BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 27, Number 2, October 1992

0273-0979/92 $1.00 + $.25 per page

Algebraic-geometric codes, by M. A. Tsfasman and S. G. Vlăduţ. Kluwer Academic Publishers, Dordrecht, Boston and London, 1991, xxiv+667 pp., $229.00. ISBN 0-7923-0727-5

In the theory of error-correcting codes a *code* C is a subset of Q^n where Q is a finite set called the *alphabet*. The elements of C are called *codewords* (or *vectors*) and n is called the *wordlength*. In practice, the codewords are messages that are sent over a so-called "noisy" channel to a receiver. The channel has the effect that if a codeword $\mathbf{c}$ is sent, the received word $\mathbf{r}$ may differ from $\mathbf{c}$ in a number of places. We say that *errors* occur in the received message. In the set Q^n a distance function is introduced by

$$d(\mathbf{x}, \mathbf{y}) := |\{i : 1 \leq i \leq n,\ x_i \neq y_i\}|.$$

The *minimum distance* d of the code C is defined by

$$d := \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x} \in C,\ \mathbf{y} \in C,\ \mathbf{x} \neq \mathbf{y}\}.$$

If $d = 2e + 1$, then the code C is called an e-error-correcting code because if a received word $\mathbf{r}$ has distance $\leq e$ to the transmitted message $\mathbf{c}$, the receiver can "correct" the errors and retrieve the word $\mathbf{c}$, since the distance from $\mathbf{r}$ to all other codewords is larger than e.

Shannon's paper (1948) on the mathematical theory of communication [8] marks the beginning of coding theory. Since then, most of the theory has been concerned with so-called *linear codes*. For the alphabet Q one chooses a finite field $\mathbb{F}_q$ and the code C is a linear subspace of $\mathbb{F}_q^n$. If C has dimension k, then C is called an $[n, k]$ code. The easiest situation is that of a *systematic* code C, where the first k coordinates $c_1, \ldots, c_k$ of codewords $\mathbf{c}$ take on all q^k possible values and the code is obtained by a mapping from $\mathbb{F}_q^k$, to $\mathbb{F}_q^n$ that adjoins "redundant" symbols $c_{k+1}, \ldots, c_n$. The efficiency of C for transmission of information is measured by the ratio k/n, which is called the *information rate* of C.

If C is a q-ary $[n, k]$ code with minimum distance d, then two distinct codewords cannot be identical on the first $n - (d - 1)$ positions and, therefore, the number of codewords cannot exceed q^{n-d+1}. This yields what is known as the Singleton bound

$$d \leq n - k + 1.$$

If equality holds in this bound, then the code is called a maximum distance separable code (MDS code). Here the word separable indicates that the code is systematic on any k coordinate positions (trivially). For a linear code C, the *dual code* $C^\perp$ is defined by

$$C^\perp := \{\mathbf{y} \in \mathbb{F}_q^n : \forall_{\mathbf{x} \in C}[\langle \mathbf{x}, \mathbf{y} \rangle = 0]\},$$

where $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^n x_i y_i$ is the usual inner product. It is an easy exercise to show that the dual of an MDS code is also an MDS code. This occurrence in pairs of codes that are in some sense "good" is also a feature of the algebraic-geometric codes treated in the book under review.

If a code C in $\mathbb{F}_q^n$ has minimum distance d and if adjoining any word that is not in the code to C results in a new code with smaller minimum distance, then the following inequality is obvious:

$$|C| \cdot \sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i \geq q^n .$$

This lower bound on the size of maximal codes is known as the Gilbert-Varshamov bound. It was proved in the 1950s, the second author proving the somewhat surprising fact that requiring C to be a linear code does not give a smaller bound. For more than thirty years this elementary bound was not improved. This explains that the paper [10] by Zink and the two authors of the book under review, yielding a better lower bound by using deep results from algebraic geometry, was a sensation for coding theorists. For this paper they received the IEEE best paper award (1983).

