65. C. C. Moore, "Group extensions of p-adic and adelic linear groups," Publ. Math. Inst. Hautes Etudes Scient., No. 35, 157-222 (1968, 1969).
66. M. P. Murthy and A. Roy, "Torsion in $K_2$ of fields and O-cylces on rational surfaces," Tata Inst. Fund. Research, Preprint (1983).
67. J. Neisendorfer, Primary Homotopy Theory, Mem. AMS, No. 232 (1980).
68. D. Quillen, "Higher algebraic K-theory. I," Lect. Notes Math., 341, 85-147 (1973).
69. D. Quillen, "Cohomology of groups," Actes Congr. Int. Mathematiciens, 1970, Vol. 2, Paris, pp. 47-51 (1971).
70. U. Rehman, "Zentrale Erweiterungen der speziallen linearen Gruppe eines Schiefkorpers," J. Reine Angew. Math., No. 301, 77-104 (1978).
71. C. Sherman, "Some theorems on the K-theory of coherent sheaves," Commun. Algebra, 7, No. 14, 1489-1508 (1979).
72. C. Sherman, "K-cohomology of regular schemes," Commun. Algebra, No. 10, 999-1029 (1979).
73. $SK_1$ von Shiefkorpern, Lect. Notes Math., 778 (1980).
74. C. Soule, "K-theorie des anneux d'entiers de corps de nombres et cohomologie etale," Invent. Math., 55, No. 3, 251-295 (1979).
75. A. A. Suslin, "Torsion in $K_2$ of fields," Leningr. Otd. Mat. Inst. Akad. Nauk SSSR, Preprint No. E 2 (1982).
76. A. A. Suslin, "Homology of $GL_n$, characteristic classes and Milnor K-theory," Preprint LOMI, Leningr. Otd. Mat. Inst. Akad. Nauk SSSR, No. E 4 (1982).
77. R. G. Swan, "Algebraic K-theory," Lect. Notes Math., 76 (1968).
78. J. Tate, "Relations between $K_2$ and Galois cohomology," Invent. Math., 36, 257-274 (1976).
79. "Theorie global des intersection et theoreme de Riemann-Roch (SGA6)," Semin. Geom. Algebr. du Bois Marie 1966-67 (Lect. Notes Math., 225), Springer-Verlag, Berlin (1971).
80. "Theorie des topos et cohomologie etale des schemas (SGA-4)," Lect. Notes Math., 269, 270, 305 (1972).
81. J. B. Wagoner, "Developing classifying spaces in algebraic K-theory," Topology, 11, No. 4, 349-370 (1972).
82. F. A. Waldhausen, "Algebraic K-theory of generalized free products. I, II," Ann. Math., 108, No. 1, 135-204 (1978).
83. S. Wang, "On the commutator group of a simple algebra," Am. J. Math., 72, 323-334 (1950).
84. C. A. Weibel, "A survey of products in algebraic K-theory," Lect. Notes Math., 854, 494-517 (1981).

# LINEAR CODES AND MODULAR CURVES

S. G. Vlĕduts and Yu. I. Manin

UDC 519.725+512.624

Results of recent investigations at the juncture of coding theory, the theory of computability, and algebraic geometry over finite fields are presented. The basic problems of the asymptotic theory of codes and Goppa's construction of codes on the basis of algebraic curves are presented, and a detailed algorithmic analysis is given of the codes arising on the modular curves of elliptic modules of V. G. Drinfel'd.

## INTRODUCTION

In the present work we present results of recent investigations at the juncture of coding theory, the theory of computability, and algebraic geometry over finite fields. These investigations were initiated by the remarkable idea of V. D. Goppa [7, 8] who suggested considering linear systems on algebraic curves as codes and discovered that among them there are very good codes which are called isolated codes in Sec. 1 below. Tsfasman [28, 16] then showed that the asymptotic parameters of Goppa's codes also improve the long unsurpassed Varshamov-Gilbert bound if there exist curves having a number of points which is sufficiently large as compared with the genus. Indeed, Ihara [24, 23] earlier discovered that modular

Translated from Itogi Nauki i Tekhniki, Seriya Sovremennye Problemy Matematiki, Noveishie Dostizheniya, Vol. 25, pp. 209-257, 1984.

0090-4104/85/3006-2611$09.50  

curves and the classical and Shimura curves are just such curves; this was discovered independently by Vleduts and Zink [28]. An estimate of the maximal number of points over the fields $F_q$ was then obtained by Drinfel'd and Vleduts [5] (Theorem 3.8); it is sharp for $q = p^{2\alpha}$. Algorithms constructing codes near the Varshamov–Gilbert bound are exhaustive; there thus arises the natural problem of generating good codes by means of algorithms which work sufficiently rapidly. It turns out that Goppa codes corresponding to modular curves can be constructed in polynomial time. For classical modular curves this was demonstrated in the work of S. G. Vleduts [4]. In this survey the modular curves of Drinfel'd [10] are obtained in a more convenient form from a computational aspect. Codes obtained from modular curves have good asymptotic parameters only for sufficiently large q. In particular, binary codes (q = 2) cannot be obtained in this manner. G. L. Katsman had the idea of using cascade codes with a fixed internal binary isolated code and external codes obtained from modular curves. This leads to the best known binary codes with polynomial complexity of construction (see parts 1.2.13, 1.3.7, and [6]).

Part of the works mentioned were carried out within the framework of seminars on Diophantine geometry and applied algebra which Yu. I. Manin held in the Mechanics and Mathematics Faculty of Moscow State University in 1981 and 1982. Chapter I of the paper was written by Yu. I. Manin using the notes of these seminars and of a course of lectures. The main problems of asymptotic coding theory and Goppa's construction are presented there. Chapter II, written by S. G. Vleduts, contains the detailed algorithmic analysis he made of modular-code constructions.

The authors convey their sincere thanks to V. G. Drinfel'd for very useful conversations regarding elliptic modules, to S. I. Gel'fand and M. A. Tsfasman for their attention to the work and valuable remarks, and to D. Yu. Grigor'ev for communicating the algorithm of decomposition of polynomials into factors used in part 2.6.5.

## CHAPTER I

## ASYMPTOTIC PROBLEMS OF THE THEORY OF CODES

### 1. Codes and Their Asymptotic Properties

1. Notation. Let S be a finite set; $|S|$ denotes the number of its elements; $S^n = S \times \ldots \times S$ (n factors). We fix a set F, $|F| = q$, called an alphabet; F will frequently be a finite field of q elements; it is then written $F_q$. The Hemming distance between $a, b \in F^n$ is the number of positions $i \in (1, \ldots, n)$ for which $a_i \neq b_i$. It is denoted by $d(a, b)$. The set $F^n$ with the Hemming distance is a finite metric space.

2. Codes. A q-ic block code of length $n = n(C)$ is a subset $C \subset F^n$. Its code distance is the number $d = d(C) = \min\{d(a, b) \mid a, b \in C.\ a \neq b\}$. Its (logarithmic) power is the number $k = k(C) = \log_q |C|$ (it is not necessarily an integer). Below the following relative characteristics are important: $R(C) = k(C)/n(C)$ and $\delta(C) = d(C)/n(C)$. A code with parameters [n, k, d] is sometimes called an [n, k, d]-code.

3. The Code Region. In the (R, δ)-plane we consider points corresponding to all possible q codes (a point is counted with a multiplicity equal to the number of codes corresponding to it up to isomorphism).* We set

$V_q$ = the family of code points $\{R(C), \delta(C)\}$,

$U_q$ = the set of limit points of the family $V_q$.

Obviously, $U_q \subset V_q \subset [0, 1]^2$. It will be proved below that $U_q$ is the set of points lying below the graph of a certain continuous function $R = \alpha_q(\delta)$. Codes corresponding to points of $V_q$ $U_q$ are called isolated.

4. Coding and Decoding. Let M be a set (the space of communications), and let $C \subset F^n$ be a code. A coding is a mapping (usually an imbedding) $E: M \to C$. Decoding is a mapping $D: F^n \to C$ with the property $D(a) = a$ if $a \in C$.

We call a decoding D standard ("relative to maximum plausability") if for any word $b \in F^n$ $D(b)$ is the code word closest to it (the latter is, of course, not necessarily unique). If

*In the present work we use a nonstandard notation for the coordinates of a point in the (R, δ)-plane. Namely, in the notation (R, δ) R denotes the ordinate of a point and δ its abscissa.

$d = d(C)$, $t = [d - 1/2]$, $a \in C$ and $d(a', a) \leqslant t$, then $\mathbf{D}(a') = a$ for a standard decoding. It is usually said that a $[n, k, d]$-code corrects $[d - 1/2]$ errors. This statement acquires meaning in the scheme below.

5. Noise-Immune Coding. Suppose the information to be transmitted over a noisy channel is produced in the form of a sequence of symbols of the alphabet F of potentially unbounded length. The standard scheme of noise-immune coding is as follows. We choose a code $C \subset F^n$ with parameters $R = k/n$, $\delta = d/n$; for simplicity we assume that k is an integer. We fix a coding mapping $E: F^k \to C$ and a decoding mapping $\mathbf{D}: F^n \to C$.

a) Let $a \subset F^{kN}$ be a communication of length kN. We decompose it into N blocks of length k and convert it into a code sequence $E_N(a)$ of length nN by coding each block by means of E:

$$E_N(a) = E(a_1 \dots E_k) E(a_{k+1} \dots a_{2k}) \dots$$

It will be transmitted along the communications channel. Its length is greater than the length of the communication by $nN/kN = 1/R$ times. Therefore, the transmission speed $R \leqslant 1$ actually measures the degree of increase in the volume of information due to coding.

b) After transmission $E_N(a)$ is converted into a distorted signal $\tilde{E}_N(a)$. We postulate simple statistical properties of the noise: it acts independently on successive symbols $a_i$ and distorts each symbol with probability p.

c) Let N be so large that with probability close to one in each block of length n in $\tilde{E}_N(a)$ there are no more than $(p + \varepsilon)n$ errors ($\varepsilon$ is small). Suppose also that $pn < (d - 1)/2$, i.e., $p < \delta/2$. Then the standard block decoding corrects all errors at the site of the receiver: $\mathbf{D}_N \circ \tilde{E}_N(a) = E_N(a)$ almost surely.

Thus, having at our disposal a code of large length n with characteristics $(R, \delta)$, we can correct errors occurring with probability $< \delta/2$ on a symbol. This explains the role of the limit code region $U_q$ (especially its boundary) and also the role of isolated codes if their length is sufficiently large to guarantee smoothing of noise.

We shall explicitly indicate the price paid for this method of protecting information:

— additional computational work in coding and decoding;

— decrease of the transmission speed;

— delay in the start of coding by the time required to process n successive symbols of information.

6. Codes with Structure; Linear Codes. For small values of $q^n$ it is possible to give E and $\mathbf{D}$ by a table, but even in the realistic case $q = 2$, $n = 100$ this is completely unthinkable. Hence, on $F^n$ there must be given a mathematical structure which would allow economic description of some subclass of mappings E, $\mathbf{D}$ and effective computation of the values of E and $\mathbf{D}$ on words. Usually the choice of such a class leads also to a restriction of the class of codes $C \subset F^n$ to which these mappings can be applied.

A code C is called linear if on F there is given the structure of a finite field $F_q$, and $C \subset \mathbf{F}_q{}^n$ is a linear subspace. In this case $k = \dim_{F_q} C$; unfortunately, the function $d(C)$ has bad linear properties.

A linear code C can be described either as the matrix of a linear mapping C or as the matrix of a linear mapping $\mathbf{F}_q{}^k \to \mathbf{F}_q{}^n$ with kernel C. The first matrix is called a generating matrix while the latter is called a control matrix. These matrices consist of kn or $n(n - k)$ letters of the alphabet $F_q$ while direct enumeration of all elements of C would require $nq^k$ letters. Therefore, giving a linear code by a matrix provides logarithmic curtailment of message length. The coding and decoding algorithms are given by analogous matrices if it is required that $E: \mathbf{F}_q{}^l \to C$ be a linear mapping and $\mathbf{D}: \mathbf{F}_q{}^n \to \mathbf{F}_q{}^l$ be a linear projection onto the image of E.

Other classes of codes and algorithms D, E are obtained if another structure, for example, a tree structure, is given on $F^n$.

7. Formulation of the Problems. The main problems of coding theory are optimization problems. It is desirable to achieve simultaneously a high transmission speed and a large fraction of correctable errors whereby the coding and decoding algorithms should admit simple machine realization and have a short working time. Of course, all these demands are contradictory. The mathematical theory of asymptotic properties of codes establishes the bounds of

the achievable. We shall mainly concern ourselves with describing the region $U_q$ and the set of isolated points of $V_q \setminus U_q$ and also analogues of these sets $U_q^{\text{lin}}$, $V_q^{\text{lin}}$ (points corresponding to linear codes) and $U_q^{p\ \text{lin}}$: by definition $(R, \delta) \in U_q^{p\ \text{lin}}$, if $(R, \delta)$ is a limit point of a sequence $(R(C_n), \delta(C_n))$ where $C_n$ are polynomial codes, i.e., codes whose matrix is computable in time polynomially bounded by the magnitude of this matrix.

In Sec. 2 the following results are proved.

8. THEOREM. There exists a continuous function $[0, 1 - 1/q]$ which is decreasing on the segment $\alpha_q(\delta)$, $\delta \in [0, 1]$, such that

$$U_q = \{(R, \delta) \mid 0 \leqslant R \leqslant \alpha_q(\delta)\}.$$

It satisfies the following inequalities:

$$\alpha_q(0) = 1,\ \alpha_q(\delta) \leqslant \max\left(1 - \frac{q}{q-1}\delta,\ 0\right) \text{ (the Plotkin upper bound);}$$

$$\alpha_q(\delta) \geqslant \max\left[1 - (\delta \log_q(q-1) - \delta \log_q \delta - (1-\delta)\log_q(1-\delta),\ 0\right] \text{ (the Varshamov–Gilbert lower bound).}$$

More precise upper bounds for $\alpha_q(\delta)$ are known (see below). The lower bound remained unimproved until the discovery of Goppa codes which are connected with modular curves; they provide the best codes for $q = p^{2a} \geqslant 49$. So far it is not known if it can be improved for the most interesting cases $q = 2, 3$.

9. THEOREM. There exist continuous functions $\alpha_q^{\text{lin}}(\delta)$ and $\alpha_q^{p\ \text{lin}}(\delta)$ which are decreasing on the segment $[0, 1 - 1/q]$, such that $U_q^{\text{lin}}$ and $U_q^{p\ \text{lin}}$, respectively, are parts of $[0, 1]^2$ lying below their graphs. The curve $\alpha_q^{\text{lin}}(\delta)$ lies no lower than the Varshamov–Gilbert curve.

It is obvious that any upper bound for the class of all codes (for example, the Plotkin bound) is simultaneously an upper bound for $\alpha_q^{\text{lin}}$ and $\alpha_q^{p\ \text{lin}}$. The known lower bounds for $\alpha_2^{p\ \text{lin}}$ are worse than the Varshamov–Gilbert bound (regarding them, see Sec. 3).

10. Geometry of the Varshamov–Gilbert Curve. We set

$$\varphi_q(\delta) = \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta)\log_q(1-\delta).$$

In the next section we shall show that this function measures the asymptotic volume of the Hemming ball. The Varshamov–Gilbert curve is given by the equation $R = 1 - \varphi_q(\delta)$. It possesses the following properties:

a) $R(0) = 1$, $R\left(\frac{q-1}{q}\right) = 0$.

b) $-\varphi'(\delta) = -\log_q(q-1) - \log_q \frac{1-\delta}{\delta}$.

As $\delta$ decreases from $q - 1/q$ to 0 this derivative increases monotonically from 0 to $\infty$; in particular, $-\varphi'(q-1)/(2q-1) = 1$. Therefore, the Varshamov–Gilbert curve is convex downward and is tangent to the coordinate axes at the end points $R = 1$, $\delta = 0$ and $R = 0$, $\delta = (q-1)/q$.

c) $\varphi''(\delta) = \frac{1}{\ln q} \cdot \frac{1}{\delta(\delta - 1)}$; $\varphi''\left(\frac{q-1}{q}\right) = \frac{q^2}{(q-1)\ln q}$.

As $R \to 0$ this gives $1 - \varphi\left(\frac{q-1}{q} - y\right) = \frac{q^2}{2(q-1)\ln q} \cdot y^2 + O(y^3)$.

d) For $q = 2$ the term linear in $\delta$ vanishes; $\varphi_2(\delta) = -[\delta \log_2 \delta + (1-\delta)\log_2(1-\delta)]$ is the entropy function. Here is a brief table of the Varshamov–Gilbert function for $q = 2$:

| $\delta$ | 0 | 0.05 | 0.1 | 0.15 | 0.2 | 0.25 | 0.3 | 0.35 | 0.4 | 0.45 | 0.5 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $1-\varphi_2(\delta)$ | 1 | 0.7136 | 0.5310 | 0.3932 | 0.2780 | 0.1887 | 0.1187 | 0.0659 | 0.0290 | 0.0072 | 0 |

## 2. Boundaries of the Code Region

1. The purpose of this section is to prove Theorems 1.8 and 1.9; Some further details regarding codes will be obtained along the way. Let $V_t^n = V_t^n(a_0) = \{a \in F^n / d(a, a_0) \leqslant t\}$ be the Hemming ball with arbitrary center $a_0 \in F^n$.

2. LEMMA. In the notation of Sec. 1 we have

$$\frac{1}{n+1} q^{n\varphi_q\left(\frac{t}{n}\right)} < |V_t^n| = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leqslant q^{n\varphi_q\left(\frac{t}{n}\right)} = |F^n|^{\varphi_q\left(\frac{t}{n}\right)}.$$

COROLLARY. As $n \to \infty$, $t/n \to \delta$ the ball of relative radius $\delta$ in $F^n$ occupies a fraction of the "logarithmic volume" of $F^n$ equal to

Proof. In the sum for $|V_t^n| = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i$ the i-th term consists of the factor $\binom{n}{i}$, corresponding to the ways of choosing precisely i positions of "errors," $i \leqslant t$, and $(q-1)^i$ corresponds to all possible "errors" in these positions.

For any $0 < z \leqslant 1$ we have

$$\sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leqslant \sum_{i=0}^{n} \binom{n}{i} (q-1)^i z^{i-t} = z^{-t} (1 + (q-1) z)^n.$$

It is easy to verify that the function on the right has at the point $z_0 = \frac{t}{n} \Big/ \left(1 - \frac{t}{n}\right)(q-1)$ a minimum equal to $q^{n\varphi_q\left(\frac{t}{n}\right)}$, which proves the upper bound (the verification accounts with the fact that $t < \frac{q-1}{q} n$ —under this condition the extremum lies to the left of 1).

