

BOOK REVIEW

Algebraic curves over finite fields, by C. J. Moreno. Cambridge University Press, Cambridge, 1991, ix+246 pp. \$49.50. ISBN 0-521-34252-X

Confessions of a reviewer. Reviewer to himself. Great! I am glad to have been asked to review Moreno's book. Now that I will have two copies, I can keep one at home and one at the university. I will have to read it and thus hope that my first glance of it, in which the first chapter seemed too difficult, was deceptive. After all, it should be just up my street with a background in classical algebraic geometry and the combinatorics of finite projective spaces. Also, since I have been giving expository talks for some years on the Hasse-Weil theorem and Goppa codes, I will be able to learn about those parts I did not fully understand such as the proof of the Riemann hypothesis for curves and the modular curves $X_0(N)$, which give a counterexample to the hypothesis that the Gilbert-Varshamov bound is best possible.

Reviewer to reader. Mathematicians, as other scientists, hunt in separate groups mostly making minimal contact with other groups at a research level; so there is a real frisson of excitement when a new development brings disparate groups together.

In 1981 Goppa derived a class of linear codes from algebraic curves over finite fields, which (1) are quite general as codes, (2) have parameters circumscribed by the Riemann-Roch theorem, and (3) have asymptotic properties which improve the classical Gilbert-Varshamov bound. The discovery of these codes also gave renewed stimulus to investigations on the number of points on an algebraic curve for a particular genus as well as to asymptotic values of the ratio of the number of points to the genus. The Goppa codes therefore link algebraic geometry, number theory, and coding theory.

The interest in this topic is demonstrated by the number of survey articles [1, 6, 10, 14–18] and books [11, 13] that have appeared.

Reviewer to author. I like the first sentence of the preface: "This is an introduction to the theory of algebraic curves over finite fields." The last sentence I find somewhat mystifying: "Chapter 5 on error correcting codes and the appendix may be studied independently from the rest of the book; they are intended mostly for workers in the field who want to understand the new results about codes on algebraic curves over finite fields." Does this mean that coding theorists should not read the rest of the book and that it will give them no preparation for Chapter 5 or does it mean that it is the place for algebraic geometers to look to understand the applications to coding theory?

Reviewer to reader. Let \mathbf{F}_q be the finite field of q elements and let $(\mathbf{F}_q)^n$ be considered as a vector space. Then a q -ary $[n, k, d]$ -code C is a subspace of $(\mathbf{F}_q)^n$ of k dimensions such that the minimum number of nonzero coordinates in any element of $C \setminus \{0\}$ is d , the *minimum distance*; such a code corrects $\lfloor \frac{1}{2}(d-1) \rfloor$ errors. The minimum distance has the upper (Singleton) bound: $d \leq n - k + 1$. The Main Coding Theory Problem for linear codes is to find codes optimizing the third parameter among n, k, d when the other two are fixed. Another view is to define $R = k/n, \delta = d/n$; then for fixed δ , let $\alpha(\delta) = \limsup_{n \rightarrow \infty} R$. The result of Gilbert-Varshamov is that $\alpha(\delta) \geq 1 - H(\delta)$ where H is the entropy function given by $H(0) = 0, H(t) = t \log_q(q-1) - t \log_q t - (1-t) \log_q(1-t)$ for $0 < t < (q-1)/q$; also $\alpha(\delta) = 0$ for $(q-1)/q \leq \delta \leq 1$. It was long thought that this theorem gave the best lower bound.

Now to turn to algebraic geometry. It will suffice here to consider plane curves. Let F be a ternary, homogeneous polynomial over \mathbf{F}_q and let $V(F)$ be the set of zeros of F in the projective plane $PG(2, q)$. Let us regard the corresponding *curve* \mathcal{C} as a triple $(q, (F), V(F))$ where (F) is the ideal generated by F in $\mathbf{F}_q[X, Y, Z]$. A *rational point* of \mathcal{C} is an element of $V(F)$; however, a *point* of \mathcal{C} is a zero of F in $PG(2, q^r)$ for some r , that is, \mathcal{C} carries with it the zeros of F in any extension of \mathbf{F}_q .

