Discrete Applied Mathematics 33 (1991) 241-256
North-Holland

Algebraic-geometric codes and asymptotic problems

Michael A. Tsfasman

26-2-433 Akad. Piljugina st., Moscow 117393, USSR

Received 29 June 1989
Revised 12 January 1990

Abstract

Tsfasman, M.A., Algebraic-geometric codes and asymptotic problems, Discrete Applied Mathematics 33 (1991) 241-256.

This is an attempt to analyze the present state of affairs concerning asymptotic bounds in coding theory. The advantages of algebraic-geometric approach to codes are most illustrious when we consider asymptotic problems. Here we try to show how to put different asymptotic problems, what is known about their solutions, and how algebraic-geometric codes influence the situation.

Introduction

Algebraic-geometric constructions of error-correcting codes have considerably changed and entangled the picture of lower asymptotic bounds. In this paper we try to survey and analyze the present situation. Doing this we avoid proofs, but try to expose principal ideas.

We start (in Section 1) with a discussion of possible asymptotic problems, posing them rigorously. Then (in Section 2) we briefly look at upper bounds, and (in Section 3) at those lower bounds which have nothing to do with algebraic geometry. After that (in Section 4) we introduce algebraic-geometric codes (AG-codes) and discuss their properties. Section 5 is devoted to lower bounds exploiting AG-codes. We finish with diagrams, exposing the relations between various bounds, and with some numerical data.

While writing this text I borrowed greatly from our just finished book [18] written jointly with S. Vlădut, to whom I am deeply grateful.

1. Asymptotic problems

Codes. Let A be a fixed set, $q = \#A \geq 2$. On $A^n = A \cdot \cdots \cdot A$ there is a Hamming metric

$$d(a,b) = \#\{i \mid a_i \neq b_i\},$$

where $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$.

A *q-ary* code is a subset $C \subseteq A^n$; n is its *length*, $k = \log_q(\#C)$ is its *log-cardinality*, $d = \min\{d(a,b) \mid a,b \in C,\ a_i \neq b_i\}$ is its *minimum distance*. Such a code is called an $[n,k,d]_q$-code. Further on we discuss families of such codes with $n \to \infty$, and use relative parameters $R = k/n$ called the *rate* and $\delta = d/n$ called the *relative distance*; it is obvious that $0 \leq R \leq 1$, $0 \leq \delta \leq 1$.

Now let us suppose that $q = p^a$ is a power of a prime, and fix some identification $A \simeq \mathbb{F}_q$, $\mathbb{F}_q$ being a finite field. A code $C \subseteq \mathbb{F}_q^n$ is called *linear* iff it is a linear subspace. For a linear code, $d = \min\{\|a\| \mid a \in C,\ a \neq 0\}$, the Hamming norm $\|a\|$ being defined as the number of nonzero coordinates.

One of the main problems of coding theory is to describe the set of triples (n,k,d) for which there exist $[n,k,d]_q$-codes (and also to construct these codes explicitly). Here we discuss this problem for $n \to \infty$.

The main asymptotic problem. The asymptotic problem that looks most important is to understand the relations between the possible limit values of δ and R when not only n, but also k and d tend to infinity.

Define $V_q \subset [0,1]^2$ as a set of pairs (δ, R) for all possible q-ary codes, and let U_q be the set of its limit points, i.e., $(\delta_0, R_0) \in U_q$ iff there exists a sequence of such codes C_i of length $n_i \to \infty$ such that their parameters $(\delta_i, R_i) \to (\delta_0, R_0)$. If $\delta_0 > 0$ and $R_0 > 0$ we call such a sequence (a family) of codes *asymptotically good* (or just *good*). For $q = p^a$ and $A = \mathbb{F}_q$ let V_q^{lin} and U_q^{lin} be the corresponding notions for linear codes.

The following simple but important result is due to Manin [10] and Aaltonen [1].

Theorem 1. *There exists a continuous function* $\alpha_q(\delta)$, $\delta \in [0,1]$, *such that*

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

We have $\alpha_q(0) = 1$, $\alpha_q(\delta) = 0$ *for* $(q-1)/q \leq \delta \leq 1$, *and* $\alpha_q(\delta)$ *is decreasing on the segment* $[0,(q-1)/q]$. *If* $q = p^a$, *the same is valid for* U_q^{lin} *and* α_q^{lin} (*of course*, $\alpha_q(\delta) \geq \alpha_q^{\text{lin}}(\delta)$).

The proof is based on the fact that any $[n,k,d]_q$-code can be "spoiled" in two different ways so as to give an $[n-1,k-1,d]_q$-code and an $[n-1,k,d-1]_q$-code.

As yet we are rather far from any precise knowledge of $\alpha_q(\delta)$ and $\alpha_q^{\text{lin}}(\delta)$ for $0 < \delta < (q-1)/q$. We do not know whether they are concave (though it seems plausible), or not. Neither we know whether they are differentiable, nor whether $\alpha_q(\delta) = \alpha_q^{\text{lin}}(\delta)$, or not.

Polynomial problems. It is difficult to explain what we mean by saying that we know an *explicit* construction of a code. When $n \to \infty$ it is possible to give rigorous definitions.

We say that a family of codes C_i with $n_i \to \infty$ is *polynomial* iff there exist algorithms generating our codes C_i whose complexity is polynomial in n (we say that an algorithm generates an $[n,k,d]_q$-code C if as a result it gives us a polynomial algorithm of coding $\mathcal{U}: M \xrightarrow{\sim} C$, M being a fixed set of cardinality q^k, say $M=[1,2,\ldots,q^k]$; for a linear code such an algorithm $\mathcal{U}$ is given, for example, by a generator matrix $G: \mathbb{F}_q^k \to \mathbb{F}_q^n$, $C=\operatorname{Im} G$). The notion of polynomiality is well defined, and we can set U_q^{pol} and $U_q^{\text{pol lin}}$ to be the sets of limit points (δ,R) for polynomial families of codes (respectively, of linear codes).

There is an obvious analogue of Theorem 1 (see, e.g. [23]):

Theorem 2. *All the statements of Theorem* 1 *are valid for* U_q^{pol} *and* $U_q^{\text{pol lin}}$ *(instead of* U_q *and* U_q^{lin}*). We have* $\alpha_q(\delta) \geq \alpha_q^{\text{pol}}(\delta) \geq \alpha_q^{\text{pol lin}}(\delta)$ *and* $\alpha_q(\delta) \geq \alpha_q^{\text{lin}}(\delta) \geq \alpha_q^{\text{pol lin}}(\delta)$.

