Preface

The first volume of this book, *Algebraic Geometric Codes: Basic Notions*, was published by the AMS in 2007[1]. In that book we promised to complete it with the second one, *Algebraic Geometry Codes: Advanced Chapters.* Partly because of objective difficulties and partly due to our laziness, writing this book took us ten years.

For those who have already forgotten the content of the first volume, we have written an Appendix, where we present the basics of the theory and concisely recall main results.

We tried to make the text as clear and self-contained as possible; though this volume is addressed to a more experienced reader than the first one, we cannot claim that we have quite achieved this goal.

Somewhat to our own surprise we manage to cover almost all topics that we consider to be the main topics of the theory, and to fulfill the promises that we gave in the Preface to *Basic Notions* (with the exception of graphs without short cycles and codes over rings). Of course, there are many results which we were unable to cite in detail, as well as many co-adjacent domains.

We treat the following subjects: Curves with many $\mathbb{F}_q$-points, especially those attaining the Drinfeld–Vlăduţ bound, namely modular curves, classical and Drinfeld, and Elkies's explicit constructions. Class field theory and towers of curves therefrom. Oesterle bounds for the number of points. Examples of good curves, in particular curves of small genera, Deligne–Lusztig curves, recursive García–Stichtenoth towers, etc. Then we present our theory of infinite global fields, including the basic inequality and generalized Brauer–Siegel theorem, class field examples of towers, and so on. Decoding of algebraic geometry codes. Dense sphere packings, especially those that are good asymptotically, Elkies–Shioda lattices, class field constructions, and other links between number theory and algebraic geometry on one hand and lattices and sphere packings on the other. Then we touch on an intriguing subject of the number of $\mathbb{F}_q$-points on surfaces and multidimensional varieties, much less known than that on curves. And, of course, codes obtained from these varieties. There are some applications either of algebraic geometry codes directly or stylistically similar to them to fast multiplication, cryptography, quantum codes, and the like.

We hope that the book will be useful for the reader interested in algebraic geometry and number theory, as well as to one interested in what it gives for coding theory and other applications. The two volumes together form a mixture of a textbook for graduate and best undergraduate students, a handbook for specialists, and a reading for mathematicians specializing in other domains.

[1] See `https://bookstore.ams.org/surv-139`

* * * * *

Let us explain the choice of topics, chapter by chapter. Both volumes of this book are written for mathematicians of different specialties and basic education. We keep in mind specialists in coding theory, algebraic geometry, number theory, combinatorics, geometry, and so on.

In the first volume, Chapter 1 is an introduction to coding theory for those who do not know it, and a geometric view of it for those who do.

Chapter 2 is a compendium of algebraic geometry of curves we need.

Chapter 3 treats curves over finite fields, a subject that is in a sense closer to number theory than to classical algebraic geometry.

In Chapter 4 we skim off the cream, presenting what can be gotten for codes using algebraic curves.

In this volume we fill in the gaps and keep promises given in the first one.

Algebraic geometry codes with good parameters need curves with many points. There are several types of such constructions. Historically the first and one of the most beautiful is that of modular curves (Chapter 5).

Unfortunately, modular curves are not good over finite fields whose cardinality is not a square. And we know no analogue for number fields. The construction that works in these cases is that of class field towers (Chapter 6).

In Chapter 7 we treat other questions concerning curves with many points, in particular, the question of how to construct modular curves by explicit equations.

One of the most exciting sides of the theory and, in some sense, its *raison d'être*, is the parallelism between fields of functions of curves over finite fields and number fields. Together they are called *global fields*, and their theory is very beautiful and well developed. We try to go further. Being motivated initially by questions of the asymptotic behaviour of code parameters, and thus of the asymptotic behaviour of the number of points on curves in towers and families, in Chapter 8 we present the theory of infinite global fields and their zeta functions, which constitutes a very interesting part of the whole theory.

Chapter 9 is devoted to decoding of algebraic geometry codes, which is of primary importance for applications and also poses some interesting questions for algebraic geometers.

An old, nice problem of geometry—that of dense sphere packing (Chapter 10)—is linked to codes, as well as to number and function fields. The constructions that we present are close in spirit to those of algebraic geometry codes.

Multidimensional varieties over finite fields are much less studied than curves. In Chapter 11 we expose what is known about them and construct codes therefrom.

The last chapter (Chapter 12) presents some other applications and analogues of algebraic geometry codes, like fast multiplication in large finite fields, cryptography, quantum codes, and so on.

Since the first volume was published long ago, for the convenience of the reader we sum up its contents in the Appendix.