A point $P = (x, y, z)$ of \mathcal{C} is *singular* if $\partial F/\partial X = \partial F/\partial Y = \partial F/\partial Z = 0$ at (x, y, z) . We note that a singular point does not have to be a rational point. For example, if $q \equiv -1 \pmod{4}$ and $F = (X^2 + Y^2)^2 + (X^2 - Y^2)Z^2 + Z^4$, then \mathcal{C} has the singularities $(1, \pm i, 0)$, where $i^2 = -1$, which lie in $PG(2, q^2)$ but not in $PG(2, q)$.

Reviewer to author. Having now looked through Chapter 1, I have a distinct sense of foreboding. The only example states that the curves with affine equation $y^2 - y = x^3 - x^2$ over \mathbf{F}_{11} has a singularity at $x = -3$. It would have been helpful for the nonexpert had it been stated that $(-3, -5)$ satisfies the equation and both partial derivatives are zero at this point. You do state that you are giving only a “summary of key results,” but to do this without examples is terrifying. In the exercises at the end of Chapter 1 numbers 4 and 6 are contradictory. Exercise 6 implies that over \mathbf{F}_q the curve with $F = X^4 + Y^4 + Z^4$ has an automorphism group $U_3(\mathbf{F}_3)$ ($= PSU(3, 9)$) which has order 63.96, whereas exercise 4 would imply that 96 is the maximum possible order.

From the first paragraph of Chapter 2 it is clear that it is crucial to have understood discrete valuation rings of the function field of a curve since they, referred to as *closed points*, are the elements from which divisors are defined. It is already clear to me that I have previously been working with an inadequate notion of a divisor. By the end of Chapter 2, I am still looking in vain for some example that might help me or any other reader understand divisors and all the associated notions. If ever there was a subject in which examples were both easy to give and enlightening, this is one.

Reviewer to reader. Let F be absolutely irreducible over \mathbf{F}_q and define a divisor on \mathcal{C} as $D = \sum n_P P$ where P is a point of \mathcal{C} (not necessarily rational), $n_P \in \mathbf{Z}$, and $n_P = 0$ for all but a finite number of P and the *degree* of D as $\deg D = \sum n_P$. Also D is *effective* or *positive* if $n_P \geq 0$ for all P . The divisors form a free abelian group $\text{Div}(\mathcal{C})$. Now, this is not really good enough. We should consider a subgroup $\text{Div}^*(\mathcal{C})$ of $\text{Div}(\mathcal{C})$, which is defined as follows: if $D = \sum n_P P \in \text{Div}^*(\mathcal{C})$ with

$Q \in PG(2, q^r) \cap \text{supp } D$, then all the conjugates of Q occur in D with the same coefficient.

Let us illustrate with $F = X^3 + Y^3 + Z^3$ and groundfield \mathbf{F}_2 . We require $\mathbf{F}_4 = \{0, 1, \omega, \omega^2 \mid \omega^2 + \omega + 1 = 0\}$ and $\mathbf{F}_8 = \{0, 1, \varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4, \varepsilon^5, \varepsilon^6 \mid \varepsilon^3 + \varepsilon^2 + 1 = 0\}$. The points of \mathcal{C} over \mathbf{F}_2 are $\{P_0 = (0, 1, 1), P_1 = (1, 0, 1), P_2 = (1, 1, 0)\}$; over \mathbf{F}_4 are $\{P_0, P_1, P_2, Q_0 = (0, 1, \omega), Q_0^2 = (0, 1, \omega^2), Q_1 = (1, 0, \omega), Q_1^2 = (1, 0, \omega^2), Q_2 = (1, \omega, 0), Q_2^2 = (1, \omega^2, 0)\}$, and over \mathbf{F}_8 are $\{P_0, P_1, P_2, R_1 = (1, \varepsilon, \varepsilon^3), R_1^2 = (1, \varepsilon^2, \varepsilon^6), R_1^4 = (1, \varepsilon^4, \varepsilon^5), R_2 = (1, \varepsilon^3, \varepsilon), R_2^2 = (1, \varepsilon^6, \varepsilon^2), R_2^4 = (1, \varepsilon^5, \varepsilon^4)\}$.

