Families of codes exceeding the Varshamov-Gilbert bound.

Marc PERRET
- Equipe CNRS "Arithmétique et Théorie de l'Information" -
- CIRM - Luminy - Case 916 - 13288 Marseille Cedex 9.

Résumé : Le nombre A(q) est la limite supérieure du nombre maximum de points d'une courbe algébrique définie sur le corps fini à q éléments, divisé par le genre. J.-P. Serre a montré que $A(q) \geq c \log q$, où c est une constante positive non nulle. Sa méthode, liée à l'existence de tours infinies de corps de classes de Hilbert, peut donner de meilleurs résultats ; on donne ici de nouvelles minorations de A(q) pour certaines valeurs de q, après avoir montré comment on peut en déduire de nouvelles valeurs de q pour lesquelles il existe des familles de codes sur $\mathbf{F}_q$ dépassant la borne de Varshamov-Gilbert.

Abstract : The number A(q) is the superior limit of the maximum number of points of an algebraic curve defined over the finite field with q elements, divided by the genus. It has been shown by J.-P. Serre that $A(q) \geq c \log q$, where c is a positive constant. His method, based on the existence of infinite towers of Hilbert-class fields, can give better results ; we give here some new lower bounds for A(q) for certain values of q, and we deduce from these some new values of q for which there exists families of codes defined over $\mathbf{F}_q$, exceeding the Varshamov-Gilbert bound.

I. The domain of codes.

Let q be a power of a prime number, and C_q be the set of codes defined over $\mathbf{F}_q$. To each code C of C_q, we can associate its three parameters $[n, k, d]_q$: lenght, dimension and minimum weight. Let us note $\delta(c) = d/n$ the relative distance of C, and $R(c) = k/n$ its transmission rate. We put $V_q = \{(\delta(c), R(c)) ; C \in C_q\}$, and we denote by U_q the set of limit points of V_q. U_q is called the domain of codes over $\mathbf{F}_q$. The question is to study this set. For more details, see [3] .The first result is the following :

Theorem 1. (Manin). For $0 \leq \delta \leq 1$, let $a_q(\delta) = \text{Sup}\,\{R ; (\delta,R) \in U_q\}$.

1) a_q is a continuous, decreasing function on [0,1], vanishing on $[\frac{q}{q-1}, 1]$.

2) $U_q = \{(\delta,R) ; 0 \leq \delta \leq \frac{q}{q-1} ; 0 \leq R \leq a_q(\delta)\}$.

3) $a_q(0) = 1$; $a_q(\delta) \leq \text{Max}\,(1 - \frac{q}{q-1}\delta ; 0)$.

For a proof of this theorem, see [2]. The majoration 3) is called the Plotkin majoration, and is a trivial consequence of the bound of the same name. We can, in an other direction, give a very important lower bound for a_q :

Theorem 2. (Varshamov-Gilbert). For $0 \leq \delta \leq 1$, let $\alpha_q(\delta) = 1 - H_q(\delta)$, with

$$H_q(\delta) = \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta) \log_q (1-\delta)$$

the entropy function. Then, for $0 \leq \delta \leq 1$, $\alpha_q(\delta) \leq a_q(\delta)$.

More than twenty five years of research made it plausible to think that this boundary is the best possible. Throughout this lecture, we say that a family of code is **excellent** if its parameters have a limit point lying above the Varshamov-Gilbert bound. The purpose of this lecture is to prove the existence of excellent families of codes for certain values of q.

II. Goppa codes.

These codes, also called geometric codes, are constructed from algebraic curves defined over $\mathbf{F}_q$, e.g. sets defined by a finite number of polynomial equations with coefficients in $\mathbf{F}_q$. To each irreductible smooth curve X, it is possible to associate a positive integer, g, called the genus of X. One can show that given a curve X of genus g, having at least n points with coordinates in $\mathbf{F}_q$, and of an integer a satisfying $0 < a < n$, then one can construct a $\mathbf{F}_q$ - code, with parameters :

$$[n \,;\, k \geq a - g + 1 \,;\, d \geq n - a]_q \,.$$

If, in addition, $a > 2g - 2$, then $k = a - g + 1$. For more details, see for example [1]. It is clear that these codes satisfy the following :

Proposition 3 : Let $C = [n \,;\, k \geq a - g + 1 \,;\, d \geq n - a]_q$ be a Goppa code, constructed from a curve X of genus g. Then :

$$R(C) + \delta(C) \geq 1 + \frac{1 - g}{n} \,.$$

Remarks: 1) A code C is said to be MDS (Maximum Distance Separable) if its parameters satisfy $R(c) + \delta(c) = 1 + \frac{1}{n}$. Proposition 3 shows that Goppa codes constructed from curves of genus 0, e.g. from $\mathbf{P}^1(\mathbf{F}_q)$, are MDS.

2) The family of Goppa codes is not particular. In fact, each code can be obtained as a subcode of a Goppa code (see [1]). For example, Michon (see [4]) showed how to obtain BCH codes as Goppa codes. It would be interesting to obtain the Golay code in this way.

Proposition 3 shows the importance of the number g/n associated to a curve X : the smaller will be this number, the better will be the parameters of the code so constructed. For $g \in \mathbf{N}$, let $N_q(g)$ be the maximum number of points of a curve X defined over $\mathbf{F}_q$, of genus g, and let

$$A(q) = \limsup_{g \to +\infty} \frac{N_q(g)}{g} \quad .$$

The study of A(q) requires number theory and algebraic geometry. The following theorem, and its corollaries, precise the impact of this study for coding theory :

Theorem 4. (Tsfasman). The intersection of the line $R + \delta = 1 - \frac{1}{A(q)}$ with the square $[0,1] \times [0,1]$, is included in the domain of codes U_q .