* * * * *

We permit ourselves to give to the reader some advice concerning different chapters of the present volume.

If you are interested in coding theory, you need constructions of good codes, their parameters, encoding, and decoding. Then you can read Chapter 9 (Decoding: Some Examples), Chapter 11 (Codes from Multidimensional Varieties, though it needs more knowledge of algebraic geometry), and, finally, Chapter 12 can also be interesting for you. As for the other chapters, they form the algebraic geometry and number theory base and expose the deep nature of the studied objects; correspondingly, the algebraic geometry and arithmetic prerequisites are more wide. If you are mostly interested in arithmetic geometry, you would like Chapters 6, 7, and especially Chapter 8. Chapter 10 gives a beautiful application to sphere packings.

For an algebraic geometer, Chapter 11 may be of utmost interest; however, it is better to read after Chapters 5 and 7.

If you are interested in number theory, read Chapters 6 and 8.

Those who like all these domains may wish to read the whole book.

* * * * *

We are especially interested in the links and interchanges of different parts of mathematics that we see in the domain. Let us list some of these meeting-points.

1. *Codes and algebraic varieties over finite fields.* This is the main topic of the first volume [**TV91**], especially in the case of curves; see the Appendix. A linear code is equivalent to a multiset of points in $\mathbb{P}^{k-1}$; see Sec. A.1. Then it is natural to consider codes corresponding to $\mathbb{F}_q$-points of algebraic varieties, curves in particular. This leads us to many questions about curves—but also about multidimensional varieties—over finite fields.

2. *Codes and packings.* A good error-correcting code is a dense packing of equal spheres in the Hamming space $\mathbb{F}_q^n$. Thus, we are bound to look at the sphere packing problem in other spaces, in particular, that in the Euclidean space $\mathbb{R}^n$. In this setting a linear code corresponds to a lattice packing, and there are many ways to construct rather dense packings from codes with good parameters; see Chapter 10.

3. *Number fields, curves, and sphere packings.* Natural constructions of lattices from number fields known for two centuries extend to constructions of lattices from curves. Both happen to lead to dense sphere packings; see Chapter 10.

4. *Algebraic curves over finite fields and number fields.* The main question we get is to find out the number of points of a curve over the ground field and over its finite extensions. They are assembled together in the notion of the zeta function of the curve. With this notion, calculus enters into the picture together with algebra and geometry. If we look at the theory of curves from an algebraic point of view, we see one of the utmost gems of modern mathematics, the parallelism between curves over finite fields and number fields, i.e., finite extensions of $\mathbb{Q}$. We see this in Chapters 6 and 8, and keep it in mind everywhere.

5. *Curves with many points and modular functions.* This same theory leads to modular curves, giving us examples of large genus curves with many points; see Chapter 5. In geometric language this is a part of another gem and the center of modern mathematics, moduli spaces. Note that the recent solution of the densest sphere packing problem in dimensions 8 and 24 also uses modular functions.

6. *Curves, varieties, and group theory.* The group theory and the algebraic group theory appear when we consider class field towers (Chapter 6) and when

we look for varieties with many points (Deligne–Lusztig varieties, Grassmannians, and so on); automorphism groups of varieties, especially those of curves, are also sometimes important for applications.

7. *Asymptotic parameters of families of codes and limit zeta functions.* To find and study codes of large length, we set asymptotic questions: what happens when the parameters tend to infinity? This corresponds to the asymptotic study of zeta functions of families of algebraic varieties and number fields as the genus of the curve (the discriminant of the field) tends to infinity. At present we have a beautiful—though highly incomplete—theory of limit zeta functions; see Chapter 8. Since a zeta function is characterized by the set of its zeroes, in the limit we get a measure on the critical line, and a study of such measures adds another analytic taste to our geometric and arithmetic objects.

* * * * *

It may be useful to point out the interdependence of these topics. Roughly speaking, the first four chapters (Chapters 5–8, the enumeration being continuous throughout both volumes of the book) are linearly ordered, i.e., each chapter uses something from the preceding ones. On the contrary, Chapters 9–12 are essentially independent of each other, as well as of Chapters 5–8.

Acknowledgments. Our research while working on this book was supported by the French National Scientific Research Center (CNRS), in particular by the Institut de Mathématique de Luminy, the Institut de Mathématiques de Marseille, the French–Russian Poncelet laboratory, and the Laboratoire de Mathématique de Versailles; by the Institute for Information Transmission Problems; and by the Independent University of Moscow. It was also supported in part by the Russian Science Foundation (project no. 14-50-00150) and by ANR project FLAIR (ANR-17-CE40-0012).