The effective divisors in $\text{Div}^*(\mathcal{C})$

of degree 1 are P_0, P_1, P_2 (a total of 3);

of degree 2 are $2P_i, Q_i + Q_i^2, P_i + P_j$ (a total of 9);

of degree 3 are $3P_i, 2P_i + P_j, P_0 + P_1 + P_2, P_i + Q_j + Q_j^2, R_i + R_i^2 + R_i^4$ (a total of 21).

For f in the function field $K(\mathcal{C})$ of \mathcal{C} let (f) be the associated divisor. With $D = \sum n_P P$ let us take $L(D) = \{f \in K(\mathcal{C}) \mid (f) + D > 0\} \cup \{0\}$; that is, $L(D)$ contains those elements of the function field whose associated divisor has poles of order not greater than n_P at P . For example, if $\mathcal{C} = (4, (X^3 + Y^3 + Z^3), V(F))$ and $D = 3P_0$ then $f_1 = X/(Y + Z)$ has $(f_1) = P_0 + Q_0 + Q_0^2 - 3P_0 = Q_0 + Q_0^2 - 2P_0$ and $f_2 = Y/(Y + Z)$ has $(f_2) = P_1 + Q_1 + Q_1^2 - 3P_0$; thus f_1 has a pole of order 2 at P_0 and f_2 a pole of order 3, whence both f_1 and f_2 are in $L(3P_0)$.

Reviewer to author. Now that I have reached Chapter 5, I cannot understand why §§5.2 and 5.4 are not at the start of the book, because many of my and perhaps other readers' difficulties would have been alleviated.

Reviewer to reader. To give the essential idea of Goppa codes, it now suffices to give Riemann's theorem rather than the Riemann-Roch theorem: if $l(D) = \dim L(D)$, then $l(D) \geq \deg D + 1 - g$ with equality if $\deg D > 2g - 2$, where g is the genus of the curve \mathcal{C} .

To construct the codes that we want, let $D = P_1 + \cdots + P_n$, where the P_i are distinct points in $V(F)$ and let E be a divisor of degree m with support disjoint from D . Then let $\theta: L(E) \rightarrow (\mathbf{F}_q)^n$ be given by $\theta(f) = (f(P_1), \dots, f(P_n))$, and denote the image of θ by $C(D, E)$. Let us also take $n > m > 2g - 2$. The code $C(D, E)$ is an $[n, k, d]$ -code with $n \leq N_1$ where (i) $|N_1 - (q + 1)| \leq 2g\sqrt{q}$; (ii) $k = m + 1 - g$; (iii) $d \geq n - m$. Part (i) is the Hasse-Weil estimate; parts (ii) and (iii) follow from Riemann's theorem.

As a corollary, it follows immediately that

$$(i) \quad n - k + 1 \geq d \geq n - k + 1 - g;$$

$$(ii) \quad R + \delta \geq 1 - (g - 1)/n.$$

As an example, take as before

$$\mathcal{C} = (4, (X^3 + Y^3 + Z^3), \{P_0, P_1, P_2, Q_0, Q_0^2, Q_1, Q_1^2, Q_2, Q_2^2\}).$$

Let $D = P_1 + P_2 + Q_0 + Q_0^2 + Q_1 + Q_1^2 + Q_2 + Q_2^2$ and let $E = 3P_0$. The curve \mathcal{C} is elliptic; that is, $g = 1$. By Riemann's theorem $l(E) = 3 + 1 - 1 = 3$. Hence a basis for $L(E)$ is $\{1, f_1, f_2\}$. This therefore gives a generator matrix G for $C(D, E)$, where the first column is 1, $f_1(P_1)$, $f_2(P_1)$, and so on:

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & \omega^2 & \omega & \omega^2 & \omega \\ 0 & 1 & \omega & \omega^2 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Part (i) of the corollary says that, with $n = 8$ and $k = 3$, we have $6 \geq d \geq 5$. As the third row of G has weight 5, this means that $d \neq 6$. So, in this case, $C(D, E)$ is an $[8, 3, 5]$ -code. Tsfasman, Vladut and Zink [12] and independently Ihara [7–9] investigated modular curves to obtain the following result.