To be able to appreciate the introduction of algebraic geometry into this area of mathematics, we must first explain the structure of the class of codes that is most widely used in practice. (Surely the most impressive example of application of these codes is the compact disc; the incredible quality of the sound would not be possible without coding theory. The reason why the codes treated below are used, and not other "better" codes, is the fact that a very fast algorithm for locating and correcting errors is known for these codes. The mathematically fascinating codes from algebraic geometry are still quite far from being useful in practice. Some readers may consider that an asset; chacun son goût.) The codes are known as Reed-Solomon codes (RS codes).

Let the alphabet be $\mathbb{F}_q = \{\alpha_0, \ldots, \alpha_{q-1}\}$. Consider the k-dimensional vector space L of polynomials $f(x)$ of degree $< k$ in $\mathbb{F}_q[x]$. The code C of length $n = q$ is obtained by the linear mapping that sends $f(x)$ to $(f(\alpha_0), \ldots, f(\alpha_{q-1}))$. Since a polynomial of degree l in $\mathbb{F}_q[x]$ has at most l zeros, the code C has minimum distance at least $n-(k-1)$. By the Singleton bound, C must be an MDS code.

The fact that these codes are "best possible" in a sense and that they have a fast decoding algorithm does not mean that the subject of coding theory ends with these codes. The famous paper by Shannon, mentioned above, showed that for channels with a probability p of a symbol being received as an error, there is a corresponding information rate $R(p)$, such that codes exist with rate arbitrarily close to $R(p)$, for which the probability of error after decoding is arbitrarily small. In this theory, the alphabet is fixed and the codes (whose existence is proved but we still are nowhere near constructing any) have very large length n. The RS codes have length equal to the alphabet size, so they may be good and, in fact, extremely useful but they have nothing to do with "good" codes in the sense of Shannon. The codes constructed using algebraic geometry do not achieve equality in the Singleton bound (they get close), but they have the advantage that the length n can be very much larger than q.

A final step in introducing the algebraic-geometric codes is the following geometric reformulation of the definition of RS codes. Let $\mathbb{F}$ be the algebraic closure of $\mathbb{F}_q$ and let X be the projective line over $\mathbb{F}$. The rational points on X are $P_i := (\alpha_i, 1)$, $(0 \leq i \leq q-1)$ and $Q := (1, 0)$. Let $\mathscr{L}$ be the space of rational functions on X, with coefficients in $\mathbb{F}_q$, that are defined at all the

points P_i and that have a pole of order less than k in Q (possibly no pole) and, furthermore, have no poles on X. We map $\mathscr{L}$ to a q-ary code by letting the rational function $f \in \mathscr{L}$ correspond to the codeword $(f(P_0), \ldots, f(P_{q-1}))$. Since $\mathbb{F}$ is closed, it is obvious that $\mathscr{L}$ is simply the space L used in the definition of RS codes, with the variable x replaced by x/y. In this way, a vector space of rational functions defined on the projective line is mapped to a linear code by taking values of the functions at a specified set of points of the line to be the coordinates of the words. The set of rational functions was defined by a restriction on the possible poles and their orders. The simplest way of explaining what algebraic-geometry codes are is to replace X by some other (nonsingular, smooth) projective curve. We will be more precise below. Similar to the RS codes, the codes from algebraic geometry will occur in pairs (a code and its dual).

The book by Tsfasman and Vlăduţ has two introductory chapters. The first of these is an introduction to coding theory. This contains the necessary definitions and some elementary theory, a number of examples of well-known codes, and a section on bounds. Asymptotic bounds are treated thoroughly so that the reader will be able to appreciate the improvement of the asymptotic Gilbert-Varshamov bound given in Chapter 3. Instead of the standard terminology of coding, q-ary $[n, k, d]$ code, the authors prefer the concept of *projective* $[n, k, d]_q$ *system*, a basisfree definition of an equivalence class of codes. This makes the exposition more geometric. The second chapter contains the algebraic geometry that is needed. This has algebraic curves, divisors and differential forms, the Riemann-Roch theorem (the most essential tool; the proof is only sketched) and the Hurwitz formula, rational points, elliptic curves, singular curves, and a section on reductions and schemes.