Again we do not know whether $\alpha_q(\delta)=\alpha_q^{\text{pol}}(\delta)$, $\alpha_q^{\text{lin}}(\delta)=\alpha_q^{\text{pol lin}}(\delta)$, or not.

Relations for different q's. Though we know little about functions $\alpha_q^*(\delta)$ (here * stands for lin, pol, pol lin, or for nothing), we can relate these functions with one another for different q's. The scheme is quite simple. Suppose that for any $[n,k,d]_q$-code C by some operation or other we can construct another $[n',k',d']_{q'}$-code C' and write its parameters in terms of that for C, then we can relate α_q and $\alpha_{q'}$. If the operation is polynomial in n, then we can relate α_q^{pol} and α_q^{pol}. If it preserves the linear structure, then we can add lin.

The following statement is taken from [8].

Theorem 3. $\alpha_q(\delta) \geq \max\{\max_{q' \geq q}\{1-(1-\alpha_{q'}(\delta))\cdot \log_q q',\ \max_{q' \leq q}\{\alpha_{q'}(\delta)\cdot \log_{q'} q'\}\}$.

The proof is based on the one hand on the reduction of alphabet (identify $A' \simeq \mathbb{Z}/q'$, let $A \subseteq A'$, consider all possible shifts of $C \subseteq (A')^n$ and their intersection with A^n, and take "the best one"), and on the other hand on the extension of alphabet (for $A' \subseteq A$, a q'-ary code $C \subseteq (A')^n \subseteq A^n$ can be considered as a q-ary code). These operations are not linear, but the second one is polynomial when $q'=q^2$ yields

Theorem 4. $\alpha_q^{\text{pol}}(\delta) \geq \max_{q' \leq q}\{\alpha_{q'}^{\text{pol}}(\delta)\cdot \log_q q'\}$.

Here is another result, taken from [23]:

Theorem 5. $\alpha_q^{\text{pol}}(\delta) \geq \max_C\{(k/n)\cdot \alpha_{q^k}^{\text{pol}}((d/n)\cdot\delta)\}$, *where* max *is taken over all* q*-ary codes* C ($[n,k,d]_q$ *being the parameters of* C*). The same is valid for* α_q*, and if* $q=p^a$ *then the same is valid also for* α_q^{lin} *and* $\alpha_q^{\text{pol lin}}$.

The proof is based on a very useful operation, called concatenation. In the case of linear codes it can be described as follows. For an $[n,k,d]_q$-code C and an $[N,K,D]_{q^k}$-code C' a new code is given by the composition of maps

$$\mathbb{F}_q^{Kk} \simeq \mathbb{F}_{q^k}^K \xrightarrow{C'} \mathbb{F}_{q^k}^K \simeq (\mathbb{F}_q^k)^N \xrightarrow{(C,\dots,C)} \mathbb{F}_q^{nN},$$

its parameters being $[Nn, Kk, \geq Dd]_q$.

We can also use reduction to a subfield to get a linear version of the first part of Theorem 3. Note that in the case of $A=\mathbb{F}_q \subset \mathbb{F}_{q^m}=A'$ we do not need to consider all shifts and the operation is in fact polynomial:

Theorem 6. $\alpha_q^{\text{pol lin}}(\delta) \geq \max_m \{1-m\cdot(1-\alpha_{q^m}^{\text{pol lin}}(\delta))\}$, max *being taken over all* $m\in\mathbb{Z}$, $m\geq 1$. *The same is valid for* α_q^{lin}.

Relations for a fixed q. We end this section with the following recent result due to Litsyn and Zinoviev [9] which summarizes different methods used to establish upper bounds.

Theorem 7. $\alpha_q(\delta) \leq \min_{\tau,\gamma} \{\tau + (1-\tau)\cdot\alpha_q(\delta') - \tau\cdot H_q(\gamma/\tau)\}$, *where* min *is taken over* $0\leq\tau\leq 1$, $0\leq\gamma\leq 1$, $\gamma\leq\delta/2$, *and*

$$\delta' = \begin{cases} (\delta-2\gamma)/(1-\tau) & \text{for } \gamma\leq\tau/2, \\ (\delta-\tau)/(1-\tau) & \text{for } \gamma\geq\tau/2. \end{cases}$$

Here $H_q(x) = x\cdot\log_q(q-1) - x\cdot\log_q x - (1-x)\cdot\log_q(1-x)$ is the q-ary entropy function.

Self-dual codes. A linear code $C\subseteq\mathbb{F}_q^n$ is called self-dual iff $k=n/2$ and $\sum a_i b_i = 0$ for any $a,b\in C$. It is called quasi-self-dual iff $k=n/2$ and there exists $y\in(\mathbb{F}_q^*)^n$ such that $\sum y_i a_i b_i = 0$ for any $a,b\in C$. For a (quasi-)self-dual code $R=1/2$. Set

$$\delta_q^{\text{qsd}} = \limsup \delta(C),$$

the limit being taken over all quasi-self-dual codes C. If we consider only self-dual codes we define δ_q^{sd}.

Constant-weight codes. Consider nonlinear codes $C\subset A^n$ such that all Hamming weights are equal: $\|a\| = w$ for any $a\in C$, w being fixed. Let $\omega = w/n$, $n\to\infty$. It is possible to define $\alpha_q(\psi,\delta)$ in the same way as $\alpha_q(\delta)$.

Other asymptotics. There are several natural asymptotics different from the main one.

First fix d and let $n\to\infty$. Set

$$\kappa_q(d) = \liminf\left(\frac{n-k}{\log_q n}\right),$$

the limit being taken over all $[n, k, d]_q$-codes for given q and d. Its analogue for linear codes is denoted $\kappa_q^{\text{lin}}(d)$.

Another way round, fix k and let $n \to \infty$. Set

$$\delta_q(k) = \limsup \frac{d}{n},$$

the limit being taken over all $[n, k, d]_q$-codes for given q and k. For linear codes we get another function $\delta_q^{\text{lin}}(k)$ (in fact, these functions are known and equal).

Now let $\varphi(n)$ be an increasing function such that $\varphi(n)/n \to 0$. We can set

$$\varrho_\varphi(n) = \inf(n-k),$$

inf being taken over all $[n, k, d]_q$-codes with given n and $d \geq \varphi(n)$. Now the problem is to study asymptotic behaviour of $\varrho_\varphi(n)$ for $n \to \infty$.

Another question of the same type is to study asymptotic behaviour of

$$d_\varphi(n) = \sup(d),$$

sup being taken over all $[n, k, d]_q$-codes with $k \geq \varphi(n)$.