On the other hand,

$$\sum_{i=0}^{t} \binom{n}{i} (q-1)^i > \binom{n}{t} (q-1)^t > \frac{1}{n+1} \tilde{z}^{-t} (1 + (q-1)\tilde{z})^n$$

for some point $\tilde{z} \in (0, 1]$. Indeed, if we choose $\tilde{z}$ in the interval $t/(n-t+1)(q-1) \leqslant \tilde{z} \leqslant (t+1)/(n-t)(q-1)$, then the term $\binom{n}{t}(q-1)^t \tilde{z}^t$ is maximal among all terms of the expansion $(1 + (q-1)\tilde{z})^n = \sum_{i=0}^{n} V_i z^i$ because of the inequalities $V_{i-1}/V_i \leqslant V_{i-1}/V_t \leqslant \tilde{z}$ for $i < t$ and $\tilde{z} \leqslant V_t/V_{t+1} \leqslant V_i/V_{i+1}$ for $i \geqslant t$. This proves the lower bound for the volume.

3. Proposition. a) The Varshamov–Gilbert curve $R = 1 - \varphi_q(\delta)$, $0 \leqslant \delta \leqslant \frac{q-1}{q}$, lies entirely in $U_q$. b) Above the Hemming curve $R = 1 - \varphi_q\left(\frac{\delta}{2}\right)$ there is no point of $U_q$.

Proof. a) We choose a point $(R, \delta)$ on the Varshamov–Gilbert curve (not an end point). In order to construct a code $C \subset F^n$ with parameters arbitrarily close to $(R, \delta)$ we choose large numbers $[n, k, d]$ with $R \approx k/n$, $\delta = d/n$ and consider the following (sorting) algorithm for successive choice of code words contained in C. The first word is chosen arbitrarily; if $a_1, \ldots, a_m \in C$ have already been chosen and if $F^n \neq \bigcup_{i=1}^{m} V_d^n(a_i)$, then $a_{m+1}$ is an arbitrary element of the complement $F^n \setminus \bigcup_{i=1}^{n} V_d^n(a_i)$. Since $|V_d^n(a_i)| \leqslant q^{n\varphi_q\left(\frac{d}{n}\right)}$, the algorithm does not terminate until the completion of $q^k$ steps under the condition that $q^k \cdot q^{n\varphi_q\left(\frac{d}{n}\right)} \leqslant q^n$, i.e., $\left(\frac{d}{n}, \frac{k}{n}\right)$ lies below the Varshamov–Gilbert curve.

Let C be an $[n, k, d]$-code, $t = \left[\frac{d-1}{2}\right]$. Then the balls $V_t^n(a)$, $a \in C$, are pairwise disjoint so that the sum of their volumes is not greater than $q^n$; hence, by Lemma 2

$$\frac{1}{n+1} q^{k + n\varphi_q\left(\frac{1}{n}\left[\frac{d-1}{2}\right]\right)} \leqslant q^k |V_t^n| \leqslant q^n.$$

Therefore, if $\left(\frac{d}{n}, \frac{k}{n}\right) \to (\delta, R)$; $n, k \to \infty$, then $R \leqslant 1 - \varphi_q\left(\frac{\delta}{2}\right)$.

Remark. Near R = 1, i.e., $\delta = 0$, the Hemming upper bound is better than the Plotkin bound; they intersect at the point $\varphi_q(\delta_0/2) = (q/(q-1))\delta_0$. Near R = 1 the Hemming curve deviates from the vertical axis approximately twice as much as the Varshamov–Gilbert curve. Therefore, the true boundary of $U_q$, the curve $\alpha_q$, being contained between them, has a vertical tangent at the left end point. The same goes for $\alpha_q^{\text{lin}} \leqslant \alpha_q$ by the following result.

4. Proposition. a) The Varshamov–Gilbert curve lies entirely in $U_q^{\text{lin}}$. b) For any linear [n, k, d]-code $k + d \leqslant n + 1$ (in particular, $U_q^{\text{lin}}$ lies below the diagonal $R + \delta = 1$).

Proof. Suppose the linear code C is the kernel of a mapping $\mathbf{F}_q^n \to \mathbf{F}_q^{n-k}$ given by a matrix H. Each code word is a linear relation between the columns of H; hence, $d(C) \geqslant d$ if any $d - 1$ columns of H are independent. Thus, $d-1 \leqslant \operatorname{rk} H \leqslant n-k$, whence b) follows.

We shall construct codes close to the Varshamov–Gilbert curve by successively choosing the columns of H. We denote them by $a_1, a_2, \ldots$. A successive vector $a_{m+1} \in F_q^{n-k}$ is to be chosen so that it cannot be linearly expressed in terms of any $d - 2$ preceding vectors. Those vectors which do not satisfy this condition are linear combinations with all nonzero coefficients of some i of the vectors chosen earlier. There are no more than $\sum_{l=2}^{d-2} \binom{m}{l} (q-1)^l$ of them. If

$$q^{n-k} - 1 \geqslant \sum_{i=1}^{d-2} \binom{n}{i} (q-1)^i \geqslant \frac{1}{n+1} \cdot q^{n\varphi_q\left(\frac{d-2}{n}\right)},$$

then it is possible to choose the succeeding vector. This proves assertion a).

5. Examples. a) Reed–Solomon Codes. These are isolated codes over $F_q$ with parameters [n, k, d] where n is any divisor of $q - 1$, $1 \leqslant k \leqslant n$ is any integer, and $k + d = n + 1$. They are constructed as follows: since the group $F_q$ is cyclic of order $q - 1$, there exist $\varphi(n)$ elements $x \in F_q^*$ of order equal to n. We set $H = (h_{ij})$, $h_{ij} = x^{i(j-1)}$, $i = 1, \ldots, n - k$, $j = 1, \ldots, n$. Any $n - k$ columns of this matrix are linearly independent, since the corresponding minor can be computed by means of Vandermode's formula. The code with control matrix H has the required parameters.

b) Goppa Codes of Genus Zero. These are isolated codes over $F_q$ with any parameters of the form [n, k, d] where $n \leqslant q$ and $k + d = n + 1$.

Namely, we set $C = \{f \in \mathbf{F}_q[t] / \deg t \leqslant k-1\}$, where t is an independent variable; we choose n distinct elements $x_1, \ldots, x_n \in F_q$ where $k \leqslant n \leqslant q$. We define the mapping $C \to \mathbf{F}_q^n$ by setting $f \mapsto (f(x_1), \ldots, f(x_n))$. It is an imbedding, since a nonzero polynomial of degree $\leqslant k - 1$ cannot have $n \geqslant k$ zeros. Therefore, the image of C in $\mathbf{F}_q^n$ is an [n, k, d]-code.

It will soon be clear that these codes are isolated: the Plotkin upper bound for $U_q$ lies below the diagonal $R + \delta = 1$.

6. LEMMA. If an [n, k, d]-code exists, then $d \leqslant n \frac{q^k}{q^k-1} \cdot \frac{q-1}{q}$.

COROLLARY. In the region $R > 0$, $\delta > (q - 1)/q$ there are no limit points of $U_q$ (and $U_{q\,\text{lin}}$). (Indeed, for any sequence $[n_i, k_i, d_i]$ with $n_i \to \infty$ either $k_i$ are bounded, and thus $k_i/n_i \to 0$, or $k_i$ are unbounded and then $d_i/n_i \leqslant ((q - 1)/q)(1 + \varepsilon_i)$, $\varepsilon_i \to 0$ by the lemma.)

Proof. Let C be some [n, k, d]-code. We set $X_{a,l} = |\{x \in C \mid x_l = a\}|$. It is obvious that $X_{\alpha,i}$ are nonnegative integers and $\sum_{a \in F} X_{a,l} = q^k$. The code distance d(C) is no greater than the average pairwise distance: $d(C) \leqslant \frac{1}{q^k(q^k-1)} \sum_{x,y \in C} d(x, y)$, and equality is achieved only for so-called equidistant codes with the property $\forall x \neq y$, $d(x, y) = d(C)$. Further,

$$\sum_{x,y \in C} d(x, y) = \sum_{l=1}^{n} \sum_{x,y \in C} (1 - \delta_{x_l y_l}) = \sum_{l=1}^{n} \sum_{a,b \in F} (1 - \delta_{ab}) X_{a,l} X_{b,l} \leqslant n \cdot \max_X Q,$$

where $\delta_{\alpha b}$ is the Kronecker symbol, Q is a quadratic form with matrix $1 - \delta_{\alpha,b}$, $X = (X_a)_{a \in F}$

runs through the simplex $\sum_{a\in F} X_a = q^k$, $X_a \geqslant 0$. This maximum is equal to $q^{2k}\frac{q-1}{q}$, as can be seen by induction on $q = |F|$: the maximum is achieved at an interior point where all $X_a$ are identical: $X_a = \frac{q^k}{q}$. This proves the lemma.

7. LEMMA. a) If there exists an [n, k, d]-code, then for any $l \leqslant k$ there exists a code with parameters [n − l, k − l, d]. b) The same holds for linear codes.

Proof. a) Let C be an [n, k, d]-code. For $\xi \in F^l$ we set $C_l(\xi) = \{x \in F^{n-l} \mid (x, \xi) \in C\}$. Then $\sum_{\xi \in F^l} |C_l(\xi)| = q^k$; and hence $|C_l(\xi_0)| \geqslant q^{k-l}$ for some $\xi_0$. The code $C_l(\xi_0)$ obviously has parameters $[n-l, \geqslant k-d, \geqslant d]$. They can be reduced to [n − l, k − l, d] by first discarding superfluous points and then shifting one of the points so that its distance to its closest neighbor in the code is d.

b) Suppose now that $F = F_q$ and C is a linear [n, k, d]-code given by a generating matrix G of size n × k. It has a nonzero minor of rank k; by renumbering the basis of $F_q^n$, it can be arranged that it occurs at the very bottom of G. Then the projection $F^n \to F^k$ induces a surjective mapping of C onto $F^l$, $l \leqslant k$. In the notation of the previous paragraph $C_l(\xi)$ are cosets of $C_l(0)$ in $F_q^{n-l}$; therefore, $|C_l(\xi)| = q^{k-l}$ for all ξ, and the shortest vector of C in the Hemming sense lies in $C_l(0) \times (0)$. Hence, the parameters of $C_l(0)$ are [n − l, k − l, d].

8. Proposition. The sets $U = U_q$, $U_q^{\text{lin}}$ and $U_q^{p\,\text{lin}}$ possess the following property: if $(R_0, \delta_0) \in U$, $R_0 > 0$, $\delta_0 > 0$, then the entire segment of the line joining $(R_0, \delta_0)$ with (1, 0), which lies to the right of and below $(R_0, \delta_0)$ in the square $[0, 1]^2$, belongs to U.

Proof. According to Lemma 7, if $\left(\frac{k}{n}, \frac{d}{n}\right) \in U_q$ or $U_q^{\text{lin}}$, then for all $l \leqslant k$ we have $\left(\frac{k-l}{n-l}; \frac{d}{n-l}\right) \in U_q$ (respectively, $U_q^{\text{lin}}$). All these points lie on the line $R = 1 - \delta(n-k)/d$ joining $\left(\frac{k}{n}, \frac{d}{n}\right)$ with (1, 0) to the right and below. If $[n_i, k_i, d_i[$ is a sequence of codes with $n_i \to \infty$, $\frac{k_i}{n_i} \to R_0$, $\frac{d_i}{n_i} \to \delta_0$, then the derived points lie ever more dense on the corresponding segments. Finally, if the generating matrices of the $[n_i, k_i, d_i]$-codes are constructed in a time bounded by a polynomial in the size of the matrix, then the additional work to seek the maximal nonzero minor (for example, by the Gauss method) and discard parts of the rows in it can only increase this polynomial somewhat (q is fixed).

9. Corollary (the Upper Hemming–Plotkin Bound). The set $U_q$ lies entirely below the curve

$$R = \begin{cases} \min\left(1 - \frac{q}{q-1}\delta,\ 1 - \varphi_q\left(\frac{\delta}{2}\right)\right), & \delta \leqslant \frac{q-1}{q} \\ 0, & \delta \geqslant \frac{q-1}{q}. \end{cases}$$

Proof. If there existed a limit point above the curve $R = 1 - (q/(q-1))\delta$ with $\delta < (q-1)/(q)$, then the right lower end point of the segment constructed in Proposition 8 would contain points $(R_0, \delta_0)$ with the property $\delta_0 > (q-1)/(q)$, $R_0$ which is impossible by the corollary of Lemma 6.

It remains for us to prove the existence of the functions $\alpha_q$, $\alpha_q^{\text{lin}}$, $\alpha_q^{p\,\text{lin}}$. To this end we first establish an analogue of Lemma 7 which provides derived codes to the left of and above the original code.

10. LEMMA. a) If there exists an [n, k, d]-code, then for any $l \leqslant \min(d-1, n-k)$ there exists a code with parameters [n − l, k, d − l]. The same holds for linear codes.

Proof. Let $C \subset F^n$ be some [n, k, d]-code. We consider the projection $p: F^n \to F^{n-l}$ onto the last n − l coordinates; let C' = p(C). If p(x) = p(y), then $d(x, y) \leqslant l$; therefore, for $l \leqslant d-1$ and for x, y ∈ C necessarily x = y. Hence, $C' \subset F^{n-l}$ is a code with parameters [n − l, $k \geqslant d-l$]; it is linear if C is linear. In the general case it is possible to take d(C') into d − l by shifting only one point of the code. In the linear case we must first renumber the basis of $F^n$ so that the nondegenerate minor is found at the bottom.

11. Proposition. The sets $U = U_q$, $U_q^{\text{lin}}$ and $U_q^{\text{plin}}$ possess the following property: if $(R_0, \delta_0) \in U$, $R_0 > 0$, $\delta_0 > 0$, then the entire segment of the line joining $(R_0, \delta_0)$ with (0, 1), which lies to the left of and above $(R_0, \delta_0)$ in the square $[0, 1]^2$, belongs to U.

This result is derived from Lemma 10 in the same way as Proposition 8 was derived from Lemma 7: the points $\left(\frac{k}{n-l}, \frac{d-l}{n-l}\right)$ lie precisely on the line joining $\left(\frac{k}{n}, \frac{d}{n}\right)$ with (0, 1).

12. Completion of the Proof of Theorems 1.8 and 1.9. It remains only for us to establish the existence of functions $\alpha_q$, $\alpha_q^{\text{lin}}$, $\alpha_q^{\text{plin}}$ whose graphs bound U from above. We shall write * in place of the indices $\varnothing$, lin, or plin. We set $\alpha_q^*(x) = \sup\{R \mid (R, x) \in U_q^*\}$. For any point $(R_0, \delta_0)$ lying no higher than the Plotkin line, we denote by I and II the lines joining it with (0, 1) and (1, 0), respectively. Let $I_+$, $II_+$ be the half lines lying to the right of $(R_0, \delta_0)$, and let $I_-$, $II_-$ be the half lines lying to the left. The angular sectors formed by $(I_+, II_+)$ and $(I_-, II_-)$ we call the right and left cone of the point $(R_0, \delta_0)$, respectively.

From the facts proved above it follows that for $0 < x < y < (q-1)/q$ the point $(\alpha_q^*(x), x)$ lies in the left cone of the point $(\alpha_q^*(y), y)$, while $(\alpha_q(y), y)$ lies in the right cone of the point $(\alpha_q^*(x), x)$. We shall verify, for example, the first assertion. The point $(\alpha_q^*(x), x)$ cannot lie above the line $I^y$ for the point $(\alpha_q^*(y), y)$ — otherwise its half line $II_+^x$ passes above $(\alpha_q^*(y), y)$ which contradicts the definition of $\alpha_q^*(y)$ by Proposition 8. Similarly, $(\alpha_q^*(x), x)$ cannot lie below the line $II^y$ for the point $(\alpha_q^*(y), y)$ by Proposition 11 and the definition of $\alpha_q^*$.

From this it follows that the function $\alpha_q^*$ is continuous; unfortunately, it is not known whether it is differentiable. The entire region below the graph of $\alpha_q^*$ (with boundary) belongs to $U_q$, since it is swept out, say, by the segments $I_+$ or $II_-$ for points of the graph. Finally, it is clear that above $\alpha_q^*$ there lie only isolated code points.

13. Cascading and Code Boundaries. We consider a code $C \subset F^n$ and code the elements of F by words in a new alphabet G, i.e., we assume that $F \subset G^m$. The induced imbedding $C \subset G^{mn}$ is the code obtained by cascading the two original codes. Let $q_F = |F|$, $q_G = |G|$. The code $C \subset G^{mn}$ is called a $q_G$-ic code.

14. Proposition. Let $(R_1, \delta_1)$ be a code point of $C \subset F^n$, and let $(R_2, \delta_2)$ be a code point of $F \subset G^m$. Then $(R_1R_2, \delta_1\delta_2)$ is a code point of $C \subset G^{mn}$.

Proof. Let [n, k, d] be the parameters of $C \subset F^n$; let $[m, \log_{q_G} q_F, d']$ be the parameters of $F \subset G^m$; then the parameters of $C \subset G^{mn}$ are $[mn, k \log_{q_G} q_F, dd']$ which proves the result.

15. COROLLARY. Let q, q' be two numbers, and let $(R_1, \delta_1) \in V_q$; then the curve $(R_1\alpha_{q'}(t), \delta_1(t))$ given parametrically (t is the parameter, $0 \leqslant t \leqslant (q'-1)/q'$) lies entirely in $U_q^*$.

This construction leads to lower bounds which are the best known if we apply it to the case * = plin, q = 2, $(R_1, \delta_1)$ are isolated binary codes, and in place of $\alpha_q^{\text{plin}}(t)$ we substitute the lower bound corresponding to Goppa's modular codes which can be constructed in polynomial time by the results of Chap. II. We shall present further details below.

## 3. Algebrogeometric Codes

1. Construction. Let W be an algebraic variety over a field $F_q$, let $\mathscr{L}$ be an invertible sheaf on it, and let $W(F_q)$ be the set of points of W which are rational over $F_q$. The geometric stalks $\mathscr{L}(x)$ of the sheaf $\mathscr{L}$ over points $x \in W(F_q)$ are one-dimensional; we choose a basis in each of them. We consider the mapping

$$v: \Gamma(W, \mathscr{L}) \to \bigoplus_{x \in W(F_q)} \mathscr{L}(x) = \mathbf{F}_q^{|W(F_q)|}.$$

where $v(s) = (\ldots, s(x), \ldots)$. Its image is a linear subspace of $\mathbf{F}_q^{|W(F_q)|}$; such subspaces we shall call algebrogeometric codes. The parameters of algebrogeometric codes are precisely those characteristics of the pair (W, $\mathscr{L}$) which have been actively studied. Namely, the

length of the code is $n = |W(F_q)|$; the dimension is bounded above by the number $\dim \Gamma(W, \mathscr{L})$, and coincides with it in computable examples; finally, $n - d$ is the maximal number of $F_q$-points on the variety of zeros of any section of $\mathscr{L}$, i.e., a characteristic of the same nature as n.