In their little introductory book on codes and algebraic geometry, G. van der Geer and the reviewer [6] observe that one can review basic notions from algebraic geometry but that the reader, who really wishes to apply algebraic geometry to coding, must first work his way through a standard textbook. The same holds for the present volume. The algebraic geometry used in the remaining three chapters (i.e., the essential part) of the book is much too difficult for a reader who is not already familiar with this area. Chapter 2 (163 pages) provides an excellent memory refresher for the reader, who has some knowledge of the field. In the more precise definition of algebraic-geometric codes given below we adopt the same point of view, i.e., we assume that the reader of this review knows the concepts that are used (nonsingular curves, rational points, divisors, differential forms). For a short introduction we refer to [5]. If D is a divisor on a curve X, then we use the usual notation $\mathscr{L}(D)$ for the vector space over the (specified) field K defined by

$$\mathscr{L}(D) := \{f \in K(X)^* : (f) + D \geq 0\} \cup \{0\},$$

where $K(X)$ is the field of rational functions on X.

Similarly, the space of differentials ω on X such that $(\omega) - D \geq 0$ is denoted by $\Omega(D)$.

Although the paper by Zink and the present authors triggered the tremendous interest in the relation between coding and algebraic geometry, the idea of the codes is due to Goppa [2]. In his prize-winning paper of 1970 [3], he defined a class of codes that generalize RS and the well-known BCH codes. These codes

became known as Goppa codes but have now been renamed "classical" Goppa codes, since the codes from algebraic geometry also deserve to be known as Goppa codes. Once again, the idea of generalizing RS codes has led to a great discovery. In their preface, the authors state that Yu. I. Manin was the first to understand and appreciate the link between the seemingly unrelated parts of mathematics. This led to research on the number of points on curves over a finite field and a seminar on the subject, where the authors were present, etc.!

Let X be a nonsingular projective curve defined over the field $\mathbb{F}_q$ and let $P_1, \cdots, P_n$ be rational points on X. Let D be the divisor $P_1 + \cdots + P_n$, and let G be a divisor on X with support disjoint from D. The first Goppa code associated with the pair D, G is the linear code $C(D, G)$, which is the image of the linear mapping $\alpha: \mathscr{L}(G) \to \mathbb{F}_q^n$ defined by $\alpha(f) := (f(P_1), \ldots, f(P_n))$.

The other Goppa code is the code $C^*(D, G)$, which is the image of the linear mapping $\alpha^*: \Omega(G - D) \to \mathbb{F}_q^n$ defined by

$$\alpha^*(\eta) := (\mathrm{Res}_{P_1}(\eta), \ldots, \mathrm{Res}_{P_n}(\eta)).$$

The dimension and a bound on the minimum distance of these codes are found by using the Riemann-Roch theorem. The codes $C(D, G)$ and $C^*(D, G)$ are duals, which follows from the residue theorem.

These codes are introduced in Chapter 3 (in both senses, the central one). The algebraic geometry treated in Chapter 2 suffices to appreciate this main chapter. As examples, codes of small genera are treated ($g = 0$ corresponds to RS and BCH codes), e.g., elliptic codes ($g = 1$) and also codes corresponding to curves with the maximum possible number of rational points. Furthermore hermitian codes and hyperelliptic codes are treated (the names being derived from the curves).

The third section of this chapter is devoted to decoding algorithms, the topic of interest to those who actually hope to use these codes in practice. An anecdote must be saved for posterity. The reviewer gave a talk about codes from algebraic geometry in Denmark some years ago, explaining their incredibly good parameters. From the audience Justesen commented that his experience as an engineer told him that codes that were that good had to be very much longer, so there must be some mistake in the theory. On the way home (a long train ride) he convinced himself that the geometers had made no mistake and a year later he and his collaborators [4] had designed the first good decoding algorithm for these codes! Their ideas were made precise by Skorobogatov and Vlăduţ [9] and the procedure was improved considerably (in theory) by Pellikaan [7].