We do not discuss these problems here any more, in order to concentrate on the main asymptotic problem. For further information see [18].

Polynomially decodable codes. Up to this moment we were interested only in the parameters of a code and in its construction. We can also add the requirement of its being constructively decodable. Consider a family of $[n_i, k_i, d_i]_q$-codes C_i which have a polynomial decoding algorithm correcting any number of errors up to t_i, where $t_i \leq \lceil (d_i - 1)/2 \rceil$. Let $\tau = \lim(t_i/n_i)$, $R = \lim(k_i/n_i)$. This family gives us a point $(\delta = 2\tau, R)$, and we can describe the sets $U_q^{\text{pol dec}}$ and $U_q^{\text{pol dec lin}}$ of such points in a usual way. We obtain the problem of finding out functions $\alpha_q^{\text{pol dec}}(\delta)$ and $\alpha_q^{\text{pol dec lin}}(\delta)$. Of course, $\alpha_q^{\text{pol}}(\delta) \geq \alpha_q^{\text{pol dec}}(\delta) \geq \alpha_q^{\text{pol dec lin}}(\delta)$, $\alpha_q^{\text{pol lin}}(\delta) \geq \alpha_q^{\text{pol dec lin}}(\delta)$. Note that in our definition δ corresponding to a polynomially decodable family can be less than $\lim(d_i/n_i)$, δ being not the relative minimum distance but rather "the relative minimum polynomially decodable distance" (δ depends on the chosen decoding algorithm).

2. Upper bounds

"Classical" bounds. There exist several theorems giving upper bounds for the mysterious function $\alpha_q(\delta)$. We know no asymptotic upper bound either for $\alpha_q^{\text{lin}}(\delta)$, $\alpha_q^{\text{pol}}(\delta)$, or $\alpha_q^{\text{pol lin}}(\delta)$, which is not valid for $\alpha_q(\delta)$.

Setting $\gamma = 0$ and $\tau = 1 - q/(q-1) \cdot \delta$ in Theorem 7 we get the Plotkin bound:

Theorem 8. $\alpha_q(\delta) \leq R_{\text{P}}(\delta) = 1 - q/(q-1) \cdot \delta$.

Choosing γ and τ in such a way that $\delta = (\delta - 2\gamma)/(1 - \tau)$ we get the Hamming bound:

Theorem 9. $\alpha_q(\delta) \le R_H(\delta) = 1 - H_q(\delta/2)$.

In fact, Theorem 8 is based on the simple consideration that the minimum distance of a code is at most the average one, and Theorem 9 can be proved by counting the total number of points inside nonintersecting spheres of radius $\lceil (d-1)/2 \rceil$ centered at code points.

The Bassalygo-Elias bound is obtained by using both ideas together:

Theorem 10. $\alpha_q(\delta) \le R_{BE}(\delta) = 1 - H_q((q-1)/q - (q-1)/q \cdot \sqrt{1 - (q \cdot \delta)/(q-1)})$.

The following McEliece-Rodemich-Ramsey-Welch bounds ("bounds of four") are obtained using (explicitly or implicitly) the fact that, as metric spaces, both $\mathbb{F}_q^n$ and a sphere in it are equipped with double-transitive group actions. The first one reads (see [7]):

Theorem 11. $\alpha_q(\delta) \le R_4(\delta) = H_q(((q-1) - (q-2)\delta - 2\sqrt{(q-1)\delta(1-\delta)})/q)$.

For $q = 2$ there is a stronger one:

Theorem 12. $\alpha_2(\delta) \le R_{4(2)}(\delta) = \min_{0 < u \le 1-2\delta} \{1 + h(u^2) - h(u^2 + 2\delta u + 2\delta)\}$, *where* $h(x) = H_2((1 - \sqrt{1-x})/2)$.

The upper bound $R_{4(2)}(\delta)$ is the best one known for $q = 2$.

A new bound. Recently, Aaltonen [2] has given its q-ary analogue, which has been improved by Litsyn and Zinoviev [9] (using Theorem 7):

Theorem 13. $\alpha_q(\delta) \le R_{ALZ}(\delta) = \min\{\tau + (1-\tau) \cdot (1 - H_q(w) + f_q(\xi, \eta) - \tau \cdot H_q(\gamma/\tau))\}$, *where* $f_q(\xi, \eta) = H_q(\eta) + (1-\eta) \cdot H_q((\xi - \eta)/(1-\eta)) - \xi \cdot \log_q(q-1) + \eta \cdot \log_q(q-2)$, *and* min *is taken over* τ, w, ξ, η, γ *subject to the conditions* $0 \le \tau \le 1$, $0 \le \gamma/\tau \le 1/2$, $0 \le w \le 1$, $0 \le \eta \le (q-2) \cdot w/(q-1)$, $0 \le \xi - \eta \le \min\{w - \eta, 1 - w\}$, $\beta = (1-\eta) \cdot g((w-\eta)/(1-\eta), (\xi - \eta)/(1-\eta)) \le w - (q-1)/(q-2) \cdot \eta$, $\delta \ge 2\gamma + (2\beta + (w-\beta) \cdot K_{q-1}(\eta/(w-\beta))) \cdot (1-\tau)$, *where* $g(x,y) = (x \cdot (1-x) - y \cdot (1-y))/(1 + 2\sqrt{y \cdot (1-y)})$, $0 \le x, y \le 1$, *and* $K_{q-1}(x) = (q-2)/(q-1) - (q-3)/(q-1) \cdot x - 2/(q-1) \cdot \sqrt{(q-2) \cdot x \cdot (1-x)}$, $0 \le x \le 1$.

At the end of this paper there is a small table of values of different bounds. For more extensive tables see [18].

3. Lower bounds before AG-codes

The random bound. To establish a lower bound one should construct a family of codes (or at least to prove their existence).

We start with the Gilbert-Varshamov bound:

Theorem 14. $\alpha_q(\delta) \geq R_{GV}(\delta) = 1 - H_q(\delta)$; *if* $q = p^a$ *then* $\alpha_q^{\text{lin}}(\delta) \geq R_{GV}(\delta)$.

This is an expurgation bound. To prove the first inequality, fix d and choose points of C one by one with the only requirement that each new point does not lie in the union of spheres of radius d centered at the points we have already chosen; this is surely possible when the total number of points inside these spheres is less than q^n. To prove the second inequality we choose the columns of the parity check matrix (a matrix of the map $\varphi: \mathbb{F}_q^n \to \mathbb{F}_q^{n-k}$ such that $C = \operatorname{Ker} \varphi$), so that each $d-1$ of them are linearly independent, each time estimating the number of those dependent.