2. Examples. a) $W = P^r$ (r-dimensional projective space), $\mathscr{L} = \mathcal{O}(1)$. Here $v: \Gamma(W, \mathscr{L}) \xrightarrow{\sim} C$, since a nonzero linear form cannot vanish at all $F_q$-points. The parameters of the code are equal to $\left(\frac{q^{r+1}-1}{q-1}, r+1, q^r\right)$. Since the zeros of all sections of $\mathscr{L}$ are $P^{r-1}$, these codes are quidistant, and the Plotkin upper bound is achieved for them (Lemma 2.6).

b) $W = P^r$; $\mathscr{L} = \mathcal{O}(m)$. For $m \leqslant q$ the mapping v, as before, is an isomorphism: for $r = 1$ this can be verified in the obvious way, and we then proceed by induction on r. The number of $F_q$-points on a hypersurface of degree $m \leqslant q$ does not exceed $m(q^r - 1)/(q - 1)$: indeed, we pass a pencil of projective lines through a point lying off the hypersurface. There are $|P^{r-1}(F_q)| = \frac{q^r-1}{q-1}$, such lines, and each line contains no more than m points of the hypersurface by Bezout's theorem. The code has parameters $\left[\frac{q^{r+1}-1}{q-1}, \binom{r+m}{m}, \geqslant \frac{q^{r+1}-1}{q-1} - m\frac{q^r-1}{q-1}\right]$. Many good isolated codes are thus obtained. For example, for $q = 2$, $r = 3$, $m = 2$ we find a code with parameters [15, 10, 4], while for $q = 2$, $r = 4$, $m = 2$ we find a code with parameters [31, 15, 8]. Examples a) and b) are Reed–Mahler codes of orders 1 and m, respectively.

3. Goppa Codes. These are algebrogeometric codes for which W is a smooth irreducible algebraic curve. We denote its genus by $g = g(W)$ and the number of points on it by $n = n(W) = |W(F_q)|$. We set $\gamma_q = \liminf \frac{g(W)}{n(W)}$ over all W. Since by Weil's theorem $n \leqslant q + 1 + 2g\sqrt{g}$, we have $\gamma_q \geqslant (1)/(2\sqrt{q})$. It will be proved below that the exact bound is $\gamma_q = (\sqrt{q} - 1)^{-1}$ for $q = p^{2a}$.

4. THEOREM. a) The segment of the line $R + \delta = 1 - \gamma_q$, $0 \leqslant R$, $\delta \leqslant 1$ lies entirely in $U_q^{p\,lin}$. b) For $q = p^{2a}$ it also lies entirely in $U_q^{p\,lin}$.

Proof. The second assertion of the theorem will be proved in Chap. 2 by direct verification of the fact that concrete curves with an asymptotically maximal number of points (more precisely, the codes connected with them) can be constructed in polynomial time.

To prove the first assertion we choose a curve W with g/n close to $\gamma_q$ and any integer $a$ satisfying the conditions $g - 1 \leqslant a \leqslant n$. On W we construct an invertible sheaf $\mathscr{L}$ of degree $a$, for example, $\mathcal{O}(AP)$, where $P \in W(F_q)$. No section of $\mathscr{L}$ can vanish at all points of $W(F_q)$; therefore, $v: \Gamma(W, \mathscr{L}) \xrightarrow{\sim} C$ and by the Riemann–Roch theorem $k = \dim \Gamma(W, \mathscr{L}) \geqslant a - g + 1$. On the other hand, $n - d \leqslant a$. Finally, the parameters of the code are $[n, \geqslant a - g + 1, \geqslant n - a]$, while the coordinates of a code point are $\left[\geqslant \frac{a}{n} - \frac{q-1}{n}, \geqslant 1 - \frac{a}{n}\right]$. In other words, we consider a segment $r + \delta = 1 - \gamma_q - \varepsilon$ where $\varepsilon > 0$ is arbitrarily small; then in the region $U_q^{lin}$ there are infinitely many points lying to the right of and above any point of this segment. Arguing as in the proof of Lemma 2.7, we find that this entire segment lies in $U_q^{lin}$.

5. Classical Modular Curves and Improvement of the Varshamov–Gilbert Boundary. For any prime number p and $q = p^2$ there exist sequences of curves with the property $g/n \to (p - 1)^{-1} = (\sqrt{q} - 1)^{-1}$. These are the classical modular curves. We shall present an analytic description of them. Let $N \not\equiv 0 \bmod p$ be a prime number (we impose this condition only to simplify subsequent formulations; if it is dropped the asymptotics of g/n remains the same).

a) We set

$$J(z) = (12 \cdot 60)^3 \left[\sum_{m,n \in \mathbb{Z}^2 \setminus \{0,0\}} (mz + n)^{-4}\right]^3 \Big/ \left[(2\pi)^{12} e^{2\pi i z} \prod_{n=1}^{\infty} (1 - e^{2\pi i n z})^{24}\right].$$

This is a classical modular invariant, a mermorphic function defined in the upper half plane.

b) The functions $J = J(z)$, $J_N = J(Nz)$ are related by an integral polynomial relation $\Phi_N(J, J_N) = 0$. We choose a minimal relation.

c) A smooth projective curve with a special affine model given by the equation $\Phi_N \bmod p = 0$ has the following parameters:

genus $X_0(N) - \left[\frac{N}{12}\right]$,

$\left| |X_0(N)(F_{p^2})| - \frac{N(p-1)}{12} \right| \leqslant c_p$, where $c_p$ does not depend on N.

We shall not prove these assertions here. We note only that $F_{p^2}$ – rational points on $X_0(N)$ – correspond to supersingular elliptic curves over $F_{p^2}$, i.e., to elliptic curves not having non-trivial points of order p. For Drinfel'd's modular curves detailed calculations giving curves with $\frac{n}{g} \sim \frac{1}{\sqrt{q}-1}$ are carried out in Chapter 2.

6. Proposition. For $q \geqslant 49$ the segment $R + \delta = 1 - \frac{1}{\sqrt{q}-1}$ intersects the Varshamov–Gilbert curve at two points: the part of it between these points lies above the curve.

Proof. In part 1.10 it was verified that the line $R + \delta = 1 - (\log_q(2q-1) - 1)$ is tangent to the Varshamov–Gilbert curve, since at the point of tangency $\delta_0 = (q-1)/(2q-1)$. The inequality $(\sqrt{q}-1)^{-1} < \log_q(2q-1) - 1$ for squares q is satisfied starting at q = 49.

7. Lower Boundary of $U_2^{\text{plin}}$. By applying the cascade construction of 2.13 with internal binary isolated codes C and external codes obtained from modular curves, we arrive at binary codes having polynomial complexity of construction and parameters lying above the parameters of all known binary codes with polynomial complexity of construction.

Until recently, the best estimate for the function $\alpha_2^{\text{plin}}(\delta)$, due to É. A. Blokh and V. V. Zyablov, was the following [3]:

$$\alpha_2^{\text{plin}}(\delta) \geqslant \tilde{\psi}_2(\delta),$$

where

$$\tilde{\psi}_2(\delta) = 1 - \varphi_2(\delta) - \delta \int_0^{1-\varphi_2(\delta)} dx/\chi_2(1-\delta),$$

$\varphi_2(\delta)$ is the entropy function, and $\chi_2(R)$ is its inverse. Using as internal codes a binary code with parameters [20, 8, 8], excess-free codes with parameters $[2l, 2l, 1]$, $l \geqslant 5$, codes with a single verification for parity and parameters $[2l+1, 2l, 2]$, $l = 3, 4$, and binary Reed–Mahler codes of first order with parameters $[2^{2m+1}, 2(m+1), 2^{2m}]$, $m \geqslant 2$, we obtain by 2.15 a new estimate for $\alpha_2^{\text{plin}}(\delta)$; we denote it by $\psi_2(\delta)$.

It was shown in [6] that $\psi_2(\delta) > \tilde{\psi}_2(\delta)$ everywhere in the interval (0, 1/2).

It is useful to compare the following table of the functions $\psi_2(\delta)$, $\tilde{\psi}_2(\delta)$ (the table for $\psi_2(\delta)$ was taken from [6] and that for $\tilde{\psi}_2(\delta)$ was taken from [3]) with the table of part 1.10:

| $\delta$ | 0.05 | 0.1 | 0.15 | 0.2 | 0.25 | 0.3 | 0.35 | 0.4 | 0.45 |
|---|---|---|---|---|---|---|---|---|---|
| $\psi_2(\delta)$ | 0.6298 | 0.4347 | 0.2847 | 0.1733 | 0.1233 | 0.0733 | 0.0295 | 0.0107 | 0.0021 |
| $\tilde{\psi}_2(\delta)$ | 0.4456 | 0.2524 | 0.1450 | 0.0807 | 0.0422 | 0.0198 | 0.0077 | 0.0021 | 0.0002 |

We now proceed to the estimate of $\gamma_q$. It is more convenient to work with the inverse quantity

$$A_q = \limsup_W \frac{n(W)}{g(W)}.$$

8. THEOREM. $A_q \leqslant \sqrt{q} - 1$; for $q = p^{2a}$ equality holds.

Proof. We restrict ourselves to establishing the inequality; for the fact that it is achieved see Chap. 2. By Weil's theorem we have

$$N_r = |W(\mathbf{F}_{q^r})| = q^r + 1 - \sum_{i=1}^{2g} \omega_i^r,$$

where $\omega_i$ are complex numbers entering the sum in pairs $(\omega_i, \omega_i^{-1}q)$ with the property $|\omega_i| = q^{1/2}$. We set $\omega_i = \alpha_i\sqrt{q}$. We have

$$\frac{N_r}{q^{r/2}} = q^{r/2} + q^{-r/2} - \sum_{i=1}^{g} (\alpha_i^r + \alpha_i^{-r}) \geqslant \frac{N_1}{q^{r/2}},$$

whence

$$\sum_{i=1}^{g} (\alpha_i^r + \alpha_i^{-r}) \leqslant -(N_1 q^{-r/2} - q^{r/2} - q^{-r/2}). \qquad (1)_r$$

On the other hand, we have the identity for any $\alpha_i$, m:

$$0 \leqslant \left| \sum_{r=0}^{m} \alpha_i^r \right|^2 = \sum_{r,s=0}^{m} \alpha_i^{r-s} = m + 1 + \sum_{r=1}^{m} (m+1-r)(\alpha_i^r + \alpha_i^{-r}). \qquad (2)$$

Multiplying $(1)_r$ by (m + 1 − r), summing on r, and applying (2), we obtain

$$0 \leqslant 2g(m+1) + \sum_{r=1}^{m} (m+1-r) \sum_{i=1}^{2g} (\alpha_i^j + \alpha_i^{-j}) \leqslant 2g(m+1) + 2\sum_{r=1}^{m} (m+1-r)[-N_1 q^{-r/2} + q^{r/2} + q^{-r/2}]. \qquad (3)$$

Dividing (3) by 2g(m + 1) and carrying the terms with $N_1$ to the left side, we find

$$\frac{N_1}{g} \sum_{r=1}^{m} \left[\frac{(m+1)-r}{m+1}\right] q^{-r/2} \leqslant 1 + \frac{1}{g} \sum_{r=1}^{m} \frac{m+1-r}{m+1} (q^{-r/2} + q^{r/2}).$$

If $g \to \infty$ and $m \to \infty$ slower than $[\log_q g]$, we obtain $\frac{1}{\sqrt{q}-1} \leqslant 1 + \varepsilon$, $\varepsilon \to 0$, which completes the proof.

9. How Many Points Can Lie on a Curve Over a Finite Field? This question was posed in the works of Ihara [22] and Manin [26]. Theorem 8 and calculations for modular curves provide an answer to it (in the asymptotic formulation) for $q = p^{2\alpha}$. The case where q is not a complete square has not been completely investigated. The following results were obtained by Serre and are cited here with his kind permission (letters to Yu. I. Manin of June 10, 1982 and November 6, 1982 [27]).

10. THEOREM (Serre). $A_q > 0$ for all q.

The proof is based on the construction of an infinite "tower of class fields" by the method of Golod–Shafarevich. In the functional case it consists of unramified coverings of the original curve in which the $F_q$-points completely decompose.

For $A_2$ Serre obtains the estimate $A_2 \geqslant \frac{8}{39} = 0.205\ldots$; the estimate of Theorem 8 is here $A_2 \leqslant \sqrt{2} - 1 = 0.414 \ldots$. Serre also established the maximal possible number of points on curves over $F_2$ for genera $\leqslant 7$;

| g | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| n | 5 | 6 | 7 | 8 | 9 | 10 | 10 |

## CHAPTER II

## A POLYNOMIAL ALGORITHM FOR CONSTRUCTING "MODULAR" CODES

### 1. Main Theorem

As shown in Sec. 3 of Chap. I, algebrogeometric codes constructed on the basis of curves with a "large" number of points possess very good asymptotic parameters. In the present chapter we shall show that such codes can be constructed with polynomial complexity. More precisely, suppose that for the basic curve we choose a curve $X_0(I)$ classifying elliptic $F_q[T]$-modules of rank 2 with an isogeny of degree $q^m$ (see below, Sec. 2) where m is an odd number relatively prime to q − 1. Then for $N_m$ − the number of $F_{q^2}$-rational points of the

curve $X_0(I)$ – there is the relation

$$\lim_{m\to\infty}\frac{N_m}{g_m}=q-1, \tag{1}$$

where $g_m = g(X_0(I))$ = genus $X_0(I)$. Let $C = C_{m,b}$ be an algebrogeometric $q^2$-ic code constructed on the basis of $X_0(I)$ and the sheaf $\mathscr{L}=\mathcal{O}(F)$, where $F = BQ_1 \in \mathrm{Div}(X_0(I))$ and $Q_1$ is some "cuspidal" $\mathbf{F}_q$-point of $X_0(I)$:

$$C_{m,b}=\mathrm{Im}\,(\varphi_{m,b}):$$
$$\varphi_{m,b}:\mathcal{O}(bQ_1)\to\bigoplus_{P_i\in M_m}(\mathbf{F}_{q^2})_{P_i};$$
$$\varphi_{m,b}: f\mapsto(f(P_1),\ldots,f(P_m));$$

as $M_m$ we take the set of "supersingular" points $M_m\subset X_0(I)(\mathbf{F}_{q^2})$, for which $n = n_m = |M_m| = (q_m + 1)/(q + 1)$,

$$\lim_{m\to\infty}\frac{|M_m|}{g_m}=q-1. \tag{2}$$

Then, as shown in Sec. 3 of the first chapter, the code C possesses the following parameters: $k\geqslant b-g_m+1$, $d\geqslant n_m-b$.

THEOREM. There exists an algorithm with time complexity $\mathcal{O}(n^{32}\log^2 n)$ and spatial complexity $\mathcal{O}(n^{20}\log^2 n)$, which constructs a generating matrix of the code C.

The theorem is proved in Secs. 2-6. The outline of the proof is as follows. In Sec. 2 we formulate some needed facts concerning manifolds of moduli of the elliptic modules of V. G. Drinfel'd; in particular, a precise definition of the curve $X_0(I)$ is presented, and equality (2) is proved, from which (1) follows on consideration of Theorem 8 of the first chapter. In Sec. 3 we prove a theorem providing a realization of a code C in terms of special values of some linear functionals on a space of polynomials of bounded degree. In Sec. 4 we collect formulas giving the objects used in the construction of the code C. In the fifth section we describe the computational process realizing the algorithm of constructing the code C with the complexity indicated in the theorem; it is based on standard procedures described in Sec. 6. In the last section we describe the model of the computational process we used and the standard procedures used in the proof of the main theorem. The material is presented so that Secs. 4-6 are almost independent of the contents of Secs. 2-3. Those places in Secs. 4-6 where understanding depends on Secs. 2-3 are contained in asterisks: *...*.

We use the following notation: A denotes the ring of polynomials $\mathbf{F}_q[T]$ where $q = p^s$ is a natural power of a prime number p, $GL(2, R)$ is the group of invertible $2\times 2$ matrices with coefficients in some ring R, $R^X$ is the group of units of the ring R; deg p, where $p\in k[x, y]$, k a field, denotes the degree of p in the joint variables; $\deg_x p$ denotes the degree of p in the variable x, and $\deg_y p$ denotes the degree in the variable y; $\mathrm{Mat}(m\times n, R)$ is the set of matrices of dimension $m\times n$ with coefficients in the ring R.

## 2. Manifolds of Moduli of Elliptic Modules

1. In this section we present in a necessarily brief manner facts concerning the elliptic modules of V. G. Drinfel'd, their modular manifolds, and the rational points on them which we require for the construction of codes on the corresponding modular curves. We give almost no proofs. The major part of the results of this section are proved in [10, 20, 21]; the remaining results are derived by means of arguments completely analogous to the classical case of modular curves for the group $SL(2, \mathbf{Z})$.

We consider the only case we require of elliptic A-modules of rank 2 where $A = \mathbf{F}_q[T]$.

2. Elliptic Modules over a Field. Let $k = \mathbf{F}_q(T)$ be the field of fractions of a ring A; let $k_\infty = \mathbf{F}_q((T^{-1}))$ be the completion of k relative to a norm defined by the point $\infty\in\mathbf{P}^1$ such that $A = \mathbf{F}_q[\mathbf{P}^1\setminus\infty]$. The normalized absolute value of an element $a\in k$ corresponding to the point $\infty$ is denoted by $|a|$; if $a = (b/c)$, $b, c\in A$, then $|a| = q^{\deg b-\deg c}$.

Let K be a field equipped with the structure of an A-algebra, let $i:A\to K$, and let $K\{\tau\} = \mathrm{End}(G_a\otimes K)$ be the ring of endomorphisms of an additive group scheme over K where $\tau$ is the endomorphism of $G_a\otimes K$, given by the formula $\tau: x\mapsto x^p$ ($\tau$ is the Frobenius endomorphism over the field $\mathbf{F}_p$). The ring $K\{\tau\}$ consists of "noncommutative polynomials" in $\tau$ of the form $\sum_{i=0}^{r} C_i\tau^i$,

$c_i \in K$, whereby $\tau c = c^p \tau$ for $c \in K$. We denote by D the homomorphism

$$D: K\{\tau\} \to K, \quad D: \sum c_i \tau^i \mapsto c_0.$$

3. Definition. An elliptic A-module of rank 2 over K is a ring homomorphism $\varphi: A \to K\{\tau\}$ such that a) $\varphi(a) = i(a) + \sum_{i=1}^{2|a|} \varphi_i(a) \cdot F^i$, where $F = \tau^s$ is the Frobenius endomorphism over the field $F_q$; b) $\varphi_{2|a|}(a) \neq 0$ for all $a \in A \setminus \{0\}$.