Theorem. *For $q = p^{2h}$ there exists a sequence of modular curves $X_0(N)$ such that $\lim_{N \rightarrow \infty} g/n = (\sqrt{q} - 1)^{-1}$, where g is the genus of $X_0(N)$ and n is the number of rational points of $X_0(N)$ over \mathbf{F}_q .*

Using these curves and part (ii) of the above corollary the former team deduced that for $q \geq 49$, with $\beta = (\sqrt{q} - 1)^{-1}$, the line $\alpha = 1 - \beta - \delta$ meets the curve $\alpha = 1 - H_q(\delta)$ in two points δ_1 and δ_2 ; thus there exists an infinite sequence of q -ary codes lying above the Gilbert-Varshamov bound.

Reviewer to author. This is all clearly explained, but the part on modular curves is still tough going. It seems to me regrettable, however, that the basic ideas of linear codes were not explained.

Reviewer to reader. Let $\mathcal{C} = (q, (F), V(F))$ and let N_i be the number of points of \mathcal{C} in $PG(2, q^i)$, that is, rational over \mathbf{F}_{q^i} . The Hasse-Weil theorem states that $\zeta(\mathcal{C}, T) = \exp(\sum N_i T^i / i) = \sum T^{\deg D} (D \in \text{Div}^*(\mathcal{C}) \text{ with } D \text{ effective})$ satisfies

$$\zeta(\mathcal{C}, T) = f(T) / \{(1 - T)(1 - qT)\}$$

where

$$f(T) = (1 - \alpha_1 T) \cdots (1 - \alpha_{2g} T)$$

and

- (i) $\alpha_i \alpha_{g+i} = q$, $1 \leq i \leq g$,
- (ii) $|\alpha_i| = \sqrt{q}$, $1 \leq i \leq 2g$.

The last part is known as the Riemann hypothesis for function fields over finite fields, there being an appropriate analogy with the classical case. This has the consequence that $N_h = 1 + q^h - (\alpha_1^h + \cdots + \alpha_{2g}^h)$. An immediate consequence is that $|N_1 - (q + 1)| \leq 2g\sqrt{q}$. The upper bound is achieved when q is square and \mathcal{C} is the Hermitian curve given by $F = X\sqrt{q} + 1 + Y\sqrt{q} + 1 + Z\sqrt{q} + 1$. It should be noted that the Frobenius automorphism $x \rightarrow x\sqrt{q}$ does not induce an automorphism in the sense of algebraic geometry, since it does not give an invertible polynomial map over any extension of \mathbf{F}_q .

As an example of the theorem, take $\mathcal{C} = (2, (X^3 + Y^3 + Z^3), \{P_0, P_1, P_2\})$. Then $\zeta(\mathcal{C}, T) = (1 - cT + 2T^2) / \{(1 - T)(1 - 2T)\}$. As $N_1 = 3 = 1 + 2 - c$, so $c = 0$. Hence $\zeta(\mathcal{C}, T) = (1 + 2T^2) / \{(1 - T)(1 - 2T)\}$. Now, $\log \zeta(\mathcal{C}, T) = \sum N_h T^h / h = \sum (-1)^{j-1} (2T^2)^j / j + \sum T^h / h + \sum (2T)^h / h$. Hence

$$N_h = \begin{cases} 1 + 2^h, & h \text{ odd,} \\ 1 + 2^h + 2 \cdot 2^{h/2}, & h \equiv 2 \pmod{4}, \\ 1 + 2^h - 2 \cdot 2^{h/2}, & h \equiv 0 \pmod{4}. \end{cases}$$