In fact almost all linear codes (with probability 1) lie on the Gilbert–Varshamov bound, and almost all nonlinear codes can be "rectified" (by removing some part of points so that asymptotically δ and R are not changed) to lie on it.

Polynomial bounds. The problem of bounding $\alpha_q^{\text{pol}}(\delta)$ and $\alpha_q^{\text{pol lin}}(\delta)$ is more difficult. In fact it is rather difficult even to show that they are not identically zero (this was first shown by Ziablov and Justesen). Using generalized concatenation it is possible to establish the following Bloch–Ziablov bound.

Theorem 15.

$$\alpha_q^{\text{pol lin}}(\delta) \geq R_{BZ}(\delta) = R_{GV}(\delta) - \delta \cdot \int_0^{R_{GV}(\delta)} \frac{dx}{R_{GV}^{-1}(x)},$$

$R_{GV}^{-1}(x)$ *being the inverse function to* $R_{GV}(\delta)$.

4. Algebraic-geometric codes

Constructions and parameters. Since our purpose in this paper is rather to give an impression of the possibilities of algebraic-geometric codes than to expose the inner problems of the theory, we are quite brief here. Algebraic-geometric codes were discovered by Goppa [4], for detailed information see [18]. The following version of the construction is due to Manin [11].

Let X be a smooth variety over $\mathbb{F}_q$, fix a set $\mathscr{P} \subseteq X(\mathbb{F}_q)$ and an invertible sheaf $\mathscr{L}$ on X. There is a natural map

$$H^0(X, \mathscr{L}) \to \bigoplus_{p \in \mathscr{P}} \mathscr{L}_p,$$

$\mathscr{L}_p$ being a (geometric) fiber of $\mathscr{L}$ at P. There is a (noncanonical) isomorphism t_p: $\mathscr{L}_p \xrightarrow{\sim} \mathbb{F}_q$; let us fix it. Then we get a map

$$\varphi: H^0(X, \mathscr{L}) \to \mathbb{F}_q^n,$$

where $n = \#\mathscr{P}$. Its image $C = \operatorname{Im} \varphi \subseteq \mathbb{F}_q^n$ is a code which we denote $C = (X, \mathscr{P}, \mathscr{L})_H$.

Theorem 16. *Let X be a smooth projective curve of genus g over $\mathbb{F}_q$, $C=(X,\mathscr{P},\mathscr{L})_H$, $n=\#\mathscr{P}$, $a=\deg\mathscr{L}$. Then C is an $[n,\geq a-g+1,\geq n-a]_q$-code.*

The proof is more or less trivial, since a section from $H^0(X,\mathscr{L})$ has at most a zeroes and $\dim H^0(X,\mathscr{L})$ is given by the Riemann-Roch theorem.

If $\mathscr{P}\cap\operatorname{Supp}D=\emptyset$, this construction is equivalent to the following one. Let D be a divisor on the curve X, $L(D)=\{f\in\mathbb{F}_q(X)^* \mid (f)+D\geq 0\}\cup\{0\}$. Define $C=(X,\mathscr{P},D)_L$ as the image of the map

$$\begin{aligned}\operatorname{Ev}: L(D)&\to\mathbb{F}_q^n,\\ f&\mapsto(f(P_1),\ldots,f(P_n)),\end{aligned}$$

where $\mathscr{P}=\{P_1,\ldots,P_n\}$. Let $C^\perp=(X,\mathscr{P},D)_\Omega$ be the dual code, then it can be shown that it is given as the image of the map

$$\begin{aligned}\operatorname{Res}: \Omega\Big(\sum_{P_i\in\mathscr{P}}P_i-D\Big)&\to\mathbb{F}_q^n,\\ \omega&\mapsto(\operatorname{Res}_{P_1}(\omega),\ldots,\operatorname{Res}_{P_n}(\omega)),\end{aligned}$$

where Res: $\Omega(\sum_{P_i\in\mathscr{P}}P_i-D)$ is the space of differential forms ω on X such that $(\omega)+\sum P_i-D\geq 0$, and Res_P denotes the residue at P.

The following simple result was noticed in [19,17].

Theorem 17. *Let $A(q)=\limsup N/g$, the limit being taken over all curves X over $\mathbb{F}_q$, $N=\#X(\mathbb{F}_q)$, g being the genus of X. Then*

$$\alpha_q(\delta)\geq 1-A(q)^{-1}-\delta.$$

Asymptotically good curves. Now the crucial point is to determine $A(q)$. Drinfeld and Vlădut [22] proved the following estimate:

Theorem 18. $A(q)\leq\sqrt{q}-1$.

The opposite inequality is rather subtle, and it constitutes the basis of all applications of AG-codes to asymptotic problems. It was first proved by Ihara (see [5]), who used reductions of Shimura curves; independently (for $q=p^2$ and p^4) it was proved in [19], using reductions of classical modular curves and some special Shimura curves; maybe the most simple and conceptual proof is provided by Drinfeld modular curves (see, e.g. [11] or [18, Chapter 4]).

Theorem 19. *If q is an even power of a prime, then*

$$A(q)=\sqrt{q}-1.$$

In the case of q being an odd power, as yet we know no definite answer. Serre

[15] proved that there exists a constant c such that $A(q) \geq c \cdot \log q$ for any q. Zink [24] proved that if $q = p^{3m}$, then $A(q) \geq 2 \cdot (p^{2m} - 1)/(p^m + 2)$. For $q = p^m$, $m \geq 3$, m being odd, Perret [12,13] proved that $A(q) \geq (\sqrt{q+1} - 2)/(2 \cdot (p-1))$ for $q \neq 8$, and that $A(q) \geq (\sqrt{p \cdot q + 1} - 2)/(4 \cdot (p-1))$ for $p \neq 2$, $q \neq 27$.

5. Algebraic-geometric bounds

Algebraic-geometric codes have considerably changed the situation with lower bounds.

The first AG-*bound.* Let us start with the simplest result obtained in [19]:

Theorem 20. *If q is an even power of a prime, then*

$$\alpha_q^{\text{lin}}(\delta) \geq R_{\text{TVZ}}(\delta) = 1 - (\sqrt{q} - 1)^{-1} - \delta.$$

This immediately follows from Theorems 17 and 19. The bound $R_{\text{TVZ}}(\delta)$ intersects $R_{\text{GV}}(\delta)$ iff $q \geq 49$, thus ameliorating it for some δ.

A thorough study of modular curves shows that there exists a polynomial construction, and we get the following result due to Vlăduț (see [20,11,18]).