Below we shall deal only with elliptic A-modules of rank 2 and speak simply of an "elliptic module" in place of an "elliptic A-module of rank 2."

It is clear that an elliptic module over K is determined by giving the element

$$\varphi(T) = i(T) + c_1 \cdot F + c_2 \cdot F^2, \quad c_1\, c_2 \in K,\ c_2 \neq 0.$$

4. Definition. A homomorphism of an elliptic module $\varphi: A \to K\{\tau\}$ into an elliptic module $\psi: A \to K\{\tau\}$ is an element $u \in K\{\tau\}$ such that $u \cdot \varphi(a) = \psi(a) \cdot u$ for all $a \in A$. If $u \neq 0$, then u is called an isogeny. The composition of homomorphisms is given, by definition, by the multiplication in $K\{\tau\}$. The set of all homomorphisms from $\varphi$ to $\varphi$ forms an A-subalgebra in $K\{\tau\}$ denoted by $\mathrm{End}(\varphi)$. Elliptic modules $\varphi$ and $\psi$ are isomorphic if and only if there exists $\lambda \in K^\times$ such that $\varphi(a) = \lambda \psi(a) \lambda^{-1}$ for all $a \in A$. In other words, let

$$\varphi(T) = i(T) + c_1 \cdot F + c_2 \cdot F^2,$$
$$\psi(T) = i(T) + d_1 \cdot F + d_2 \cdot F^2;$$

then $\varphi$ and $\psi$ are isomorphic if and only if $d_1 = \lambda^{q-1} c_1$, $d_2 = \lambda^{q^2-1} c_2$ for some $\lambda \in K^\times$. In particular, the group of automorphisms $\mathrm{Aut}(\varphi) = \mathrm{End}(\varphi)^\times$ can be described as follows:

$$\mathrm{Aut}(\varphi) = \begin{cases} F_q^\times, & c_1 \neq 0, \\ F_{q^2}^\times \cap K, & c_1 = 0. \end{cases}$$

5. "Characteristic" and Points of Finite Order. Let $i: A \to K$ be as above. Then the kernel Ker i of the homomorphism i is a prime ideal P(i) in A; P(i) is called the "characteristic" of the A-algebra K and is written "char" K. If i is injective then we speak of the general "characteristic"; otherwise, "char" K is a closed point of Spec A.

The ring A is a principal-ideal ring; therefore, for any nonzero ideal I there is defined a unitary polynomial $p_I$ such that $I = p_I A$. For an elliptic module $\varphi$ we define the scheme $G_I$ — the analogue of the scheme of "points of order n on an elliptic curve":

$$G_I = \bigcap \{\mathrm{Ker}\, \varphi(a) \mid a \in I\} = \mathrm{Ker}\, \varphi(p_I) \subset G_a \otimes K,$$

$G_I$ is a finite, flat group subscheme in $G_a \otimes K$.

6. Proposition. Let $\varphi: E \to K\{\tau\}$ be an elliptic module, and let I be a nonzero ideal in A. Then

a) The scheme $G_I$ is etale if and only if

$$\text{«char»}\, K \notin V(I) = \{P \in \mathrm{Spec}\, A \mid P \supseteq I\}.$$

b) The order of $G_I$ is equal to $|A/I|^2 = q^{2m}$, where $m = \deg p_I$.

7. Elliptic Modules over a Scheme; Modular Manifolds. In order to define schemes of moduli of elliptic modules it is necessary to consider the relative situation, i.e., elliptic modules over an A-scheme S. Thus, let S be a scheme over A.

8. Definition. An elliptic module over S is a pair $(L, \varphi)$ consisting of a linear bundle L on S and an $F_q$-linear homomorphism $\varphi: A \to \mathrm{End}_{F_q}(L)$ such that

a) $\varphi(a) = i(a) + \sum_{i=1}^{2|a|} \varphi_i(a) F^i$,

where $i(a)$ is the image of $a \in A$ under the natural action of A on L, $F \in \mathrm{End}_{F_q}(L)$ is the morphism of raising to the power q, and $\varphi_i(a) \in \Gamma(S, L^{\otimes(1-q^i)})$;

b) a section $\varphi_{2|a|}(a) \in \Gamma(S, L^{\otimes(1-q^{2|a|})})$ for any $a \in A \setminus \{0\}$ vanishes nowhere on S. For S = Spec K

Definition 8 goes over into Definition 3. Analogous to the situation existing in the theory of elliptic curves, in order that there exist (fine) schemes of modules it is necessary to fix some additional structure on the elliptic modules called a "level structure" as in the case of elliptic curves.

9. Definition. Let $E = (L, \varphi)$ be an elliptic module over S, let $I = (p_I)$ be a nonzero ideal in A, and let $G_I = \operatorname{Ker}\varphi(p_I) \subset G_a \times S$ be the subscheme of points of order I on E. A level structure of I on E is an isomorphism of group schemes over S:

$$\lambda : (I^{-1}/A)^2 \times S \to G_I,$$

consistent with the action of A.

It follows from Proposition 6 that a level structure of I on E exists only if for all points of S their "characteristics" do not lie in V(I). If this condition is satisfied, then there exists an etale covering $S' \to S$ such that $E \underset{S}{\times} S'$ possesses a level structure of I.

Suppose now that $F_I$ is a functor assigning to each scheme S over A the set of isomorphism classes of elliptic modules equipped with a level structure of I.

10. Proposition. The functor $F_I$ can be represented by an affine scheme $M_I$ of finite type over A. The morphism $M_I \to A$ is smooth; its fibers are one-dimensional over $\operatorname{Spec} A \setminus V(I)$ and are empty over V(I).

On the scheme $M_I$ there is a natural action of the group GL(2, A/I). This action arises from the following action of GL(2, A/I) on the functor $F_I$: if E is an elliptic module over S, $\lambda : (I^{-1}/A)^2 \times S \to G_I$ is a level structure of I, and $h \in GL(2, A/I)$, then we set

$$h : (E, \lambda) \mapsto (E, \bar{\lambda}),$$

where $\bar{\lambda}$ is the level structure of I on E given by the composition

$$(I^{-1}/A)^2 \times S \xrightarrow{(h^{-1} \times \mathrm{Id}_S)} (I^{-1}/A) \times S \xrightarrow{\lambda} G.$$

11. Compactification of $M_I$. In analogy to the fact that classical modular curves admit canonical compactification by means of parabolic points, for the scheme $M_I$ there is also a canonical compactification. We denote by $B_I$ the integral closure of A in the maximal Abelian extension of the field k with conductor I which completely splits over the point $\infty$. Let $M_I^1 = \operatorname{Spec} B_I$.

12. Proposition. a) There exists exactly one smooth scheme $\bar{M}_I$ that is proper over $\operatorname{Spec} A[I^{-1}]$, contains $M_I$ as an open subscheme, and is such that the morphism $\bar{M}_I - M_I \to \operatorname{Spec} A[I^{-1}] = \operatorname{Spec} A \setminus V(I)$ is finite.

b) The scheme $\operatorname{Cusps}_I = \bar{M}_I - M_I$ as a reduced scheme over $\operatorname{Spec} A[I^{-1}]$ is isomorphic to the disjoint union of a finite number of copies of $M_I^1$.

For the scheme $\bar{M}_I - M_I$ there is also an "analytic" description which is altogether analogous to the description of parabolic points for classical modular curves. Let $\Gamma(I) = \operatorname{Ker}(GL(2, A) \to GL(2, A/I))$ be the principal congruence-subgroup of the level I in GL(2, A).

13. Proposition. On each connected component of the curve $\bar{M}_I \otimes k_\infty$ the part of the set $(\bar{M}_I - M_I) \otimes k_\infty$ lying on this component is in canonical bijection with the set of representers of $\Gamma(I) \setminus P^1(k)$ under the natural action of $\Gamma(I)$ on $P^1(k)$.

14. Proposition. The genus of any of the components of the curve $\bar{M}_I \otimes k_\infty$ is equal to

$$1 + (q^2-1)^{-1} \cdot q^{2\deg p_I} (q^{\deg p_I} - q - 1) \cdot \prod_{r \mid p_I,\ r \text{ is irreducible and unitary}} (1 - q^{-2\deg r}).$$

15. Proposition. There exists a morphism $\pi : \bar{M}_I \to M_I^1$ with complete, smooth, geometrically irreducible fibers.

The action of the group GL(2, A/I) on $M_I$ extends to an action on $\bar{M}_I$. On the other hand, on the scheme $M_I^1$ according to class field theory there acts the group $\mathcal{A}_f^\times / k^\times V_I$, canonically isomorphic to $(A/I)^\times / F_q^\times$, where $\mathcal{A}_f$ is the adele ring of the field k without the $\infty$-component; $V_I$ is the kernel of the natural mapping of the closure $\prod_{v \in \operatorname{Max}(A)} A_v$ of the ring A in $\mathcal{A}_f$, into

$(A/I)^\times$. It turns out that the actions of the group GL(2, A/I) on $\overline{M}_I$ and the group $(A/I)^\times/F_q^\times$ on $M_I^1$ are consistent with the morphism $\pi$:

16. Proposition. There is the relation

$$\pi \circ g = \mu(g) \circ \pi,$$

where $g \in GL(2, A/I)$ and $\mu(g) \in (A/I)^\times/F_q^\times$ is the image of $\det g \in (A/I)^\times$.

17. Curves $X_0(I)$, $X_1(I)$, $C(I)$. Let $\nu: A \to F_q$ be the morphism of factorization by the ideal (T). We denote by X(I) the smooth curve $\overline{M}_I \otimes_A F_a$, where the tensor product is taken relative to the morphism $\nu$. From the smoothness of the scheme $\overline{M}_I$ over Spec $A \setminus V(I)$ it follows that for the curve X(I) Propositions 13-16 remain in force. We now define the curves $X_0(I)$, $X_1(I)$ and C(I) which we shall need in constructing codes.

Let $\Gamma_0(I)$, $\Gamma_1(I)$, H(I) be the following subgroups of G = GL(2, A):

$$\Gamma_0(I) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \mid c \in I \right\};$$

$$\Gamma_1(I) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \mid c \in I,\ a - 1 \in I \right\};$$

$$H(I) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \mid b, c, a - d \in I \right\}$$

and let $\overline{\Gamma_0(I)}$, $\overline{\Gamma_1(I)}$, $\overline{H(I)}$ be the images of $\Gamma_0(I)$, $\Gamma_1(I)$, H(I) in GL(2, A/I). We set

$$X_0(I) = X(I)^{\overline{\Gamma_0(I)}};$$
$$X_1(I) = X(I)^{\overline{\Gamma_1(I)}};$$
$$C(I) = X(I)^{\overline{H(I)}}.$$

We now suppose that the ideal I is prime and is generated by an irreducible polynomial $p_I(T) \in A$ of odd degree m.

18. LEMMA. a) The curves $X_0(I)$, $X_1(I)$, C(I) are smooth, absolutely irreducible curves over $F_q$.

b) The curve C(I) is a form of one of the components of X(I).

Proof. a) By Proposition 15 the fibers of the morphism $X(I) \to M_I^1 \otimes F_q$ are absolutely irreducible. Hence, considering Proposition 16, we see that the fibers of the morphisms, $X_0(I) \to (M_I^1 \otimes F_q)^{H_0}$, $X_1(I) \to (M_I^1 \otimes F_q)^{H_1}$, $C(I) \to (M_I^1 \otimes F_q)^F$, where $H_0$, $H_1$, F are the images of $\overline{\Gamma_0(I)}$, $\overline{\Gamma_1(I)}$ and $\overline{H(I)}$ in $(A/I)^\times$, are absolutely irreducible. It is easy to verify that $H_0 = H_1 = F = (A/I)^\times$ whence $(M_I^1 \otimes F_q)^{H_0} = (M_I^1 \otimes F_q)^{H_1} = (M_I^1 \otimes F_q)^F = F_q$. b) The assertion follows from the fact that under our assumptions on I the mapping $\bar{\mu}: \overline{H(I)}/F_q^\times \to (A/I)^\times/F_q^\times$ is an isomorphism.

We shall now show that on the curves C(I) and $X_0(I)$ the possible maximum of the ratio of the number of points to the genus of the curve is achieved.

19. Proposition. Let N(I) be the number of $F_{q^2}$-rational points on C(I), let g(I) be the genus of C(I), and let m(I) be the degree of the irreducible polynomial generating I. Then

$$\lim_{m(I) \to \infty} \frac{N(I)}{g(I)} = q - 1.$$

Proof. It suffices to establish that $\lim(N(I)/g(I)) \geqslant q - 1$, since the reverse inequality was proved in part 3.8 of the first chapter. Since C(I) is a form of an irreducible component of X(I), the following formula holds for g(I) (Proposition 14): $g(I) = 1 + (q^{2m} - 1)(q^m - q - 1)/(q^2 - 1)$, $m = m(I)$. We consider the projection $C(I) \to P^1 = C(I)^{PGL(2, A/I)}$; its degree is equal to $|PGL(2, A)| = q^m(q^{2m} - 1)$. Points corresponding to the elliptic module $\varphi_0$, $\varphi_0(T) = F^2$ are branch points with indices $(q + 1)$; this follows from the description of the group $\mathrm{Aut}(\varphi)$ given following Definition 4. Hence, the number of such points is equal to $(q + 1)^{-1}|PGL(2, A/I)| = q^m(q^{2m} - 1)/(q^2 - 1)$. It suffices to show that all these points are $F_{q^2}$-rational, so that

$$\frac{N(I)}{g(I)} \geqslant \frac{q^m(q^{2m}-1)/(q+1)}{1+(q^{2m}-1)(q^m-q-1)/(q^2-1)} \geqslant q-1.$$

For this, in turn, it suffices to show that any structure $\lambda$ of the level I on the module $\varphi_0$ under the action of $F^2$ gives a structure lying over the same point in C(I) as the original structure (here the pair $(\varphi_0, \lambda)$ is considered as a point of X(I)). This fact follows from the remark that under the representation of $(\mathrm{End}(\varphi_0)\otimes_A A/I)^\times$ in GL(2, A/I) given by the action of $(\mathrm{End}(\varphi_0)\otimes_A A/I)^\times$ on the level structure of I the element $F^2$ goes into H(I). The latter follows from the fact that $F^2$ lies in the center of $\mathrm{End}(\varphi_0)$, since $\mathrm{End}(\varphi_0)=\mathbf{F}_{q^2}\{F\}$, $\mathrm{Cent}(\mathrm{End}(\varphi_0))=\mathbf{F}_q[F^2]$; therefore, the image of $F^2$ lies in $\mathrm{Cent}(\mathrm{GL}(2, A/I)) = H(I)$.

COROLLARY. Let $N_0(I)$ be the number of $\mathbf{F}_{q^2}$-rational points on $X_0(I)$, $g_0(I)$ = genus $X_0(I)$. Then

$$\lim_{m(I)\to\infty} \frac{N_0(I)}{g_0(I)} = q-1.$$

Proof. Let d be the degree of the natural projection $C(I) \to X_0(I)$. Then it is clear that $N_0(I) \geqslant N(I)/d$, $g_0(I) \leqslant g(I)/d$ whence the corollary follows.

The images of $(\bar{M}_I - M_I)$ in $X_0(I)$, $X_1(I)$, and C(I) we shall call cusps and write $(\mathrm{Cusps})_0$, $(\mathrm{Cusps})_1$, $(\mathrm{Cusps})_C$. Taking into account the description of $\bar{M}_I - M_I$ given in Propositions 12 and 13, it is easy to prove the following proposition which is analogous to those that hold for classical modular curves.

20. Proposition. a) The number of cusps of the curve $X_0(I)$ is equal to 2, $(\mathrm{Cusps})_0 = \{Q_1, Q_2\}$. b) The projection $p: X_1(I) \to X_0(I)$ is a principal bundle with structure group $H = (A/I)^\times/\mathbf{F}_q^\times$; in particular, $|(\mathrm{Cusps})_1| = 2h$, where $h = |H| = (q^m - 1)/(q - 1)$.

Proof. a) From Proposition 13, which remains in force for X(I), it follows that $(\mathrm{Cusps})_0 \simeq \Gamma_0(I)\backslash \mathbf{P}^1(k)$. Standard arguments showing that the set $\Gamma_0(p)\backslash\mathbf{P}^1(\mathbf{Q})$ consists of two elements if p is a prime number (see, for example, [19, p. 46]) carry over literally to the case $\Gamma_0(I)\backslash\mathbf{P}^1(k)$. b) It suffices to show that the action of H on $X_1(I)$ is free. This follows from the description of the groups $\mathrm{Aut}(\varphi)$, where $\varphi$ is the elliptic module given after Definition 4, and the fact that $h = (q^m - 1)/(q - 1) \equiv 1 \pmod{q+1}$, so that H does not contain $\mathbf{F}_{q^2}^\times/\mathbf{F}_q^\times$.

In exactly the same way as in the classical case of curves $X_1(p)$ we obtain the following result.

COROLLARY. For one of the points $Q \in (\mathrm{Cusps})_0$ all points of $p^{-1}(Q)$ are determined over $\mathbf{F}_q$.

Below we shall denote by $Q_1$ that point of $(\mathrm{Cusps})_0$ for which the points of $p^{-1}(Q_1)$ are determined over $\mathbf{F}_q$. The next proposition, which is analogous to the classical description of noncuspidal points of the modular curve $X_1(n)$, gives a representation of $X_1(I)\backslash(\mathrm{Cusps})_1$ as manifolds of moduli.

Proposition. Let L be an extension of $\mathbf{F}_q$. Then there is the natural bijection

$$Y_1(I)(L) \rightleftarrows \left\{\begin{array}{l}\text{Isomorphism classes of pairs } (\varphi, c), \text{ where } \varphi \text{ is an elliptic}\\ \text{A-module over L and } c \neq 0 \text{ is a point of order I on } \varphi\end{array}\right\}.$$

Here $Y_1(I) = (M_I\otimes\mathbf{F}_q)^{\overline{\Gamma_1(I)}} = X_1(I)\backslash(\mathrm{Cusps})_1$.