The final section of this chapter presents the asymptotic results, i.e., the improvement of the Gilbert-Varshamov bound. The improvement depends on a sequence of codes coming from a sequence of modular curves. These codes are the topic of Chapter 4, in which both classical modular curves and Drinfeld curves are treated. Although there are many differences between these curves, both types have many rational points (with respect to their genus), which is the key to the good asymptotic results. This chapter and the final one are only suitable for experts in number theory and algebraic geometry.

A *sphere-packing* in $\mathbb{R}^n$ is an arrangement of equal spheres such that no point of the space is in more than one of the spheres. Many of the best known packings are obtained from *lattices*. A number of authors have studied the connection between lattices and sphere-packings on the one hand and binary codes on the

other. The simplest example of such a connection is the lattice that has as centers all vectors $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$ for which $\sqrt{2}\mathbf{x} \pmod 2 \in C$, where C is a binary code. Most of what is known in this area can be found in the book by Conway and Sloane [1]. Chapter 5 of the book under review starts with a treatment of this connection and shows how codes from algebraic geometry lead to good sphere-packings. The main results are of an asymptotic nature. The essential part of the chapter treats codes that are analogues of codes from algebraic geometry, now based on algebraic number fields. The corresponding lattices are always mentioned.

It is clear that this book is a valuable addition to the existing literature on this fairly young field. The expert will definitely need to have it in his library. For this he must pay the exorbitant price of the book. The least one could expect from the publisher to justify the cost would be a copy editor to have corrected the often clumsy English; (for example, the article is missing very often where it is required but occurs where it should not). The reviewer was disturbed by many mistakes in the references and confused by some of the strange notation, e.g., $\lceil x \rceil$ where others use $\lfloor x \rfloor$. The authors expect the next decade to witness many new results in this area. They are probably right and their book will contribute to the research that produces these results!

References

1. J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, Springer-Verlag, New York, 1988.
2. V. D. Goppa, *Codes on algebraic curves*, Soviet Math. Dokl. **24** (1981), 170–172.
3. ———, *A new class of linear error-correcting codes*, Problems Inform. Transmission **6** (1970), 207–212.
3. J. Justesen, K. J. Larsen, H.. Elbrønd Jensen, Al Havemose, and T. Høholdt, *Construction and decoding of a class of algebraic geometry codes*, IEEE Trans. Inform. Theory **IT-35** (1989), 811–821.
5. J. H. van Lint, *Algebraic geometric codes*, Coding Theory and Design Theory (D. Ray-Chaudhuri, ed.), vol. 1, Springer-Verlag, New York, 1990, pp. 137–162.
6. J. H. van Lint and G. van der Geer, *Introduction to coding theory and algebraic geometry*, Birkhäuser Verlag, Boston and Berlin, 1988.
7. R. Pellikaan, *On a decoding algorithm for codes on maximal curves*, IEEE Trans. Inform. Theory **IT-35** (1989), 1228–1232.
8. C. E. Shannon, *A mathematical theory of communication*, Bell Syst. Tech. J. **27** (1948), 379–423 and 623–656.
9. A. N. Skorobogatov and S. G. Vlăduţ, *On the decoding of algebraic geometric codes*, IEEE Trans. Inform. Theory **IT-36** (1990), 1051–1060.
10. M. A. Tsfasman, S. G. Vlăduţ, and Th. Zink, *Goppa codes that are better than the Varshamov-Gilbert bound*, Problems Inform. Transmission **18** (1982), 163–165.

J. H. van Lint
Eindhoven University of Technology, Netherlands
E-mail address: wsdwjhvl@urc.tue.nl