Theorem 21. *If q is an even power of a prime, then*

$$\alpha_q^{\text{pol lin}}(\delta) \geq R_{\text{TVZ}}(\delta).$$

The expurgation bound. In contrast with this result, the following Vlăduț bound [21] is not polynomial. Let q be an even power of a prime, fix a family of curves X over $\mathbb{F}_q$ with $\lim_X N/g = \sqrt{q} - 1$, and consider the set W_q of codes obtained from these curves for different choices of $\mathscr{L}$. It is easy to prove an analogue of Theorem 1 for W_q; call the corresponding function $\beta_q(\delta)$.

Theorem 22. *Let q be an even power of a prime.*

(a) *If $q < 49$, then*

$$\beta_q(\delta) \geq R_{\text{GV}}(\delta).$$

(b) *Let $q \geq 49$, $\gamma = (\sqrt{q} - 1)^{-1}$. Define δ_1 and δ_4 as the roots of the equation*

$$H_q(\delta) + \frac{q-1}{q} \cdot (1 - \delta) = 1 + \gamma,$$

and δ_2 and δ_3 as the roots of

$$H_q(\delta) + (1 - \delta) \cdot \log_q(q-1) = 1 + \gamma,$$

$0 < \delta_1 < \delta_2 < \delta_3 < \delta_4 < (q-1)/q$.

Then

$$\alpha_q^{\text{lin}}(\delta) \geq \beta_q(\delta) \geq R_V(\delta),$$

where

$$R_V(\delta) = \begin{cases} R_{GV}(\delta) & \text{for } \delta \leq \delta_1 \text{ and for } \delta \geq \delta_4, \\ R_{TVZ}(\delta) & \text{for } \delta_2 \leq \delta \leq \delta_3, \end{cases}$$

and for $\delta_1 \leq \delta \leq \delta_2$ *and* $\delta_3 \leq \delta \leq \delta_4$ *the function* $R_V(\delta) = R_V^0(\delta)$ *is given by the implicit equation*

$$(R_V^0(\delta) + \gamma) \cdot H_q\left(\frac{1-\delta}{R_V^0(\delta)+\gamma}\right) + H_q(\delta) = 1 + \gamma.$$

The proof of this theorem is rather subtle, but the idea is simple and very nice. It uses the expurgation process of the Gilbert–Varshamov bound, but this time we expurgate $\mathbb{F}_q$-points of the Jacobian J_X by "bad" sheaves. Any section from $H^0(X, \mathscr{L})$ has $n - \deg \mathscr{L}$ zeroes (counted with appropriate multiplicities), but it can of course happen that some of these zeroes are concentrated out of $X(\mathbb{F}_q)$. We can estimate the number of sheaves, some section of which has at least a given number of zeroes in $X(\mathbb{F}_q)$ and compare it with the total number of sheaves, i.e., with $\# J_X(\mathbb{F}_q)$. Just as for R_{GV}, almost all codes obtained from the given family of curves (with $\lim_X N/g = \sqrt{q} - 1$) lie on $R_V(\delta)$.

The concatenation bound. The following result, obtained in [23] is an easy consequence of Theorems 5 and 21.

Theorem 23. *Let q be a power of a prime. Then*

$$\alpha_q^{\text{pol}}(\delta) \geq R_{KTV}(\delta),$$

$$\alpha_q^{\text{pol lin}}(\delta) \geq R_{KTV(\text{lin})}(\delta),$$

where $R_{KTV}(\delta)$ *(respectively,* $R_{KTV(\text{lin})}(\delta)$*) is defined as*

$$\max\left\{1 - (q^{k/2} - 1)^{-1} \cdot \frac{k}{n} - \frac{k}{d} \cdot \delta\right\},$$

max *being taken over all* $[n, k, d]_q$*-codes such that* q^k *is an even power of a prime (respectively, over such linear codes).*

Suppose we want to tabulate $R_{KTV}(\delta)$. It is impossible since we do not know parameters of all q-ary codes (which we need to calculate the maximum). However, each family of codes gives a lower bound of $R_{KTV}(\delta)$. In this way it is possible to prove that $R_{KTV}(\delta) > R_{BZ}(\delta)$ for any $\delta \in (0, (q-1)/q)$.

The restriction bound. Another bound can be obtained using Theorems 6 and 21. However it can be ameliorated using rather simple algebraic geometry, see [6]. We get

Theorem 24. *Let q be a power of a prime. Then*

$$\alpha_q^{\text{pol lin}}(\delta) \geq R_{\text{KT}}(\delta) = \max_m \left\{ 1 - \frac{2m(q-1)}{q(q^{m/2}-1)} - \frac{m(q-1)}{q} \cdot \delta \right\},$$

max *being taken over all integers $m \geq 1$ such that q^m is an even power of a prime.*

The idea of the proof is that functions f and f^q have the same values at $\mathbb{F}_q$-points, therefore they give linearly dependent rows of the parity-check matrix. This bound is rather good for small δ (for $\delta \to 0$ and $q=2$ it behaves just as $R_{\text{GV}}(\delta)$).

Nonlinear bounds. Now we melt together Theorems 3 and 22, see [8].

Theorem 25. *For any q*

$$\alpha_q(\delta) \geq R_{\text{LT}}(\delta) = \max\{R'_{\text{LT}}(\delta), R''_{\text{LT}}(\delta)\},$$

where

$$R'_{\text{LT}}(\delta) = \max\{(1 - (R_{\text{V}}^{(q')}(\delta)) \cdot \log_q q'\},$$

max *being taken over even powers of primes $q' = p^{2a} \geq q$ (here $R_{\text{V}}^{(q')}$ means R_{V} for q'-ary codes), and*

$$R''_{\text{LT}}(\delta) = \max\{R_{\text{V}}^{(q')}(\delta) \cdot \log_q q'\},$$

max *being taken over $q' = p^{2a} \leq q$.*

Dec-bound. In [16] a method of decoding AG-codes up to $t \leq \lceil (d-1)/2 - g/2 \rceil$ is described. It yields

Theorem 26. *If q is an even power of a prime, then*

$$\alpha_q^{\text{pol dec lin}}(\delta) \geq R_{\text{SV}}(\delta) = 1 - 2 \cdot (\sqrt{q} - 1)^{-1} - \delta.$$