Proof. It suffices to note that $M_I^{\Gamma_1(I)}$ is a functor on the category of schemes over A:

$$G(S) = \left\{\begin{array}{l}\text{Isomorphism classes of pairs } (\varphi, c), \text{ where } \varphi \text{ is an elliptic}\\ \text{A-module over S and } c \neq 0 \text{ is a point of order I on } \varphi\end{array}\right\}.$$

This follows from the fact that $M_I$ is a scheme of moduli of elliptic modules with a level structure of I such that the pairs $(\varphi, c)$ have no nontrivial automorphisms and such that the set of classes $\lambda \bmod \Gamma_1(I)$, where $\lambda$ is a level structure of I on the elliptic module, can be canonically identified with the set of points $c \neq 0$ of order I on $\varphi$.

## 3. Realization of "Modular" Codes

1. In the present section we shall prove a theorem giving a realization of a code C in terms of special values of polynomials in two variables of bounded degree which satisfy some linear conditions. A code C is given, by definition, in terms of a curve $X_0(I)$, but it will

be more convenient for us to work with $X = X_1(I)$, since $X_1(I)$ has a flat (special) model $\tilde{X}_1$. The objects connected with $X_0(I)$ we describe by means of the projection $p: X_1(I) \to X_0(I)$. Below we assume that the ideal $I = p_I A$ is generated by a unitary polynomial of degree m that is irreducible over $\mathbf{F}_q$:

$$p(T) = p_I(T) = \sum_{k=0}^{m} a_m T^m, \quad a_i \in \mathbf{F}_q, \quad a_m = 1,$$

where $m \geqslant 3$ is an odd natural number relatively prime to $q - 1$.

We define the polynomials $\varphi_k(x, y) \in \mathbf{F}_q[x, y]$, $k = 0, 1, \ldots$, by induction, setting

$$\varphi_0(x, y) = 1,$$
$$\varphi_{k+1}(x, y) = x \cdot \varphi_k(x, y)^{q^2} + y \cdot \varphi_k(x, y)^q$$

for $k \geqslant 0$.

We note that for the elliptic module

$$\varphi: A \to \bar{F}_q\{F\}, \quad \varphi(T) = aF^2 + bF, \quad a, b \in \bar{\mathbf{F}}_q$$

the action of $\varphi(T)^k$ on the element $1 \in \bar{\mathbf{F}}_q$ is given as

$$\varphi(T^k)(1) = \varphi_k(a, b).$$

2. LEMMA. Let $\tilde{X}_1 \subset \mathbf{P}^2$ be a curve with the affine equation

$$F(x, y) = \sum_{k=0}^{m} a_k \varphi_k(x, y).$$

Then

a) $\tilde{X}_1$ is an absolutely irreducible curve that is smooth in $A^2$.

b) The curve $\tilde{X}_1$ has exactly two singular points $P_1 = (0:0:1)$, $P_2 = (0: -1:1)$.

c) $\tilde{X}_1$ is birationally isomorphic to X over $\mathbf{F}_q$.

Proof. a) The irreducibility of $\tilde{X}_1$ follows from c). We shall prove the smoothness of $\tilde{X}_1$ in $A^2$. It is easy to verify that

$$\frac{\partial \varphi_k(x, y)}{\partial x} = \varphi_{k-1}(x, y)^{q^2}, \quad \frac{\partial \varphi_k(x, y)}{\partial y} = \varphi_{k-1}(x, y)^q$$

for all $k \geqslant 1$. Hence,

$$F_x = \partial F / \partial x = \sum_{k=1}^{m} a_k \varphi_{k-1}(x, y)^{q^2},$$

$$F_y = \partial F / \partial y = \sum_{k=1}^{m} a_k \varphi_{k-1}(x, y)^q.$$

We shall show that the system of equations

$$\begin{cases} F_x(x, y) = 0, \\ F_y(x, y) = 0, \\ F(x, y) = 0 \end{cases}$$

has no solutions. Indeed,

$$F - (xF_x + yF_y) = F - \sum_{k=1}^{m} a_k (x\varphi_{k-1}^{q^2} + y\varphi_{k-1}^q) = \sum_{k=0}^{m} a_k \varphi_k - \sum_{k=1}^{m} a_k \varphi_k = a_0 \neq 0,$$

by the irreducibility of

$$p(T) = \sum_{k=0}^{m} a_k T^k.$$

b) Let $(X_0, X_1, X_2)$ be homogeneous coordinates on $P^2$, $x = X_1/X_0$, $y = X_2/X_0$.

It is easy to verify that the homogeneous equation $G(X_0, X_1, X_2) = 0$ of the curve $\tilde{X}_1$

$$G = X_0^{(q^{2m}-1)/(q^2-1)} \mathbf{E}(X_1/X_0, X_2/X_0)$$

has the form

$$G(X_0, X_1, X_2) = X_1^{(q^{2m-2}-1)/(q^2-1)}(X_1+X_2)^{q^{2m-2}} + X_0^2 H(X_0, X_1, X_2),$$

where $H(X_0, X_1, X_2) \in F_q[X_0, X_1, X_2]$. Hence $(\mathbf{P}^2 \setminus \mathbf{A}^2) \cap \tilde{X}_1$ consists of exactly two points $P_1$ and $P_2$, and it is easy to verify that they are both singular.

c) As shown in Proposition 2.21, the $F_q$-points of $X \setminus (\mathrm{Cusps})_1$ are in bijection with the isomorphism classes of pairs $(\varphi, c)$ where $\varphi$ is an elliptic module over $\bar{F}_q$ and $c \neq 0$ is a point of order $p_I$ on $\varphi$. Let $\varphi(T) = aF^2 + bF$. Then the isomorphism classes of pairs $(\varphi, c)$ are in bijection with triples $(a, b, c)$, where $a \neq 0$, $c \neq 0$, $a, b, c \in \bar{F}_q$, considered up to the equivalence relation $(a, b, c) \sim (a', b', c')$, if $a' = \lambda^{q^2-1}a$, $b' = \lambda^{q-1}b$, $c' = \lambda^{-1}c$ for some $\lambda \in \bar{F}_q^{\times}$, and the relation $\varphi(p_I(T))(c) = 0$ is satisfied. It is clear that for each triple $(a, b, c)$ there exists a unique triple $(a', b', 1)$, equivalent to it where $a' = c^{q^2-1}a$, $b' = c^{q-1}b$. Now, defining the mapping

$$\nu: (a', b', 1) \mapsto (a', b') \in \mathbf{A}^2,$$

we see that it is a bijection $\nu: (X \setminus (\mathrm{Cusps})_1)(\bar{F}_q) \xrightarrow{\sim} \tilde{X}_1 \cap (\mathbf{A}^2 \setminus \{x = 0\})$.

It is clear that the mapping constructed is equivariant relative to the action of $\mathrm{Gal}(\bar{F}_q/F_q)$. It is therefore defined over $F_q$, and, because of the fact that it is bijective on $\bar{F}_q$-points, it is the composition of a birational isomorphism and a purely inseparable mapping. Applying, if necessary, the Frobenius morphism over $F_q$ several times to the curve X, we obtain assertion c).

3. LEMMA. a) The mapping $\nu: X \to \tilde{X}_1$ is a normalization of the curve $\bar{X}_1$. b) Let $r(T) \in A = F_q[T]$, $\deg r(T) \leqslant m-1$, and let $r(T) = \sum_{k=0}^{m-1} r_k T^k$ be a polynomial whose image in $H = (A/I)^{\times}/F_q^{\times}$ is a generator $\theta$ of the group H. Then the action of $\theta$ on $\tilde{X}_1$ induced by the action on X is given as follows:

$$\theta: (x, y) \mapsto (x', y'),$$

where

$$x' = x\left(\sum_{k=0}^{m-1} r_k \varphi_k(x, y)\right)^{q^2-1},$$

$$y' = y\left(\sum_{k=0}^{m-1} r_k \varphi_k(x, y)\right)^{q-1}.$$

c) In the notation of the corollary of Proposition 2.20 we have $\nu^{-1}(\{P_1, P_2\}) = p^{-1}(Q_1)$, $\nu^{-1}(\tilde{X}_1 \cap \{x = 0\}) = p^{-1}(Q_2)$.

d) Let $z = x/y = X_1/X_2$, $t = 1/y = X_0/X_2$ be coordinates in $\mathbf{P}^2 - \{X_2 = 0\}$. Then the local equation of $\tilde{X}_1$ in a neighborhood of the points $P_1$ and $P_2$ is

$$F^*(z, t) = t^{(q^{2m}-1)/(q^2-1)} F(z/t, 1/t).$$

Proof. a) and d) are obvious. b) It suffices to observe that on triples $(a, b, 1)$ the action of $\theta$ is given as follows:

$$\theta: (a, b, 1) \mapsto (a, b, c),$$

where

$$c = \sum_{k=0}^{m-1} r_k \varphi_k(a, b),$$

since $\varphi(T^k)(1) = \varphi_k(a, b)$ for $\varphi(T) = aF^2 + bF$.

c) The set $\tilde{X}_1 \cap \{x = 0\}$ is given by the equation

$$F(y) = F(0, y) = \sum_{k=0}^{m} a_k \varphi_k(0, y) = \sum_{k=0}^{m} a_k y^{(q^k-1)/(q-1)} = 0.$$

It contains $h = (q^m - 1)/(q - 1)$ elements, and by the irreducibility of $p_I(T)$ no one of them is defined over $F_q$. It is clear also that by b) $\tilde{X}_1 \cap \{x=0\}$ is taken into itself by the action of $\theta$. Therefore, $\nu^{-1}(\tilde{X}_1 \cap \{x=0\})$ coincides with $p^{-1}(Q_2)$, and $\nu^{-1}(\{P_1, P_2\}) = p^{-1}(Q_1)$.

4. Divisor of Double Points of $\tilde{X}_1$. We recall that in the situation where there is a singular, absolutely irreducible curve $C'$ over a perfect field $l$ and its normalization $C$ there is defined an effective divisor $D \in \mathrm{Div}(C)$ called in classical theory the divisor of double points of the curve $C'$. In the notation of the fourth chapter of [13] we have $D = \sum_P nP$, so that for the conductor $\mathfrak{c} = \mathfrak{c}(C/C')$ there is the equality

$$\mathfrak{c} = \{f \in l(C) \mid f \equiv 0 \bmod D\};$$

usually the divisor D is identified with the conductor $\mathfrak{c}$ (see, for example, [13, Chap. 4]). For a plane curve with equation $F(x, y) = 0$ there is the following formula which can also be taken as the definition of D [17, p. 192]:

$$D = \mu \cdot (x) + (\nu - 2) \cdot (y) - B_x + (F_x'),$$

where $\mu = \deg_x F$, $\nu = \deg_y F$, $(f)$ denotes the divisor of a rational function f on the curve C, and $B_X$ is the branching divisor of the projection $C \to \mathbf{P}^1$ given by a rational function $x \in l(C)$.

In the definition of D summation goes over points $P \in C$ lying over singular points of $C'$. We need to consider a divisor of double points $D \in \mathrm{Div}(X)$ of the curve $X_1$. For its degree it is easy to obtain the following estimate.

5. LEMMA. Let $d = \deg D$. Then $d < q^{4m-2}$.

Proof. There is a classical formula for the degree of a divisor of double points of a plane curve [17, p. 193]: $d = (\mu - 1)(\nu - 1) - g$, where g is the genus of the curve. Noting that $\mu = \deg_x F(x, y) = (q^{2m} - 1)/(q - 1)$, $\nu = \deg_y F = q^{2m-2}$, we obtain the assertion of the lemma.

6. The Linear System $\mathcal{L}(F)$. To construct the generating matrix of a code we must have an explicit description of the space $\mathcal{L}(F)$ where $F = bQ_1 \in \mathrm{Div}(X_0(I))$, $1 \leqslant b \leqslant q^m$, and $\{Q_1, Q_2\}$ is the set of cusps of the curve $X_0(I)$.

To determine $\mathcal{L}(F)$ explicitly it is more convenient for us to work with the curve X rather than $X_0(I)$, since X has a convenient plane model. This can be done because of the following lemma.

7. LEMMA. Let $\theta$ be a generator of the group $H = (A/I)^x/F_q{}^x$. We denote by $\sigma$ the following element of the group ring $\mathbf{Z}[H]$: $\sigma = 1 + \theta + \ldots + \theta^{h-1}$, where $h = |H| = (q^m - 1)/(q - 1)$. Then $p^* \mathcal{L}(F) = \sigma(\mathcal{L}(p^*F))$, where $p: X_1(I) \to X_0(I)$.

Proof. It is easy to verify that $p^*\mathcal{L}(F) = \mathcal{L}(p^*F)^H$. Noting that $\mathcal{L}(p^*F)$ is a finite-dimensional vector space over $F_p$ and hence has $p^a$ elements and noting the circumstance that the order h of the group H is relatively prime to p, we obtain the cohomological triviality of the H-module $\mathcal{L}(p^*F)$ and the equality $p^*\mathcal{L}(F) = \mathcal{L}(p^*F)^H = \sigma(\mathcal{L}(p^*F))$.

The space $\mathcal{L}(p^*F)$ can be realized by means of polynomials of bounded degree:

8. Proposition. Let

$$V = \{p(x, y) \in \mathbf{F}_q[x, y] \mid \deg p(x, y) \leqslant e = q^{4m}\}$$

and let W be the image of V in $F_q(X)$. Then

$$\mathcal{L}(p^*F) \subset W.$$

Proof. Let $f \in \mathcal{L}(p^*F)$. Because of the fact that the singularities $P_1$, $P_2$ of the curve $\tilde{X}_1$ lie at infinity, there exists an $h \in F_q[x, y]$ such that $f = h(x, y)$ as functions on X (see for example, [17, p. 198]). Let $s = \deg h(x, y)$. We shall show that if $s > q^{4m}$, then there exists $g \in F_q[x, y]$ such that $\deg g = s' < s$ and $f = g(x, y)$ as functions on X. In homogeneous coordinates $(X_0, X_1, X_2)$ we have $h(x, y) = H(X_0, X_1, X_2)/X_0{}^S$ where $H(X_0, X_1, X_2)$ is a homogeneous form of degree s. We consider the divisor $(H) \in \mathrm{Div}(X)$ — the preimage of the cycle $(H \cdot \tilde{X}_1)$ under the normalization mapping $\nu: X \to \tilde{X}_1$. Let $Q \in \mathrm{Supp}(X_0) = \nu^{-1}(\{P_1, P_2\}) \subset \mathrm{Supp}(H)$. Because of the fact that $f \in \mathcal{L}(p^*F)$, there is the inequality $\nu_Q(f) \geqslant -b$, which can be rewritten in the form

$$-b \leqslant \nu_Q(f) = \nu_Q(H/X_0{}^s) = \nu_Q((H)) - s \cdot \nu_Q((X_0)),$$

whence

$$v_Q((H)) \geqslant s v_Q((X_0)) - b \geqslant s - b - 1 + v_Q((X_0)).$$

Thus,

$$H \geqslant \sum_{Q \in v^{-1}(\{P_1, P_2\})} (s - b - 1) Q + (X_0).$$

We now note that for the divisor D of double points of $\tilde{X}_1$ we have

$$D = \sum_{Q \in v^{-1}(\{P_1, P_2\})} n_Q \cdot Q \leqslant \sum_{Q \in v^{-1}(\{P_1, P_2\})} (\deg D) Q.$$

By Lemma 4 deg D $\leqslant q^{4m-2} < q^{4m} - q^m - 1 < s - b - 1$, and hence

$$(H) \geqslant D + (X_0).$$

Applying the (AF + BG)-theorem of Noether [9, Vol. II, p. 746], we see that there are forms A and B of degrees $s - 1$ and $s - \deg G$, respectively, such that $H = X_0 \cdot A + G \cdot B$ (equality in the ring of polynomials $F_q[X_0, X_1, X_2]$). Here G, as in part 2, is the homogeneous equation of $\tilde{X}_1$. It is now possible to set $g(x, y) = A(X_0, X_1, X_2)/X_0^{s-1}$, deg $g(x, y) \leqslant s - 1$.

9. Graph of the Resolution of Singularities of $\tilde{X}_1$. We need to consider the graph $\Gamma = \Gamma_1 \cup \Gamma_2$ where $\Gamma_1 = \Gamma_{P_1}$, $\Gamma_1 = \Gamma_{P_2}$ are trees of the resolution of singular points of the curve $\tilde{X}_1$. Let $P \in \{P_1, P_2\}$. We define the tree of the resolution $\Gamma_P$ of the point P. For its definition it is necessary to consider the process of resolving singularities of $\tilde{X}_1$ by means of a sequence of monoidal transformations. We recall some facts we need. Let C be an irreducible curve on a smooth projective surface F defined over an algebraically closed field $l$. The following classical result holds.

10. Proposition. There exists a finite sequence of monoidal transformations (with suitable centers)

$$F_n \to F_{n-1} \to \ldots \to F_1 - F_0 = F$$

such that the proper preimage of $C_n$ on $F_n$ of the curve C is a nonsingular curve (and hence coincides with the normalization of the curve C).

For a proof of the proposition see, for example, [15, p. 489].

It is most convenient to define the tree $\Gamma_P$ in terms of infinitely close points. We recall the definition of infinitely close points.

11. Definition. Let $f: F' \to F$ be a morphism of smooth projective surfaces which is the composition of a finite number of monoidal transformations. A point $Q \in F'$ is called infinitely close to a point $P \in F$ if Q belongs entirely to the curve E obtained on blowing up P. Let C be a curve on F; a point Q' is infinitely close for the curve C if $Q' \in C'$ where C' is the proper preimage of C on F'. Here if $f': F'' \to F'$ is a further sequence of monoidal transformations and $Q'' \in F''$ does not lie on the exceptional curve of f, then the infinitely close points Q'' and f(Q'') are identified. Thus, if $C \subset F$ is an irreducible curve on a surface F and $F' = F_n$ is the surface of Proposition 10, then each point $C \subset F$ has its system of infinitely close points, and this system consists of a single point if and only if the point P is a nonsingular point of C. With each point $P \in C$ there are connected two important invariants: its multiplicity $r_P \geqslant 1$ and the number $\delta_P \geqslant 0$ (for the definition of $r_P$ and $\delta_P$ see, for example, [15, pp. 379, 487], [13, p. 84]). An assertion holds which can be taken as the definition of $\delta_P$:

12. LEMMA. We have the formula

$$\delta_P = \sum_{Q \to P} 1/2 (r_Q (r_Q - 1)),$$

where $P \in C$ is an arbitrary point, $r_Q$ is the multiplicity of the point Q on the proper preimage of the curve C, and the summation goes over all infinitely close points C lying over P.

For a proof of the lemma see [15, p. 493].