In particular $N_1 = 3$, $N_2 = 9$, $N_3 = 9$, $N_4 = 9$. We have already seen the points corresponding to N_1 , N_2 , N_3 and may note that over \mathbf{F}_{16} the points of \mathcal{C} are precisely those over \mathbf{F}_4 . Expanding $\zeta(\mathcal{C}, T)$ itself gives

$$\zeta(\mathcal{C}, T) = 1 + 3T + 9T^2 + 21T^3 + \cdots + 3(2^h - 1)T^h + \cdots.$$

We have also previously seen the 3, 9, and 21 effective divisors of degrees 1, 2, and 3.

So to understand something of the Riemann hypothesis and Goppa codes, Chapters 3 and 5 are recommended.

Reviewer to author. I found the appendix on the “Simplification of the singularities of algebraic curves” very clear. This emphasizes a point that you make earlier in the book: a reader probably needs to study a book like that of Fulton before coming to yours. As a final piece of pedantry, it is well known that to describe a result as well-known without giving either the proof or a reference is neither pleasing nor helpful to the reader.

REFERENCES

1. T. Beth, *Some aspects of coding theory between probability, algebra, combinatorics and complexity theory*, Combinatorial Theory, Lecture Notes in Math., vol. 969, Springer, Berlin and New York, 1982, pp. 12–29.
2. Y. Driencourt and J. F. Michon, *Rapport sur les codes géométriques*, Université d’Aix-Marseille II and Université de Paris VII.
3. V. D. Goppa, *Algebraico-geometric codes*, Math. USSR-Izv **21** (1983), 75–91.
4. ———, *Codes and information*, Russian Math. Surveys **39** (1984), 87–141.
5. J. W. P. Hirschfeld, *Linear codes and algebraic curves*, Geometrical Combinatorics (F. C. Holroyd and R. J. Wilson, eds.), Pitman, New York and London, 1984, pp. 35–53.
6. ———, *Codes and curves*, Finite Geometries, Buildings and Related Topics, Oxford Univ Press, London and New York, 1990, pp. 129–144.
7. Y. Ihara, *Congruence relations and Shimura curves*, I, Proc. Sympos. Pure Math., vol. 33, Amer. Math. Soc., Providence, RI, 1979, pp. 291–311.
8. ———, *Congruence relations and Shimura curves*. II, J. Fac. Sci. Univ. Tokyo Sect. I A **25** (1979), 301–361.
9. ———, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo Sect. I A Math **28** (1981), 721–724.
10. G. Lachaud, *Les codes géométriques de Goppa*, Sém. Bourbaki 37ème année, 1984–85, No. 641, Astérisque **133–134** (1986), 189–207.
11. M. A. Tsfasman and S. G. Vladut, *Algebraic-geometric codes*, Kluwer, Dordrecht, 1991.
12. M. A. Tsfasman, S. G. Vladut, and T. Zink, *Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound*, Math. Nachr. **109** (1982), 21–28.
13. G. van der Geer and J. H. van Lint, *Introduction to coding theory and algebraic geometry*, Birkhäuser, Basel 1988.
14. J. H. van Lint, *Algebraic geometric codes*, Coding Theory and Design Theory, Part I, IMA Math. Appl., vol. 20, Springer, New York, 1990, pp. 137–162.
15. J. H. van Lint and T. A. Springer, *Generalized Reed-Solomon codes from algebraic geometry*, IEEE Trans. Inform. Theory **33** (1987), 305–309.
16. S. G. Vladut and Y. I. Manin, *Linear codes and modular curves*, J. Soviet Math. **30** (1985), 2611–2643.
17. J. F. Voloch, *Codes and curves*, Eureka **43** (1983), 53–61.
18. M. Wirtz, *Verallgemeinerte Goppa-Codes*, Diplomarbeit, Universität Munster, 1986.

J. W. P. HIRSCHFELD
UNIVERSITY OF SUSSEX

E-mail address: mmfd4@central.sussex.ac.uk