Melting this bound with concatenation and restriction we get

Theorem 27. *Let q be a power of a prime. Then*

$$\alpha_q^{\text{pol dec lin}}(\delta) \geq \tilde{R}_{\text{SV(lin)}}(\delta) = \max\{R'_{\text{SV(lin)}}(\delta), R''_{\text{SV}}(\delta)\},$$

where

$$R'_{\text{SV(lin)}}(\delta) = \max\left\{ 1 - 2 \cdot (q^{l/2} - 1)^{-1} \cdot \frac{k}{n} - \frac{k}{d} \cdot \delta \right\},$$

max *being taken over all $[n, k, d]_q$-codes such that q^k is an even power of a prime, and*

$$R''_{\text{SV}}(\delta) = \max_m \left\{ 1 - \frac{3m(q-1)}{q(q^{m/2}-1)} - \frac{m(q-1)}{q} \cdot \delta \right\},$$

max *being taken over all integers $m \geq 1$ such that q^m is an even power of a prime. If we omit "linear" we get*

$$\alpha_q^{\text{pol dec}}(\delta) \geq \tilde{R}_{\text{SV}}(\delta) = \max\{R'_{\text{SV}}(\delta), R''_{\text{SV}}(\delta)\}.$$

The self-dual bound. It can be proved that there exist self-dual codes lying on R_{GV}, i.e., that

$$\delta_q^{qsd} \geq \delta_q^{sd} \geq R_{GV}^{-1}(1/2).$$

The following beautiful bound was obtained by Scharlau [14]:

Theorem 28. *If q is an even power of a prime, then*

$$\delta_q^{qsd} \geq \delta_{Sch} = \frac{1}{2} - \frac{1}{\sqrt{q}-3}.$$

If q is an even power of 2, then

$$\delta_q^{sd} \geq \delta_{Sch}.$$

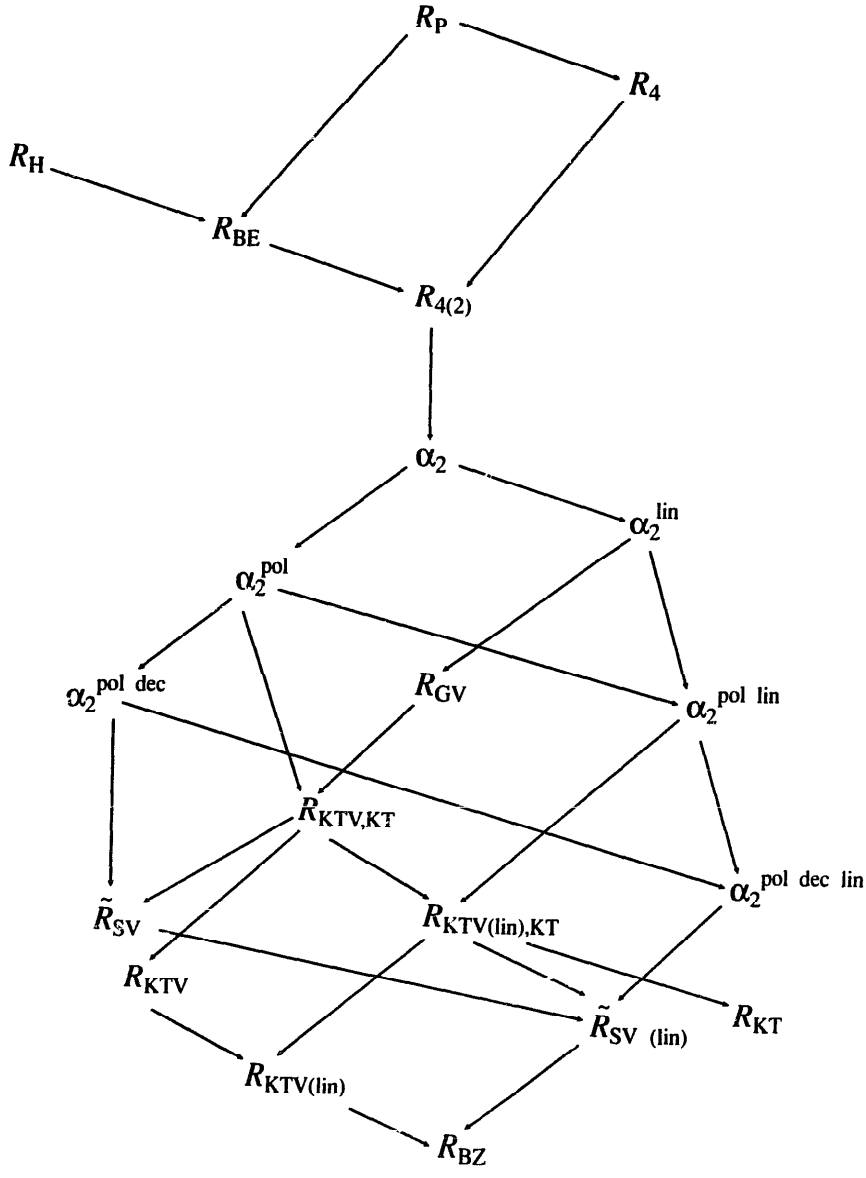

Fig. 1. $q=2$.

This nice statement is based on a subtle result from the class field theory, saying that the canonical divisor of a curve over $\mathbb{F}_q$ is always divisible by 2 (for $q=2^a$ it can be proved elementary). Then an algebraic-geometric code is shortened to obtain a quasi-self-dual one.

For $q=p^{2a}\geq 121$ this bound is better than the random one: $\delta_{\mathrm{Sch}}>R_{\mathrm{GV}}^{-1}(1/2)$.

The constant-weight bound. Ericson and Zinoviev [3] applied algebraic-geometric codes to prove

Theorem 29. $\alpha_2(\omega,\delta)\geq R_{\mathrm{EZ}}(\omega,\delta)=\omega-\delta/2-(\omega\cdot\sqrt{\omega})/(1-\sqrt{\omega})$.