COROLLARY. Let $p_a(C)$ be the arithmetic genus of a curve C. Then

$$g(C^{\nu})=p_a(C)-\sum_Q 1/2r_Q(r_Q-1), \tag{3}$$

where the summation goes over all points of the curve C including infinitely close points (the sum is meaningful, since $r_Q(r_Q-1)\neq 0$ only for a finite number of singular points Q).

Suppose now that P is a singular point of C. We call infinitely close points of first order those infinitely close points for the point P which lie on the surface $F_1$ obtained from F by blowing up the point P. Infinitely close points of r-th order ($r\geqslant 2$) are defined as infinitely close points lying on the surface obtained by blowing up one of the singular infinitely close points of (r − 1)-st order.

The tree $\Gamma_P$ of infinitely close points of a point P is defined as follows: its root $w = w_P$ corresponds to the point P; descendants of first order are in bijection with the infinitely close points of first order, ..., descendants of r-th order are in bijection with infinitely close points of r-th order. Hanging vertices of the tree $\Gamma_P$ are in bijection with points on the normalization $C^{\nu}$ of the curve C which lie over P. The set of vertices (hanging vertices) of the tree $\Gamma_P$ we denote by $V_P$ (respectively, $V_P'$); its power is $v_P$ (respectively, $v_P'$).

Below we shall consider the case of interest to us $F=\mathbf{P}^2$, $C=\tilde{X}_1$, $C^{\nu}\tilde{\to}X$, $V_1=V_{P_1}$, $V_2=V_{P_2}$, $V_1'=V_{P_1}'$, $V_2'=V_{P_2}'$. The field $\mathbf{F}_q$ can be taken as the base field, although it is not algebraically closed; all objects encountered in resolving singular points $P_1$, $P_2$ of the curve $\tilde{X}_1$ are defined over $\mathbf{F}_q$; this follows from the fact that all points in $\nu^{-1}(\{P_1, P_2\})\subset(\mathrm{Cusps})_1\subset X$ are defined over $\mathbf{F}_q$.

13. LEMMA. We have the inequality $v_1+v_2<(3/2)e=(3/2)q^{4m}$, where $v_i=|V_i|$, $i=1, 2$.

Proof. Since $d=\deg G=(q^{2m}-1)/(q^2-1)$, where G is the homogeneous equation of $\tilde{X}_1$, it follows that

$$p_a(\tilde{X}_1)=1/2(d-1)(d-2)<e/2.$$

By formula (3)

$$0\leqslant g(X)=p_a(\tilde{X}_1)-\delta_{P_1}-\delta_{P_2},$$

whence

$$v_1+v_2-v_1'-v_2'=\sum_{Q\to P_1,P_2}1\leqslant\sum_{Q\to P_1,P_2}1/2r_Q(r_Q-1)=\delta_{P_1}+\delta_{P_2}\leqslant e/2.$$

Noting that

$$v_1'+v_2'\leqslant\sum_{\substack{Q\to P_1,P_2\\ r_Q\geqslant 2}}r_Q\leqslant\sum_{Q\to P_1,P_2}r_Q(r_Q-1)=2(\delta_{P_1}+\delta_{P_2})\leqslant e,$$

we obtain the assertion of the lemma.

14. Labeled Trees $\tilde{\Gamma}_1$, $\tilde{\Gamma}_2$. For our basic purpose we shall need to consider labeled trees $\tilde{\Gamma}_1$, $\tilde{\Gamma}_2$ which are trees $\Gamma_1$, $\Gamma_2$ each vertex of which $s\in V_1\cup V_2$ is labeled by the set

$$(P_s(z_s, t_s), (\alpha_s, \beta_s), (Z_s, T_s), \Lambda_s),$$

where $z_S$, $t_S$ are local coordinates in a neighborhood of the infinitely close point $Q_S$ corresponding to s, $P_S(z_S, t_S)\in\mathbf{F}_q[z_S, t_S]$ is the local equation of the proper preimage of $\tilde{X}_1$ in a neighborhood of $Q_S$, and $(\alpha_S, \beta_S)\in\mathbf{F}_q^2$ are the values of the local coordinates of the point $Q_S$; $Z_S=Z_S(z_S, t_S)\in\mathbf{F}_q[z_S, t_S]$ is a polynomial giving the expression of the coordinate z on $\mathbf{P}^2$ in terms of $(z_S, t_S)$; $T_S=T_S(z_S, t_S)\in\mathbf{F}_q[z_S, t_S]$ is the same thing for the coordinate t; $\Lambda_S\in\{0, 1\}$ is the smoothness index of the point $Q_S$ (or, equivalently, the index of whether the vertex s is a hanging vertex or not).

The roots $w_i\in V_i$, $i=1, 2$ are labeled by the sets

$$(F^*(z, t), (\alpha_i, \beta_i), (z-\alpha_i, t-\beta_i), 0),$$

where $F^*(z, t)\in\mathbf{F}_q[z, t]$, as in Lemma 3, is the local equation of $\tilde{X}_1$ in a neighborhood of $P_i$:

$$F^*(z, t)=t^{(q^{2m}-1)/(q^2-1)}F(z/t, 1/t),$$
$$(\alpha_1, \beta_1)=(0, 0), \quad (\alpha_2, \beta_2)=(-1, 0).$$

15. Operators $R_m$ and $Q_n$. To introduce the functionals needed to construct a generating matrix of a code $C_{m,b}$ we shall find it convenient to use two types of operators acting in the ring of formal Laurent series. We shall present their definitions and elementary properties. Suppose K is a field, K((t)) is the field of formal Laurent series over K, and n is an integer.

16. Definition. Let $f = \sum_{i=h}^{\infty} a_i t^i \in K((t))$. We set, by definition,

$$R_n(f)=\sum_{i=h}^{n} a_i t^i \in K[t, t^{-1}],$$
$$Q_n(f)=a_n \in K.$$

The operator $R_n$ is a linear mapping of vector spaces over K,

$$R_n: K((t)) \to K[t, t^{-1}].$$

The operator $Q_n$ is a functional on K((t)),

$$Q_n: K((t)) \to K.$$

17. LEMMA. We have the following relations:

a) If $R_{-m-1}(f) = R_{-n-1}(g) = 0$, then for all integers k

$$R_k(f\cdot g)=R_k(R_{n+k}(f)\cdot R_{m+k}(g)),$$
$$Q_k(f\cdot g)=Q_k(R_{n+k}(f)\cdot R_{m+k}(g)).$$

b) For all integers k, n

$$R_k(t^{-n}f)=t^{-n}\cdot R_{k+n}(f),$$
$$Q_k(t^{-n}f)=Q_{k+n}(f).$$

18. The Functionals $A_{s,i}$. We now give the definition of the functionals in terms of which the generating matrix of a code C is realized. These functionals are numbered by points $Q \in \nu^{-1}(\{P_1, P_2\})$ or, equivalently, by hanging vertices $s \in V' = V_1' \cup V_2'$ of the graph $\tilde{\Gamma} = \tilde{\Gamma}_1 \cup \tilde{\Gamma}_2$. Let $Q = Q_s$ be the point corresponding to the vertex $s \in V'$, and let i be a nonnegative integer. The point $Q_s$ is nonsingular; therefore, one of the values $\frac{\partial P_s}{\partial z_s}(\alpha_s, \beta_s)$, $\frac{\partial P_s}{\partial t_s}(\alpha_s, \beta_s)$ is nonzero (notation as in part 14). We suppose to be specific that $\frac{\partial P_s}{\partial z_s}(\alpha_s, \beta_s)\neq 0$ (otherwise the places of $z_s$ and $t_s$ in all the following arguments must be interchanged). Then $u_s = (t_s - \beta_s)$ is a local parameter on the preimage of $\tilde{X}_1$ in a neighborhood of $Q_s$, and there exists an expansion of $z_s$ in a series in powers of $u_s$ (here $z_s$ and $t_s$ are considered as functions on the preimage of $\tilde{X}_1$):

$$z_s = f_s(u_s) \in \mathbf{F}_q[[u_s]].$$

By definition we set

$$A_{s,i}(p)=Q_i(p^*(Z_s(f_s(u_s), u_s+\beta_s), T_s(f_s(u_s), u_s+\beta_s)) \in F_q,$$

where $p = p(x, y) \in V$, $p^*(z, t) = t^e p(x, y)$, $e = q^4 m$, and the coordinates (x, y) are connected with the coordinates (z, t) as follows: $x = z/t$, $y = 1/t$. In other words, $A_{s,i}(p)$ is the i-th coefficient of the expansion of the rational function $t^e p(x, y)$ on X in a series in powers of $u_s$ — the local parameter in a neighborhood of the point $Q_s$; $A_{s,i}$ is an $F_q$-linear functional on V.

It follows directly from the definition of $A_{s,i}$ that the following assertion holds.

19. LEMMA. The condition

$$A_{s,0}(p)=A_{s,1}(p)=\ldots=A_{s,k}(p)=0$$

is equivalent to the condition

$$\operatorname{ord}_{Q_s}(\tilde{p}^*) \geqslant k+1,$$

where $\tilde{p}^*$ is the rational function on X defined by the polynomial p*(z, t).

We are now ready to give a realization of the space $\mathcal{L}(p^*F)$ in terms of the space V.

20. Proposition. Let $V_b$ be the following subspace of V:

$$V_b = \bigcap_{s \in V'} \bigcap_{i=0}^{(en_s - b)} \operatorname{Ker} A_{s,i}.$$

Then the image of $V_b$ in W coincides with $\mathcal{L}(p^*F)$. Here $n_s$ denotes the order of the function t at the point $Q_s$; it follows easily from Bezout's theorem that $n_s \leqslant q^{2m}$.

Proof. By Proposition 7, $\mathcal{L}(p^*F) \subset W$; it is only necessary to distinghish, among the elements of V, elements g such that $\operatorname{ord}_{Q_s}(\tilde{g}) \geqslant -b$ for all s, where $\tilde{g}$ is the rational function on X defined by the polynomial g. Considering the relation $g^* = t^e g$, the definition of $n_s$, and Lemma 19, we obtain the proposition.

21. "Supersingular" Points on X. As was shown in part 2.19, all points of $X_0(I)$ with the value y = 0 ("supersingular" points) are $F_{q^2}$-rational. It is possible to give an explicit description of the set of these points. For this it suffices to recall that there is an unramified covering $p : X \to X_0(I)$ with structure group $H = (A/I)^\times / F_q^\times$, while for X by Lemma 2 there is a plane model which is smooth at points with y = 0.

22. LEMMA. The coordination of points $\tilde{X}_1$ with y = 0 have the form $\{(\alpha, 0)\}$, where $\alpha$ is a root of the equation

$$F(x) = F(x, 0) = \sum_{k=0}^{m} a_k x^{(q^{2k}-1)/(q^2-1)} = 0.$$

The proof follows from Lemma 2.

COROLLARY. The number of "supersingular" $F_{q^2}$-points on $X_0(I)$ is equal to $n = (q^m+1)/(q+1)$.

Proof. The set of points $X_0(I)$ with y = 0 is in bijection with the set of orbits of the free action of the group H of order $h = (q^m-1)/(q-1)$ on the set R of roots of F(x) of power $|R| = (q^{2m}-1)/(q^2-1)$.

We denote by $H_1$ the subgroup of H generated by the image of an element $T \in A$, and we set $h_1 = |H_1|$, $h_2 = h/h_1 = [H : H_1]$.

23. LEMMA. The polynomial F(x) decomposes over $F_{q^2}$ into $nh_2$ factors each of which has degree $h_1$.

Proof. We note first of all that the generator $\lambda$ (the image of T) of the group $H_1$ acts as follows on points $X_1$: $\lambda : (x, y) \mapsto (x^{q^2} + x^{q^2-1}y, x^{q-1}y + y^q)$ for $(x, y) \in \tilde{X}_1$. This follows immediately from the definition of p and the action of H on points of X. From this it follows that on points with y = 0 the action of $\lambda$ coincides with the action of a generator of the group $\operatorname{Gal}(\overline{F}_q / F_{q^2})$. Noting now that the action of $H_1$ on the set R is free, we obtain the assertion of the lemma.

COROLLARY. a) Each orbit of H under the action on R is the union of sets of roots of factors of F(x) irreducible over $F_{q^2}$, the number of which is equal to $h_2$. b) The set R lies in the field $L = F_{q^{2h_1}}$.

24. Realization of the Code C. All that has been said above makes it possible to give a convenient realization of codes arising on the curve $X_0(I)$. As noted above, an algebro-geometric code C over $F_{q^2}$ is given by a generating matrix $M = (m_{\alpha\beta})$, where $\alpha$ runs through the set of indices of $F_{q^2}$-rational "supersingular" points $\{P_\alpha\}$ on $X_0(I)$, and $\beta$ is the set of indices of a basis $\{\varphi_\beta\}$ of the space $\mathcal{L}(F) \otimes F_{q^2}$ over $F_{q^2}$ or, equivalently, of a basis of $\mathcal{L}(F)$ over $F_q$;

$$m_{\alpha,\beta} = \varphi_\beta(P_\alpha) \in F_{q^2}.$$

Considering the description of the space $\mathcal{L}(F)$ given in Lemma 7, the realization of the space $\mathcal{L}(p^*F)$ given in Proposition 20, and also the description of the set of "supersingular" $F_{q^2}$-rational points on $X_0(I)$ given in parts 21-23, it is now possible to easily prove the main result of this section.

We consider the following $F_{q^2}$-linear mapping:

$$l: V_b \otimes \mathbf{F}_{q^2} \to (\mathbf{F}_{q^2})^n, \quad n = (q^m+1)/(q+1),$$
$$l: f \mapsto \sum_{\alpha \in R_\sigma} f(\alpha, 0), \quad \sigma \in S,$$

where $S \subset L$ is the set of representers of orbits of the action of the group H on the set of roots $R \subset L$ of the polynomial $F(x)$; $|S| = n$, and $R_\sigma$ for $\sigma \in S$ denotes the orbit of the element $\sigma$ under the action of H.

28. THEOREM. The image of $l$ in $(\mathbf{F}_{q^2})^n$ coincides with a $q^2$-ic algebrogeometric code $C_{m,b}$ and hence has parameters $k \geqslant b-g+1$, $d \geqslant n-b$, where $g = g(X_0(I))$.

Proof. It is clear that the mapping $l$ factors through the mapping $V_b \otimes \mathbf{F}_{q^2} \to W \otimes \mathbf{F}_{q^2} \subset \mathbf{F}_{q^2}(X)$; by Proposition 20 the image of $V_b \otimes \mathbf{F}_{q^2}$ in $W \otimes \mathbf{F}_{q^2}$ is equal to $\mathscr{L}(p^*\mathbf{F}) \otimes \mathbf{F}_{q^2}$. Since in the definition of $l$ summation goes over the orbits of the action of H, the image of $l$ coincides with the image in $(\mathbf{F}_{q^2})^n$ of the space $\sigma(\mathscr{L}(p^*\mathbf{F})) \otimes \mathbf{F}_{q^2}$, where $\sigma = (1+\theta+\ldots+\theta^{h-1}) \in \mathbf{Z}[H]$. But by Lemma 7 this space coincides with the image of $\mathscr{L}(F) \otimes \mathbf{F}_{q^2}$ in $(\mathbf{F}_{q^2})^n$ which was required to prove.

## 4. Formulas

1. In the present section formulas are given which define the objects needed in the process of constructing the generating matrix of a code C. In order to make the exposition in this and the following sections independent of the contents of Secs. 2 and 3 we give a description of these objects without appealing to algebraic geometry.

Let $p(T) = \sum_{k=0}^{m} a_k T^k \in \mathbf{F}_q[T]$ be a unitary polynomial of degree m irreducible over $\mathbf{F}_q$.

a) L denotes the field $\mathbf{F}_{q^{2h_1}}$, where $h_1$ is a divisor of $h = (q^m + 1)/(q + 1)$; the number $h_1$ is found in the process of the computations described in Sec. 5.

b) $\tilde{\Gamma}$ denotes the graph $\tilde{\Gamma} = \tilde{\Gamma}_1 \cup \tilde{\Gamma}_2$, where $\Gamma_i$ is the tree each vertex of which is labeled by the set

$$(P_s(z_s, t_s), (\alpha_s, \beta_s), (Z_s, T_s), \Lambda_s),$$

where $z_S$, $t_S$ are variables, $P_S(z_S, t_S)$, $Z_S = Z_S(z_S, t_S)$, $T_S = T_S(z_S, t_S) \in \mathbf{F}_q[z_S, t_S]$, $\alpha_S$, $\beta_S \in \mathbf{F}_q$, $\Lambda_S \in \{0, 1\}$. The root $w_1$ of the tree $\tilde{\Gamma}_1$ is labeled by the set

$$(F^*(z, t), (0, 0), (z, t), 0),$$

and the root $w_2$ of the tree $\tilde{\Gamma}_2$ is labeled by the set

$$(F^*(z, t), (-1, 0), (z+1, t), 0),$$

where

$$F^*(z, t) = t^{(q^{2m}-1)/(q^2-1)} F(z/t, 1/t),$$
$$F(x, y) = \sum_{k=0}^{m} a_k \varphi_k(x, k),$$
$$\varphi_0(x, y) = 1, \quad \varphi_{k+1} = x \cdot \varphi_k(x, y)^{q^2} + y \cdot \varphi_k(x, y)^q, \quad k \geqslant 0.$$

$V_i$ denotes the set of vertices of the tree $\Gamma_i$, $V = V_1 \cup V_2$, $V_i'$ denotes the set of hanging vertices, and $|V_1'| + |V_2'| = |V'| = h$. The set $V_S$ of descendents of a vertex $s \in V \setminus V'$ and its labels is constructed on the basis of the collection of labels of s. In part 2 formulas are given which express the labels of vertices $v \in V_S$ in terms of the labels of s. This makes it possible to recurrently construct the trees $\Gamma_1$, $\Gamma_2$, proceeding from a given collection of labels of the roots $w_1$, $w_2$ of the trees $\Gamma_1$, $\Gamma_2$.

c) The next object figuring in our arguments is a finite-dimensional vector space V of polynomials in the two variables x, y over a field $\mathbf{F}_q$ of degree no higher than $e = q^{4m}$:

$$V = \{p(x, y) \in \mathbf{F}_q[x, y] \mid \deg p(x, y) \leqslant e\}.$$

In the space V we consider the basis $\{\varphi_{a,b}\}$, $\varphi_{a,b} = x^a y^b$, $a = 0, 1, \ldots, e$; $b = 0, 1, \ldots, e-a$, and assume that some ordering of it is fixed: $\varphi_1, \ldots, \varphi_l$, $l = 1/2e(e+1)$. We need to consider the

collection of $\mathbf{F}_q$-linear functionals $\{A_{v,i}\}$ on V whose elements are numbered by pairs (v, i) where $v \in V'$ is a hanging vertex of $\tilde{\Gamma}$, i is an integer, $0 \leqslant i \leqslant q^{6m}$, and

$$A_{v,i}: V \to \mathbf{F}_q.$$

In part 3 formulas are given which provide expressions for the coefficients $\{a_{viab}\}$, $a_{viab} \in \mathbf{F}_q$ of the functionals $\{A_{vi}\}$ in the basis $\{\varphi_{ab}\}$.

d) We additionally need to consider the set of roots of the equation $F(x) = \sum_{k=0}^{m} a_k x^{(q^{2k}-1)/(q^2-1)} = 0$ and the action on them of the group $H = (A/I)^\times/F_q^\times$. The group H is cyclic; its generator is denoted by $\theta$. In part 4 an explicit expression is given for the action of $\theta$ on an element $\alpha \in R$. The basic definitions of L, $\tilde{\Gamma}$, $\{A_{v,i}\}$ and the action of H on R are given in Sec. 3 in terms of algebraic geometry. However, to understand how the algorithm proving the main theorem of this chapter works, it suffices to adopt the formulas of parts 2-4 as definitions.

