parents for their care and to our wives for their tender love.