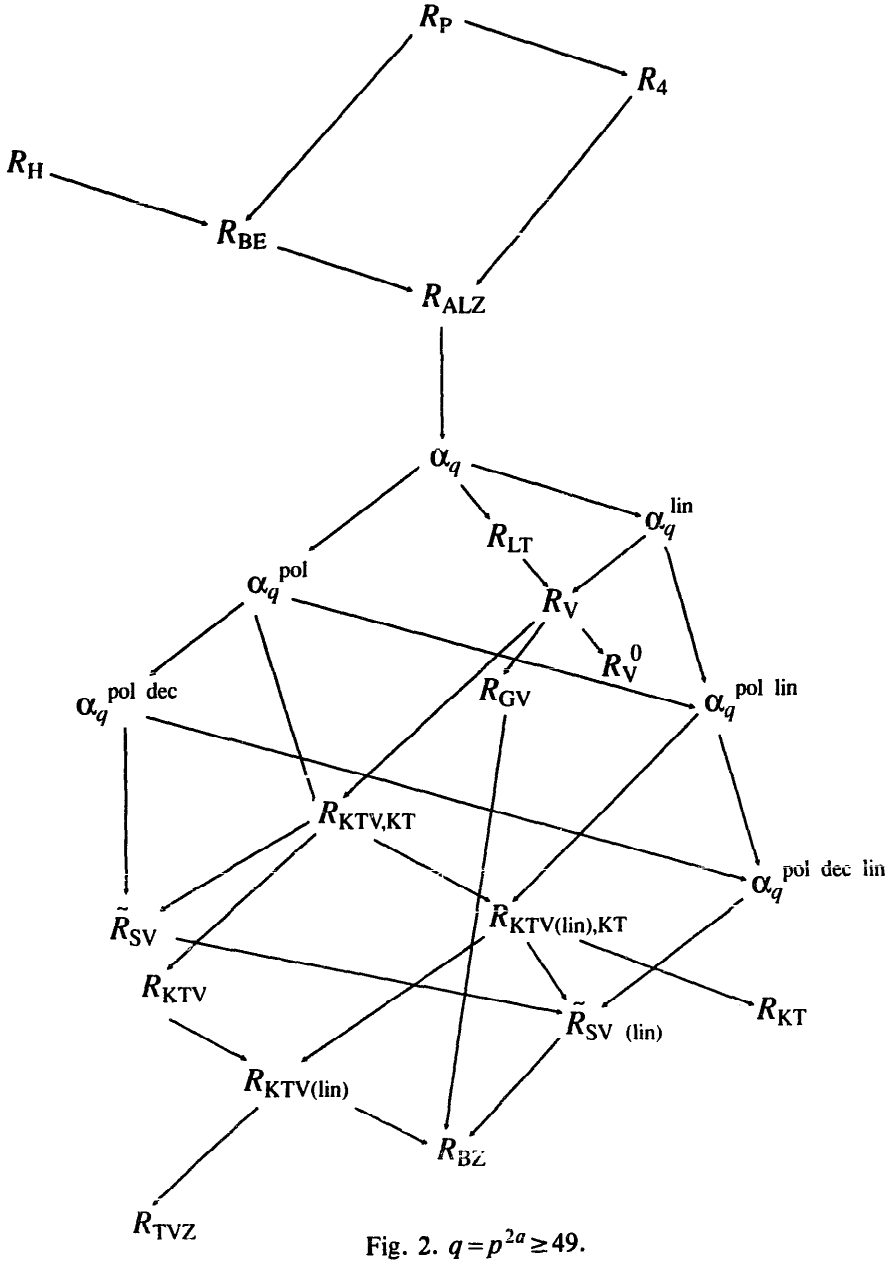

Fig. 2. $q=p^{2a}\geq 49$.

The proof is quite simple, one uses Theorem 20 and a kind of nonlinear concatenation (let $\varphi(i)=(0,0,\ldots,1,\ldots,0)\in\mathbb{F}_2^n$, where 1 stands on the ith place, then φ maps any $[n,k,d]_q$-code $C\subseteq\mathbb{F}_q^n$ to a constant-weight code $\varphi(C)\subset\mathbb{F}_2^{qn}$ whose distance is $2d$ and $\#\varphi(C)=\#C$). It can be shown that for small ω this bound is better than the random one. Of course, Theorem 29 can be generalized to the case of arbitrary q.

6. Diagrams and tables

Relations between various bounds. Since it is rather difficult to compare the bounds we have discussed, we give some auxiliary information here. Let us start with the preceding diagrams, where $A\to B$ means $A(\delta)\geq B(\delta)$ for any $\delta\in[0,(q-1)/q]$. We set $R_{*,**}(\delta)=\max\{R_*(\delta),R_{**}(\delta)\}$.

For $q=2$ we have Fig. 1, and for $q=p^{2a}\geq 49$ we have Fig. 2.

Table 1.

R	$1-R(\delta)$ for $\delta\to 0$	$R\left(\frac{q-1}{q}-x\right)$ for $x\to 0$
R_{BZ}	$\frac{\ln q}{2}\cdot\delta\cdot(\log_q\delta)^2$	$\frac{q^3}{6\cdot(q-1)^2\cdot\ln q}\cdot x^3$
$\tilde{R}_{SV}$	$-2\cdot\frac{q-1}{q}\cdot\delta\cdot\log_q\delta$	$\begin{cases}-\frac{(\sqrt{q}-1)\cdot q^4}{2\cdot(\sqrt{q}^3-1)^3}\cdot x^3\cdot\log_q x, \text{ if } q=p^{2m}\\ -\frac{(q-1)\cdot(q+1)^2\cdot q^5}{2\cdot(q^3-1)^3}\cdot x^3\cdot\log_q x, \text{ else}\end{cases}$
R_{KTV}	$-2\cdot\delta\cdot\log_q\delta$	$\begin{cases}-\frac{2\cdot(\sqrt{q}-1)\cdot q^4}{(\sqrt{q}^3-1)^3}\cdot x^3\cdot\log_q x, \text{ if } q=p^{2m}\\ -\frac{2\cdot(q-1)\cdot(q+1)^2\cdot q^5}{(q^3-1)^3}\cdot x^3\cdot\log_q x, \text{ else}\end{cases}$
R_{KT}	$-2\cdot\frac{q-1}{q}\cdot\delta\cdot\log_q\delta$	<0
R_{GV}	$-\delta\cdot\log_q\delta$	$\frac{q^2}{2\cdot(q-1)\cdot\ln q}\cdot x^2$
R_4	$\frac{2}{\ln q}\cdot\delta$	$-2\cdot x^2\cdot\log_q x$
R_{BE}	$-\frac{1}{2}\cdot\delta\cdot\log_q\delta$	$\frac{q}{2\cdot\ln q}\cdot x$
R_H	$-\frac{1}{2}\cdot\delta\cdot\log_q\delta$	>0
R_P	$\frac{q-1}{q}\cdot\delta$	$\frac{q-1}{q}\cdot x$

Table 2. $q=2$.