2. Trees $\Gamma_1$, $\Gamma_2$. Let $s \in V_i \setminus V_i$ be a nonhanging vertex of $\tilde{\Gamma}_i$ labelled by the collection $(P_s(z_s, t_s), (\alpha_s, \beta_s), (Z_s, T_s), \Lambda_s)$. Then a) the set $V_s$ of descendents of the vertex s is in bijection with the set $M_s \cup I_s$ where

$$M_s = \{\beta \in L \mid \tilde{P}_s(0, \beta) = 0\}; \tag{1}$$

$\tilde{P}_s(y, t) \in \mathbf{F}_q[y, t]$ is defined by the equality

$$P_s(y + \alpha_s, yt + \beta_s) = y^{b_s} \cdot \tilde{P}_s(y, t) \tag{2}$$

and the condition $y \nmid \tilde{P}_s(y, t)$;

$$I_s = \begin{cases} \varnothing, & \text{if } \tilde{\tilde{P}}_s(0, 0) \neq 0, \\ \text{consists of one elment, if } \tilde{\tilde{P}}_s(0, 0) = 0; \end{cases} \tag{3}$$

the polynomial $\tilde{\tilde{P}}_s(y, t) \in \mathbf{F}_q[y, t]$ is defined by the equality

$$P_s(yt + \alpha_s, t + \beta_s) = t^{b'_s} \tilde{\tilde{P}}_s(y, t) \tag{4}$$

and the condition $t \nmid \tilde{\tilde{P}}_s(y, t)$. We further identify $V_s$ and $M_s \cup I_s$.

b) If $v \in V_s$, then for the label of v there are the formulas

$b_1$)

$$P_v(z_v, t_v) = \tilde{P}_s(z_v, t_v), \tag{5}$$

if $v \in M_s$;

$$P_v(z_v, t_v) = \tilde{\tilde{P}}_s(z_v, t_v), \quad \text{if} \quad v \in I_s; \tag{6}$$

$b_2$)

$$\alpha_v = 0, \ \beta_v \in M_s \subset \mathbf{F}_q \ \text{for} \ v \in M_s \tag{7}$$

$$\alpha_v = \beta_v = 0 \ \text{for} \ v \in I_s; \tag{8}$$

$b_3$)

$$Z_v(z_v, t_v) = \begin{cases} Z_s(z_v + \alpha_s, z_v t_v + \beta_s), & \text{if} \quad v \in M_s; \\ Z_s(z_v t_v + \alpha_s, t_v + \beta_s), & \text{if} \quad v \in I_s; \end{cases} \tag{9}$$

$$T_v(z_v, t_v) = \begin{cases} T_s(z_v + \alpha_s, z_v t_v + \beta_s), & \text{if} \quad v \in M_s; \\ T_s(z_v t_v + \alpha_s, t_v + \beta_s), & \text{if} \quad v \in I_s; \end{cases} \tag{10}$$

$b_4$)

$$\Lambda_v = \begin{cases} 0, & \text{if} \ \frac{\partial P_v}{\partial z_v}(\alpha_v, \beta_v) = \frac{\partial P_v}{\partial t_v}(\alpha_v, \beta_v) = 0; \\ 1, & \text{otherwise.} \end{cases} \tag{11}$$

*The proof follows immediately from the definition of $\tilde{\Gamma}_i$, the labels of its vertices, the description of the process of resolving singularities of $\tilde{X}_1$ by means of successive monoidal transformations, and the formulas giving the monoidal transformation $\sigma: F' \to F$ in local coordinates on F and F' (see [18, pp. 141-147], [15, p. 488]).*

COROLLARY. Let $d_v$ be the length of the path in $\tilde{\Gamma}_i$ going from the root $w_i$ to the vertex $v \in V_i'$. Then

a)

$$\left.\begin{matrix}\deg_{z_v} P_v \\ \deg_{t_v} P_v\end{matrix}\right\} \leqslant (d_v+1)(q^{2m}-1);$$

b)

$$\left.\begin{matrix}\deg_{z_v} Z_v \\ \deg_{t_v} Z_v \\ \deg_{z_v} T_v \\ \deg_{t_v} T_v\end{matrix}\right\} \leqslant (d_v+1).$$

3. Functionals $\{A_{v,i}\}$. Let $v \in V'$, $0 \leqslant i \leqslant q^{6m}$. The coefficients $\{a_{via b}\}$, $a = 0, 1, \ldots, e$, $b = 0, 1, \ldots, e-a$ of the linear form $A_{v,i}$ in the basis $\{x^a y^b\}$ of the space V can be computed by the formula

$$a_{vlab} = A_{v,i}(x^a y^b) = Q_l(Z_v(f_e(u_v)u_v+\beta_v)^a \cdot T_v(f_e(u_v), u_v+\beta_v)^{e-a-b}),$$

where $u_v = t_v - \beta_v$ and for a polynomial $p(u_v) \in F_q[u_v]$ $Q_i(p)$ denotes the coefficient of $u_v^i$, $Z_v$, $T_v$ are polynomials of the collection by which the vertex v is labeled, and

$$f_e(u_v) = PS(1, P_v, e) \in F_q[u_v], \tag{12}$$

where PS is the standard procedure described in part 6.6; by definition, $\deg f_e(u_v) \leqslant e$.

*There is a little less formal definition of $f_e(u_v)$:

$$f_e(u_v) = R_e(f_v(u_v)),$$

in the notation of part 3.18.

Proof. Formula (12) follows immediately from the definition of the functionals $\{A_{v,i}\}$ and the properties of the operators $Q_m$, $R_n$ (Lemma 3.17).*

4. Action of the Group H on the Set R. The order of the group $F_q^\times$, equal to $q-1$, is relatively prime to the order $h = (q^m-1)/(q-1)$ of the group H (since m and $q-1$ are relatively prime); therefore, in the group $(A/I)^\times$ there exists a unique subgroup H' of order h such that under the factorization mapping $(A/I)^\times \to H$ the subgroup H' is mapped isomorphically onto H. The elements of $(A/I)^\times$ can be represented as nonzero polynomials of degree no higher than $m-1$ considered modulo p(T).

Let $r(T) = \sum_{k=0}^{m-1} r_k T^k$ be a polynomial whose image in $(A/-I)^\times$ is a generator of the subgroup H' (and whose image in H is the generator $\theta$ of H). Then for the action of $\theta$ on an element $\alpha \in R$ there is the formula

$$\theta\alpha = \alpha \cdot \left(\sum_{k=0}^{m-1} r_k \alpha^{(q^{2k}-1)/(q^2-1)}\right)^{q^2-1}. \tag{13}$$

*Proof. This follows from the description of the "supersingular" points of $\tilde{X}_1$ given in parts 3.22-3.24 and Lemma 3.*

## 5. Computational Process

1. In this section we describe the computational process realizing the algorithm of constructing "modular" codes with the parameters indicated in the main theorem of Sec. 1, and we estimate its temporal and spatial complexity, thus obtaining a proof of that theorem. The computational process uses the formulas of Sec. 4 and is based on the standard procedures described below in Sec. 6. Each step of the computational process is described according to the following scheme: we indicate the information delivered to the input of each step, the information obtained as a result of its operation, the temporal T and spatial S complexity of the given step, and the method of computation (including a list of standard procedures needed to realize the computations at the given step); moreover, when it is not altogether obvious we present a proof of the fact that the resources T and S indicated are sufficient to carry out the computations at the given step. The computational method is described semiformally but in such a way that translation of the description into a programming language of sufficiently high level involves no difficulties.

The computational process used breaks down into eight steps. At the first step we construct an irreducible polynomial $p_I(T)$ of degree m which is the generator of an ideal I. At the second step we construct a polynomial r(T) whose image in the group H is a generator of it; at the third step we construct the trees $\Gamma_i$, including collections of labels of their vertices. At the fourth step we compute the coefficients of the functionals $\{A_{v,i}\}$. At step 5 we compute the collection of nonnegative integers $\{n_v\}$ numbered by elements $v \in V'$, $0 \leqslant n_v \leqslant q^{2m}$. The formulas used at step 5 can be taken as the definition of $n_v$ (*we recall that, rigorously speaking, $n_v$ is the order of the function t at the point $Q_v$; see part 3.20*). The sixth step is devoted to computing the basis in the $F_q$-space $V_b$,

$$V_b = \bigcap_{v \in V'} \bigcap_{l=0}^{(en_v - b)} \operatorname{Ker} A_{v,l},$$

$V_b \subset V = \{p(x, y) \in F_q[x, y] \mid \deg p \leqslant e = q^{4m}\}$. At the seventh step we construct the set S of representers of orbits of the action of H on R — the set of roots of $F(x) = \sum_{k=0}^{m} a_k x^{(q^{2k}-1)/(q^2-1)}$ — and the orbits themselves of this action. At the final and eighth step we construct the generating matrix M of the desired $q^2$-ic code C. As the base field over which computations in steps 1-6 and 8 are made we use the field $F_q$; at the seventh step we use the field $L = F_{q^{2h_1}}$.

2. Step 1. Construction of p(T). Input: $m \in Z_+$, m odd, $(m, q-1) = 1$.

Output: An irreducible polynomial of degree m over $F_q$:

$$p(T) = \sum_{k=0}^{m} a_k T^k, \quad a_i \in F_q, \quad a_m = 1.$$

Resources: $T = \mathcal{O}(q^m \cdot m^5 \cdot \log^5 q)$, $S = \mathcal{O}(m^3 \cdot \log^3 q)$.

Method: Sorting of all $q^m$ unitary polynomials of degree m, and verification of their irreducibility over $F_q$ by means of the procedure FAC(s, ·).

3. Step 2. Construction of the Generator in H. Input: $m \in Z_+$, $p(T) \in A = F_q[T]$.

Output: a) A polynomial $r(T) \in A$, $\deg r(T) \leqslant m-1$, such that the image of r(T) in H is a generator. b) Integers $h_1$, $h_2$, $h_1 = |G| = [L:F_{q^2}]$, $h_2 = [H:G]$, where G is the subgroup in H generated by the image of $T \in A$.

Resources: $T = \mathcal{O}(q^{2m} \cdot m^2 \cdot \log^2 q)$, $S = \mathcal{O}(m \log q)$.

Method: a) Sorting of all $(q^m - 1)$ elements of the standard set of representers $\{f(T) \in F_q[T] \setminus \{0\} \mid \deg f \leqslant m-1\}$ for $(A/I)^\times$ with verification of the order in H of each element. b) $h_2 = h/h_1$ where $h = (q^m - 1)/(q - 1)$ and $h_1$ is the order of the image of T in H.

4. Step 3. Construction of the Graph $\tilde{\Gamma}$. Input: The same as in step 2.

Output: Labeled trees $\tilde{\Gamma}_1$, $\tilde{\Gamma}_2$; $\tilde{\Gamma} = \tilde{\Gamma}_1 \cup \tilde{\Gamma}_2$.

Resources: $T = \mathcal{O}(q^{18m} \cdot m^3 \cdot \log^3 q)$, $S = \mathcal{O}(q^{18m} \cdot m^3 \cdot \log^3 q)$.

Method: Construction of $\tilde{\Gamma}_i$ is realized inductively, namely, we construct a subtree $\Gamma \subset \tilde{\Gamma}_i$ at the beginning of the process of constructing $\Gamma_i$, including collectionsthe root $w_i$ of the tree $\tilde{\Gamma}_i$ that is labeled by the collection

$$(F^*(z, t), (\alpha_i, \beta_i), (z - \alpha_i, t - \beta_i), 0),$$
$$(\alpha_1, \beta_1) = (0, 0), \quad (\alpha_2, \beta_2) = (-1, 0).$$

We suppose that the subtree $\Gamma \subset \tilde{\Gamma}_i$ has already been constructed. There are then two possible situations: a) For all hanging vertices $v \in V'_\Gamma$ of the tree $\Gamma$ we have $\Lambda_v = 1$. In this case $|V'_\Gamma| = |V'_i|$, the subtree $\Gamma$ coincides with $\tilde{\Gamma}_i$, and the construction is finished. b) There exists a hanging vertex $v \in V'_\Gamma$ of the tree $\Gamma$ such that $\Lambda_v = 0$. In this case the inductive construction of $\Gamma$ by means of the formulas of part 4.2 continues.

1°. We set $V'_\Gamma = (V'_\Gamma \setminus \{v\}) \cup (M_v \cup I_v)$, $V_\Gamma = V_\Gamma \cup (M_v \cup I_v)$.

2°. The labels of the vertices $u \in M_v \cup I_v$ are computed by formulas (4.3)-(4.11) using the procedures SUBST, SR, ROOT.

*Estimate of resources: According to Lemma 3.13, for the number of vertices $v_i$ of the tree $\tilde{\Gamma}_i$ there is the inequality $v_1 + v_2 < q^{4m}$; an estimate of the resources required in working with an individual vertex is obtained from the estimates of complexity of the procedures SUBST, SR, ROOT given in Sec. 6 and the estimates of the degrees of the polynomials $P_v$, $Z_v$, $T_v$ given in part 4.2.*

5. Step 4. Computation of the Coefficients of the Functionals $A_{v,i}$. Input: Choice of labels $(P_v(z_v, t_v), (\alpha_v, \beta_v), (Z_v, T_v), \Lambda_v)$ for each hanging vertex $v \in V'$ of the graph $\tilde{\Gamma}$.

Output: Collection of coefficients $\{a_{viab}\}$, $a, b = 0, 1, \ldots, e = q^{4m}$, $a+b \leqslant e$ of linear forms $\{A_{v,i}\}$, $i = 1, \ldots, q^{6m}$, $v \in V'$ in the basis $\{x^a y^b\}$ of the space $V$, $a_{viab} \in \mathbf{F}_q$.

Resources: $T = \mathcal{O}(q^{32m} \cdot m^2 \cdot \log^2 q)$, $S = \mathcal{O}(q^{20m} \cdot m^2 \cdot \log^2 q)$.

Method: For $v \in V'$ we set

$$u_v = t_v - \beta_v;$$
$$f_e(u_v) := PS(s, P_v, e) \in \mathbf{F}_q[u_v];$$
$$P := SUBST(s, Z_v, f_e(u_v), u_v + \beta_v) \in \mathbf{F}_q[u_v];$$
$$Q := SUBST(s, T_v, f_e(u_v), u_v + \beta_v) \in \mathbf{F}_q[u_v];$$
$$a_{viab} := Q_i(SUBST(s, X_1^a X_2^{e-a-b}, P, Q) \in \mathbf{F}_q.$$

6. Step 5. Computation of the Collection $\{n_v\}$. Input: The same as in step 4.

Output: The collection $\{n_v\}$, $v \in V'$, $0 \leqslant n_v \leqslant q^{2m}$, $*n_v$ is the order of the function t at $Q_v \in X$.*

Resources: $T = \mathcal{O}(q^{24m} \cdot m^2 \cdot \log^2 q)$, $S = \mathcal{O}(q^{16m} \cdot m^2 \cdot \log^2 q)$.

Method: For $v \in V'$ we set

$$u_v := t_v - \beta_v;$$
$$f_{q^{2m}}(u_v) := PS(s, P_v, q^{2m}) \in \mathbf{F}_q[u_v];$$
$$F_v := SUBST(s, T_v, u_v + \beta_v, f_{q^{2m}}(u_v)) \in \mathbf{F}_q[u_v];$$
$$n_v := \min\{n \in \mathbf{Z}_+ \mid Q_n(F_v) \neq 0\}.$$

7. Step 6. Finding a Basis in $V_b$. Input: The collection $\{n_v\}$, $v \in V'$, and the collection of coefficients $\{a_{viab}\}$, $v \in V'$, $i = 0, \ldots, q^{6m}$, $a = 0, 1, \ldots, l$, $b = 0, 1, \ldots, l - a$, of linear forms $\{A_{v,i}\}$; an integer $b > 0$.

Output: The collection $\{p_r\}$, $r = 1, \ldots, \dim V_b$ of basis polynomials in the subspace $V_b \subset V$.

Resources: $T = \mathcal{O}(q^{28m} \cdot m^2 \cdot \log^2 q)$, $S = \mathcal{O}(q^{18m} \cdot m^2 \cdot \log^2 q)$.

Method: Application of LEQ(s, M).

8. Step 7. Construction of the Set of Orbits of the Action of H on R. Input: $p(T)$, $r(T) \in A = \mathbf{F}_q[T]$.

Output: a) The set $S \subset L$ of representers of the orbits of the action of the group H on the set R of roots of the polynomial $F(x) = \sum_{k=0}^{m} a_k x^{(q^{2k}-1)/(q^s-1)}$. b) For each $\sigma \in S$ a list of elements $R_\sigma \subset R$ lying in one $\sigma$ orbit.

Resources: $T = \mathcal{O}(q^{8(m+2)})$, $S = \mathcal{O}(q^{4(m+2)})$.

Method: a) We set $(P_1, \ldots, P_{nh_2}) := FAC(2s, F)$, where $q = p^s$, $n = (q^m + 1)/(q + 1)$ (*the fact that $nh_2$ factors are obtained is proved in Lemma 3.24*), $\deg P_j = h_1$, $j = 1, \ldots, nh_2$. For $j = 1, \ldots, nh_2$ we set

$$\Lambda_j = \{\alpha_{1j}, \ldots, \alpha_{h_1 j}\} := ROOT(2s, P_j), \quad \alpha_{ij} \in L.$$

We order the collection $\{P_1, \ldots, P_j, \ldots, P_{nh_2}\}$ so that $\forall i, \forall j$, $i = 1, \ldots, h_1$, $j = 1, \ldots, nh_2$ the following relation holds:

$$\theta\alpha_{1j} = \alpha_{ij}\left(\sum_{k=0}^{m-1} r_k \alpha_{1j}^{(q^{2k}-1)/(q^s-1)}\right)^{q^s-1} \in \Lambda_j \cup \Lambda_{j+1}$$

(i.e., in order by the action of the generator θ of the group H on an element $\alpha_{ij} \in \Lambda_j$ to obtain an element of $\Lambda_j$ or an element of $\Lambda_{j+1}$; *see the description of the orbits of the action of H on R given in part 3.24*). Further, we set

$$S := \{\alpha_{1h_2}, \alpha_{1,2h_2}, \ldots, \alpha_{1,nh_2}\}.$$

b) For $\sigma = \alpha_{1,kh_2} \in S$ we set

$$R_\sigma := \{\alpha_{i,kh_2+j}\}, \quad i = 1, \ldots, h_1, \quad j = 1, \ldots, h_2.$$

9. Step 8. Construction of the Generating Matrix of the Code. Input: The set S = R/H; the collection $\{R_\sigma\}$, $\sigma \in S$; the collection of basis polynomials $\{p_r\}$ in the space $V_b$.

Output: The generating matrix $M = M_{m,b}$ of the code $C = C_{m,b}$,

$$M \in \mathrm{Mat}(k \times n, F_{q^s}), \quad n = (q^m+1)/(q+1), \quad k \geqslant b-g+1.$$

Resources: $T = \mathcal{O}(q^{17m} \cdot \log^2 q)$, $S = \mathcal{O}(q^{10m} \cdot \log q)$.

Method: We construct the matrix

$$M' \in \mathrm{Mat}((\dim V_b) \times n, F_{q^s});$$

$$M' = (m_{rk}), \quad r = 1, \ldots, \dim V_b, \quad k = 1, \ldots, n;$$

$$m_{rk} := \sum_{\alpha \in R_\sigma} p_r(\alpha, 0) = \sum_{i=1}^{h_1} \sum_{j=1}^{h_2} p_r(\alpha_{i,(k-1)h_2+j}, 0);$$

where $\sigma \in S$ in the first sum corresponds to the k-th element of S.

The matrix M is obtained from M' by deleting rows which are linear combinations of other rows (this is done, for example, by the Gauss method).

At step 8 the algorithm finishes its work. Figure 1 shows the scheme of logical dependence of the steps of the algorithm.

## 6. Standard Procedures

1. In the present section we give a brief description of the standard procedures used in the computational process of Sec. 5 (one of them — PS — figures also in part 4.3). As a model of the computing process we choose LRAM, i.e., an equiaccess address machine (a machine with arbitrary access to memory) with a logarithmic bound on the length of cells; a description of this model of computations is contained, for example, in the survey [14]. Estimates of the complexity of procedures are given for LRAM. We hereby do not strive to use algorithms with the best known estimates, and in the presence of alternatives we choose an algorithm with the simpler structure under the condition that it has a polynomial estimate of complexity (in the sense we require). It can be verified that use of the best known algorithms with preservation of the general scheme of the computing process does not lead to basic improvement of the estimates in our main theorem. Below we use the word "algorithm" as a synonym for the acronym "LRAM".

The choice of LRAM as the basic computational model is to considerable extent arbitrary and is dictated by convenience considerations. The basic result of this chapter on the possibility of a polynomial computational process for "modular" codes is preserved for any

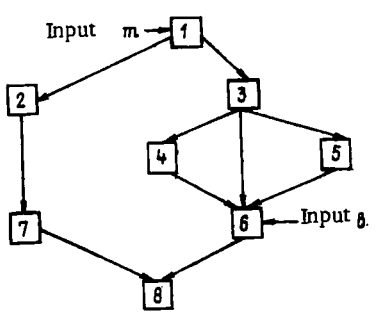


Fig. 1. Scheme of logical dependence of the steps of the algorithm.

reasonable computational model, for example, for a Turing machine MT, since for any computation on LRAM with time complexity T there exists a modelling of it on MT with complexity $\mathcal{O}(T^2\log^3 T)$ (see, for example, [1, Sec. 1.6]).

The procedure is described according to the following scheme: name of procedure, NAME, input data, output data, method of operation, estimate of time T (NAME) and space S (NAME) complexity in the computational model we adopt. A description of the method of operation of the procedure is presented only in the case where this procedure is not described (or its description requires essential modification) in [1] or the survey [14]. Moreover, we shall not present descriptions of the obvious procedures of the type of arithmetic actions on elements of finite fields and on polynomials over finite fields. The only thing we can reasonably say in this regard consists in the form in which we give the elements of finite fields.

2. Representation of Constants. By constants we mean elements of a fixed finite field $F_{p^a}$ (in our case such a field can be taken to be the field $F_{q^h}$, $h = (q^m - 1)/(q - 1)$, $a = hs$). We call such a field a collection of structural coefficients $\{c_{ijk}\}$, $i, j, k = 1, \ldots, a$, $c_{ijk} \in F_p$, for some basis $\{\alpha_1, \ldots, \alpha_a\}$ of the field $F_{p^a}$ over $F_p$:

$$\alpha_i \cdot \alpha_j = \sum_{k=1}^{a} c_{ijk} \cdot \alpha_k.$$

Generally speaking, we must go over to extensions within the field $F_{p^a}$ of fields of the form $F_{p^b}$ where $b/a$.

3. Passage to an Extension. To describe passage from a field $F_{p^b}$ to a field $F_{p^r}$, $b/r$, we introduce the following procedure.

Extension of finite fields: EXTFF(b, F).

Input: $b \in \mathbf{Z}_+$, a unitary irreducible polynomial $F \in F_{p^b}[X]$, deg F = s.

Output: a collection of structural constants $\{d_{ijk}\}$ of the field $F_{p^r}$, $r = bs$, $i, j, k = 1, \ldots, r$.

Method: we note first of all that since the field $F_{p^b}$ enters in the input of the procedure, we are given a collection of its structural constants $\{c_{ijk}\}$, $i, j, k = 1, \ldots, b$ in some basis $\{\alpha_1, \ldots, \alpha_b\}$ over $F_p$. As a basis of $F_{p^r}$ over $F_p$ we choose $\{\alpha_i \cdot \beta^j\}$, $i = 1, \ldots, b$, $j = 0, \ldots, s - 1$; $\beta$ is a root of F; $F(\beta) = \beta^s + a_{s-1}\beta^{s-1} + \ldots + a_0 = 0$, $a_i \in F_{p^b}$, $i = 0, \ldots, s - 1$.

First we inductively compute $\beta^s, \ldots, \beta^{2s-2}$: if

$$\beta^{s+j} = a_{0,j} + \ldots + a_{s-1,j}\beta^{s-1}, \quad j = 0, \ldots, s-2,$$

then

$$\beta^{s+j+1} = -(a_0 + \ldots + a_{s-1}\beta^{s-1})\, a_{s-1,j} + a_{0,j}\beta + \ldots + a_{s-2,j}\beta^{(s-1)},$$

whereby for $j = 0$, $a_{i,j} = a_i$, $i = 0, \ldots, s - 1$. We further compute the products $\{\alpha_i\beta^j \cdot \alpha_l\beta^k\}$:

$$\alpha_i\beta^j\alpha_l\beta^k = \begin{cases} \left(\sum_{t=1}^{m} c_{ilt}\alpha_t\right)\left(\sum_{u=0}^{s-1} a_{u,k+j-s}\beta^u\right) & \text{for } k+j \geqslant s; \\ \left(\sum_{t=1}^{m} c_{ilt}\alpha_t\right)\beta^{k+j} & \text{for } k+j < s. \end{cases}$$

Complexity:

$$T(EXTFF) = \mathcal{O}(b^3 s^3 l(p)^2); \quad S(EXTFF) = \mathcal{O}(b^3 s^3 l(p)).$$

Here and below $l(n)$ for $n \in \mathbf{Z}_+$ denotes $[\log_2(n)] + 1$.

4. Solution of the System of Linear Equations. Linear system: LEQ(b, M).

Input: $b \in \mathbf{Z}_+$, $M \in \mathrm{Mat}(s \times n, F_{p^b})$.

Output: a basis in the space of solutions of the system of linear equations Mx = 0, $x \in (\mathbf{F}_{p^b})^n$.

Complexity:

$$T(LEQ)=O(s^2nb^2l(p)^2);\quad S(LEQ)=O(snbl(p)).$$

5. Operations on Polynomials. Aside from the procedures of arithmetic actions and the Euclidean algorithm, we need also four procedures defining the actions with polynomials.

Substitution: SUBST(b, P, $Q_1$, $Q_2$).

Input: $b\in\mathbf{Z}_+$, $P\in\mathbf{F}_{p^b}[X_1, X_2]$, $Q_1$, $Q_2\in\mathbf{F}_{p^b}[X]$.

Output: $Q=P(Q_1(X), Q_2(X))\in\mathbf{F}_{p^b}[X]$.

Complexity: $T(SUBST)=O(s^2r^4b^2l(p)^2)$, $S(SUBST)=O(s^2r^2bl(p))$, where s = deg P, r = max (deg $Q_1$, deg $Q_2$).

Finding roots: ROOT($a$, P).

Input: $b\in\mathbf{Z}_+$, an irreducible polynomial $P\in\mathbf{F}_{p^b}[X]$.

Output: a collection $\{\beta_1, \ldots, \beta_s\}$ of roots of P in $\mathbf{F}_{p^{bs}}$, where s = deg P.

Method: use of EXTFF(b, P), finding $\{\beta^{p^i}\}$ i = 1, ..., s − 1, where $P(\beta) = 0$.

Complexity: $T(ROOT)=O(p\cdot s\cdot b^2\cdot l(p)^2+b^3\cdot s^3\cdot l(p)^2)$; $S(ROOT)=O(b^3\cdot s^3\cdot l(p))$.

Elimination of multiple roots: SR(b, P).

Input: $b\in\mathbf{Z}_+$, $P\in\mathbf{F}_{p^m}[X]$, $\deg P=s$.

Output: R = HOD(P, $P_X$), $P_X = \partial P/\partial X$.

Complexity: $T(SR)=O(s^3\cdot b^3\cdot l(p)^2)$; $S(SR)=O(sbl(p))$.

Expansion: FAC(b, P).

Input: $b\in\mathbf{Z}_+$, $P\in\mathbf{F}_{p^b}[X]$, P has no multiple roots, deg P = s.

Output: the collection ($P_1$, ..., $P_t$) of factors of P, $P_i\in\mathbf{F}_{p^b}[X]$, irreducible over $\mathbf{F}_{p^b}$.

Method: Let $\varphi$ be an $\mathbf{F}_p$-linear Frobenius operator in the semisimple algebra $R=\mathbf{F}_{p^b}[X]/(P)$, $\varphi:\sum a_iX^i \bmod P \mapsto \sum a_i^pX^{ip} \bmod P$. We first find the matrix $M_\varphi\in\mathrm{Mat}(r\times r, \mathbf{F}_p)$, r = bs, of the action of $\varphi$ in the basis $\{\alpha_iX^j \bmod P\}$, $i=1, \ldots, b$, $j=0, \ldots, s-1$, of the algebra R over $\mathbf{F}_p$, where $\{\alpha_i\}$ is a basis of $\mathbf{F}_{p^b}$ over $\mathbf{F}_p$. For this it suffices to compute $\{\alpha_i^p\}$, $i=1, \ldots, b$; $\{X^{jp} \bmod P\}$, j = 0, ..., s − 1, as done in part 3 in describing the procedure EXTFF and then compute $\{\alpha_i^pX^{jp}\}$ which gives the matrix M. Applying now the procedure LEQ(1, $M\varphi - I_r$), where $I_r\in\mathrm{Mat}(r\times r, \mathbf{F}_p)$ is the identity matrix, we find a basis in the $\mathbf{F}_p$-space $R^\varphi$ of elements of R invariant under $\varphi$. Let $r_1$, $r_2$ be two linearly independent (over $\mathbf{F}_p$) elements of $R^\varphi$ (if none such exist, then P is irreducible and t = 1). By sorting elements $f\in\mathbf{F}_p^\times$, we find f such that $a$ + fb is a zero divisor in the algebra $R^\varphi$ (in order that $a$ + fb be a zero divisor it suffices to require that the determinant of the matrix of multiplication by ($a$ + fb) in $R^\varphi$ vanish). A polynomial H(X) such that deg H < deg P and H(X) mod P = $a$ + fb has as a factor a nontrivial divisor of P(X). We then continue to act by induction on the degree of P(X)/G(X) where

$$G(X)=\mathrm{HOD}(P(X), H(X)).$$

Complexity:

$$T(FAC)=O(s^3b^5\cdot l(p)^2+p\cdot s^4\cdot l(p)^2);\qquad S(FAC)=O(s^2\cdot b^3\cdot l(p)).$$

We also need one specific simple procedure which, as far as we know, is not described in the literature (we have in mind its description as a procedure rather than as a method of computation which is well known).

6. Expansion in Power Series.

Power series: PS(b, P, d).

Input: $b, d \in \mathbf{Z}_+$, an absolutely irreducible polynomial $P(X, Y) \in \mathbf{F}_{p^b}[X, Y]$ such that $P(0, 0) = 0$, $P_Y(0, 0) \neq 0$, $s = \deg P$.

Output: a segment $f_d \in \mathbf{F}_{p^b}[X]$, $\deg f_d \leqslant d$, of length d of the power series of f obtained by expanding Y in powers of X if X and Y are connected by the relation $P(X, Y) = 0$.

Method: recurrent computation of the polynomials $f_1, \ldots, f_d$, where

$$f_1 = -a_{10} \cdot a^{-1} X;$$

$$f_{j+1} = f_j - a^{-1} \cdot X^{j+1} \cdot Q_{j+1}(P(X, f_j) - a \cdot f_j);$$

$$j = 1, \ldots, d-1;$$

$$P(X, Y) = \sum_{i,j=0}^{s} a_{ij} X^i Y^j;$$

$$a_{00} = 0, \quad a = a_{10} = P_Y(0, 0) \neq 0.$$

Complexity:

$$T(PS) = \mathcal{O}(s^2 d^4 b^2 l(p)^2); \qquad S(PS) = \mathcal{O}(s^2 d^2 b^2 \cdot l(p)).$$

LITERATURE CITED


1. A. Aho and H. Hopcroft, The Design and Analysis of Computer Algorithms, Addison-Wesley (1974).
2. L. A. Bessalygo, V. V. Zyablov, and M. S. Pinsker, "Problems of complexity in the theory of correcting codes," Prob. Peredachi Inf., 13, No. 3, 5-17 (1977).
3. É. L. Blokh and V. V. Zyablov, Linear Cascade Codes [in Russian], Svyaz', Moscow (1982).
4. S. G. Vlěduts, "Modular curves and codes with polynomial complexity of construction," Preprint No. 3302-83 (1983).
5. S. G. Vlěduts and V. G. Drinfel'd, "On the number of points of an algebraic curve," Funkts. Anal., 17, No. 1, 68-69 (1983).
6. S. G. Vlěduts, G. L. Katsman, and M. A. Tsfasman, "Modular curves and codes with polynomial complexity of construction," Probl. Peredachi Inf., 20, No. 1, 3-15 (1984).
7. V. D. Goppa, "Codes on algebraic curves," Dokl. Akad. Nauk SSSR, 259, No. 6, 1289-1290 (1981).
8. V. D. Goppa, "Algebraicogeometric codes," Izv. Akad. Nauk SSSR, Ser. Mat., 46, No. 4, 762-781 (1982).
9. P. Griffiths and J. Harris, Principles of Algebraic Geometry [Russian translation], Vols. 1, 2, Mir, Moscow (1982).
10. V. G. Drinfel'd, "Elliptic modules," Mat. Sb., 94, No. 4, 594-627 (1974).
11. T. Kasami, N. Tokura, E. Ivadari, and Ya. Inagaki, Coding Theory [Russian translation], Mir, Moscow (1978).
12. F. J. MacWilliams and N. J. A. Sloan, The Theory of Codes Correcting Errors [Russian translation], Svyaz', Moscow (1979).
13. J. P. Serre, Algebraic Groups and Class Fields [Russian translation], Mir, Moscow (1959).
14. A. O. Slisenko, "Complexity problems in the theory of computations," Usp. Mat. Nauk, 36, No. 6, 22-103 (1981).
15. R. Hartshorn, Algebraic Geometry [Russian translation], Mir, Moscow (1981).
16. M. A. Tsfasman, "Goppa codes lying above the Varshamov-Gilbert boundary," Probl. Peredachi Inf., 18, No. 3, 3-6 (1982).
17. N. G. Chebotarev, Introduction to the Theory of Algebraic Functions [in Russian], OGIZ, Moscow (1948).
18. I. R. Shafarevich, Foundations of Algebraic Geometry [in Russian], Nauka, Moscow (1972).
19. G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions [Russian translation], Mir, Moscow (1973).
20. D. Goss, "The algebraist's upper half plane," Bull. Am. Math. Soc., 2, No. 3, 391-415 (1980).
21. D. Goss, "$\pi$-adic Eisenstein series for function fields," Compos. Math., 41, No. 1, 3-38 (1980).
22. Y. Ihara, "Some remarks on the number of rational points of algebraic curves over finite fields," J. Fac. Sci. Univ. Tokyo, Sec. IA, 28, No. 3, 721-724 (1982).

23. Y. Ihara, "On the problems of congruence monodromy," J. Math. Soc. Jpn., 20, No. 1-2, 107-121 (1968).
24. Y. Ihara, "On modular curves over finite fields," Discrete Subgroups, Lie Groups, and Appl. Moduli, Papers, Bombay, Colloq. (1973), Oxford, e.a. (1975), pp. 160-202.
25. G. L. Katsman, M. A. Tsfasman, and S. G. Vladut, "Modular curves and codes of polynomial construction," IEEE Trans. Inf. Theory, 1984 (in press).
26. Yu. I. Manin, "What is the maximal number of points on a curve over $F_2$?" J. Fac. Sci. Univ. Tokyo, Sec. 1A, 28, No. 3, 715-720 (1981).
27. J. P. Serre, "Sur le nombre des points rationnels d'une courbe algebrique sur un corps fini," C. R. Acad. Sci., Ser. 1, 296, 397-402 (1983).
28. M. A. Tsfasman, S. G. Vladut, and Th. Zink, "Modular curves, Shimura curves, and Goppa codes better than the Varshamov-Gilbert bound," Math. Nachr., 109, 21-28 (1982).