δ	R_{BZ}	$\tilde{R}_{SV}$	R_{KTV}	R_{KT}	R_{GV}	R_H	R_{BE}	R_4	$R_{4(2)}$
0.0001	0.9896	0.9980	0.9973	0.9981	0.9985	0.9992	0.9992	0.9997	0.9992
0.01	0.7778	0.8739	0.8677	0.8805	0.9192	0.9546	0.9544	0.9712	0.9542
0.05	0.4456	0.6004	0.6298	0.5417	0.7136	0.8313	0.8279	0.8582	0.8251
0.1	0.2524	0.3704	0.4347	0.2048	0.5310	0.7136	0.7019	0.7219	0.6927
0.15	0.1450	0.2333	0.2847		0.3902	0.6157	0.5920	0.5919	0.5734
0.2	0.0808	0.1667	0.2000		0.2781	0.5310	0.4920	0.4690	0.4614
0.25	0.0423	0.1000	0.1333		0.1887	0.4564	0.3991	0.3546	0.3537
0.3	0.0198	0.0530	0.0733		0.1187	0.3902	0.3117	0.2502	0.2502
0.35	0.0078	0.0316	0.0345		0.0659	0.3310	0.2288	0.1581	0.1581
0.4	0.0022	0.0101	0.0132		0.0290	0.2781	0.1495	0.0815	0.0815
0.45	0.0003	0.0008	0.0035		0.0072	0.2308	0.0734	0.0253	0.0253
0.49	$2\cdot10^{-6}$	$7\cdot10^{-6}$	$3\cdot10^{-5}$		0.0003	0.1967	0.0145	0.0015	0.0015

Table 3. $q=49$.

δ	R_{BZ}	$\tilde{R}_{SV}$	R_{TVZ}	R_{KTV}	R_{KT}	R_V^0	R_{GV}	R_H	R_{BE}	R_4
10^{-4}	0.9936	0.9994	0.8332	0.9994	0.9993		0.9996	0.9998	0.9998	0.9999
0.01	0.9064	0.9642	0.8233	0.9671	0.9534		0.9757	0.9869	0.9869	0.9939
0.1	0.5589	0.7583	0.7333	0.7792	0.6889		0.8170	0.8993	0.8969	0.9236
0.2	0.3584	0.5583	0.6333	0.6333	0.3951		0.6725	0.8170	0.8082	0.8332
0.3	0.2295	0.3667	0.5333	0.5333	0.1012	0.5447	0.5446	0.7422	0.7227	0.7354
0.4	0.1422	0.2667	0.4333	0.4333			0.4292	0.6725	0.6378	0.6321
0.5	0.0828	0.1667	0.3333	0.3333			0.3245	0.6068	0.5517	0.5244
0.6	0.0435	0.0667	0.2333	0.2333			0.2302	0.5446	0.4629	0.4129
0.7	0.0191	0.0300	0.1333	0.1333			0.1467	0.4855	0.3690	0.2982
0.8	0.0059	0.0133	0.0333	0.0333			0.0757	0.4292	0.2666	0.1816
0.9	0.0007	0.0034		0.0036			0.0212	0.3756	0.1465	0.0673
0.97	$2\cdot10^{-6}$	$5\cdot10^{-6}$		$9\cdot10^{-6}$			0.0005	0.3325	0.0291	0.0029

Behaviour at the ends. We describe in Table 1 the behaviour of different bounds (in the main asymptotics) when δ is either near to 0, or to $(q-1)/q$.

Numerical tables. Now we give two small tables of values of different bound for $q=2$ (Table 2) and $q=49$ (Table 3). Much more extensive tables (comprised by A. Barg) can be found in [18].

References

[1] M.J. Aaltonen, Notes on the asymptotic behaviour of the information rate of block codes, IEEE Trans. Inform. Theory 30 (1984) 84–85.

[2] M.J. Aaltonen, A new upper bound for non-binary block codes, in: The Very Knowledge of Coding, Studies in Honor of A. Tietäväinen (1987) 7–39.

[3] T. Ericson and V.A. Zinoviev, An improvement of the Gilbert bound for constant weight codes, IEEE Trans. Inform. Theory 33 (1987) 721–722.
[4] V.D. Goppa, Codes on algebraic curves, Soviet Math. Dokl. 24 (1981) 170–172.
[5] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, J. Fac. Sci. Univ. Tokyo 28 (1981) 721–724.
[6] G.L. Katsman and M.A. Tsfasman, A remark on algebraic-geometric codes, Contemp. Math. 93 (1989) 197–199.
[7] V.I. Levenshtein, Bounds for packings in metric spaces and certain applications, Problemy Kibernet. 40 (1983) 44–110.
[8] S.N. Litsyn and M.A. Tsfasman, A note on lower bounds, IEEE Trans. Inform. Theory 32 (1986) 705–706.
[9] S.N. Litsyn and V.A. Zinoviev, Private communication (1989).
[10] Yu.I. Manin, What is the maximum number of points on a curve over $\mathbb{F}_2$?, J. Fac. Sci. Univ. Tokyo 28 (1981) 715–720.
[11] Yu.I. Manin and S.G. Vlădut, Linear codes and modular curves, J. Soviet Math. 30 (1985) 2611–2643.
[12] M. Perret, Sur le nombre de points d'une courbe sur un corps fini; application aux codes correcteurs d'erreurs, C.R. Acad. Sci. Paris Sér. I 309 (1989) 177–182.
[13] M. Perret, Tours ramifiées infinies de corps globaux, J. Number Theory, to appear.
[14] W. Scharlau, Selbstduale Goppa-codes, Preprint (1987).
[15] J.-P. Serre, Sur les nombres des points rationnels d'une courbe algebrique sur un corps fini, C.R. Acad. Sci. Paris Sér. I 296 (1983) 397–402.
[16] A.N. Skorobogatov and S.G. Vlădut, On the decoding of algebraic-geometric codes, IEEE Trans. Inform. Theory, to appear.
[17] M.A. Tsfasman, On Goppa codes which are better than the Varshamov–Gilbert bound, Problems Inform. Transmission 18 (1982) 163–166.
[18] M.A. Tsfasman and S.G. Vlădut, Algebraic-geometric codes, Kluwer Akad. Publ., to appear.
[19] M.A. Tsfasman, S.G. Vlădut and T. Zink, Modular curves, Shimura curves, and Goppa codes, better than the Varshamov–Gilbert bound, Math. Nachr. 109 (1982) 21–28.
[20] S.G. Vlădut, On the polynomiality of codes on classical modular curves, Preprint (1983).
[21] S.G. Vlădut, An exhaustion bound for algebraic-geometric modular codes, Problems Inform. Transmission 23 (1987) 22–34.
[22] S.G. Vlădut and V.G. Drinfeld, Number of points on an algebraic curve, Functional Anal. 17 (1983) 53–54.
[23] S.G. Vlădut, G.L. Katsman and M.A. Tsfasman, Modular curves and codes with polynomial construction complexity, Problems Inform. Transmission 23 (1987) 22–34.
[24] T. Zink, Examples of curves over $\mathbb{F}_{p^3}$ and Goppa codes, Preprint (1987).