See [6] for a proof.

Corollary 5. If

$$\frac{1}{A(q)} < \log_q \frac{2q-1}{q} \ ,$$

then there exist excellent families of codes defined over $\mathbf{F}_q$.

Corollary 6. For every $\delta \in [0,1]$,

$$a_q(\delta) \geq \mathrm{Max}\ (\alpha_q(\delta)\ ;\ 1 - \delta - A(q)^{-1})\ .$$

Remark : It is clear that these two corollaries remain true if we replace A(q) by any lower bound $\bar{A}(q)$ of A(q).

Corollary 6 is an easy consequence of theorems 2 and 4. Next, we prove corollary 5 : the Varshamov - Gilbert curve is convex, decreasing, and has as Tangent line of slope - 1 the line $R + \delta = 1 - \log_q \frac{2q-1}{q}$. Since this line is parallel to the line $R + \delta = 1 - A(q)^{-1}$, the latter will lie above to the former if and only if $A(q)^{-1} < \log_q \frac{2q-1}{q}$. In this case, the latter cut the Varshamov-Gilbert curve in two distinct points, and the segment of the line $R + \delta = 1 - A(q)^{-1}$ delimited by these two points lies above the Varshamov - Gilbert curve, and is included in U_q by theorem 4.

So we have to find lower bound of A(q) as great as possible.

III. Lower bounds of A(q).

1. The first lower bound, obtained in [7] by Tsfasman, Vladut and Zink, was the following : if q is a square, then $A(q) \geq \sqrt{q} - 1$. Ihara proved using Weil's formulae that for all q, $A(q) \leq \sqrt{q} - 1$. Hence, this can be reformulated as follows :

Theorem 7. If q is a square, then $A(q) = \sqrt{q} - 1$.

One can remark that, for q square, the inequality

$$A(q)^{-1} = \frac{1}{\sqrt{q} - 1} < \log_q \frac{2q-1}{q}$$

is true if $q \geq 49$. So, corollary 5 shows the well known :

Corollary 8. If q is a square, $q \geq 49$, then there exist excellent families of codes over $\mathbf{F}_q$.

The proof of theorem 7 is hard. It involves the reduction modulo q of Shimura curves. Unfortunately, these curves are intractable in practice, e.g. they do not permit an effective construction of the excellent families of codes introduced in corollary 8 (see [3]). We give, in the end of the paper, two constructive lower bounds for A(q).

2. Serre's lower bound.

Theorem 9. (Serre). There exists a constant $c > 0$, such that for all q :

$$A(q) \geq c \log q.$$

The key point of theorem 9 is the following :

Lemma 10. Let $\mathbf{l}$ be a prime number, $q \equiv 1 \pmod{\mathbf{l}}$. If there exists A and B included in $\mathbf{F}_q$, disjoint, $|A| = a \geq 2$, $|B| = b \geq 1$, such that :

a) $B - A \subset \mathbf{F}_q^{\times \mathbf{l}} = \{x^{\mathbf{l}} ; x \in \mathbf{F}_q^{\times}\}$,

b) $a + \mathbf{l}b - 1 \leq (a-1)^2/4$,

c) $(a, \mathbf{l}) = 1$,

then :

$$A(q) \geq \frac{2\mathbf{l}b}{(a-1)(\mathbf{l}-1)} .$$

The proof of this lemma involves class field theory. More precisely, we search a condition, for a given function field of one variable over $\mathbf{F}_q$ (which is a global field), to have an infinite $\mathbf{l}$-tower of class fields. For more details, see [5]. We will simply show how to deduce theorem 9 from lemma 10.

Lemma 11. Let (S,E) be a graph, $\omega = |S|$, and let a, b and m three positive integers. We suppose that :

1) $\forall y \in S, |S^{-1}\{y\}| = |\{x \in S ; (x,y) \in E\}| \geq m.$

2) $b\binom{\omega}{a} \leq \omega \binom{m}{a}$.

Then there exist $A, B \subset S$, $|A| = a$, $|B| = b$, such that $A \times B \subset E$.

Proof : Let $T = \{(A,y) \in 2^S \times S \,;\, |A| = a \,;\, A \times \{y\} \subset E\}$.

. We consider the surjective map $\psi : T \to S$, given by : $(A,y) \to y$. The first hypothesis shows that $|\psi^{-1}\{y\}| \geq \binom{m}{a}$. Since the inverse images of points are disjoint, $|T| \geq |S| \binom{m}{a} = \omega \binom{m}{a}$.

. We next consider the surjective map $\varphi : T \to \binom{S}{a} = \{X \subset S \,;\, |X| = a\}$, given by : $(A,y) \to A$. Since $|T| \geq \omega \binom{m}{a}$, and since T is the union of inverse images by φ of the elements of $\binom{S}{a}$, there exists at least one element A_0 of $\binom{S}{a}$, such that $|\varphi^{-1}(A_0)| \geq \dfrac{\omega\binom{m}{a}}{|\binom{S}{a}|} \geq b$ by 2). Now let $B_0 \subset \varphi^{-1}(A_0)$, $|B_0| = b$. The pair A_0, B_0 satisfy the conclusion of lemma 11.

Corollary 12. Let $\mathbf{l} = 2$ (resp. 3) if q is odd (resp. even). Let a(q) and b(q) two integer valued functions of q, such that $a(q) \sim d_1 \log q$, $b(q) \sim d_2 \log^2 q \leq q^{\varepsilon}$ for q large, where d_1, d_2 and ε are three real numbers satisfying $\varepsilon + d_1 \log \mathbf{l} < 1$. Then there exist, for q large enough, A and $B \subset \mathbf{F}_q$, $|A| = a(q)$, $|B| = b(q)$, such that $A - B \subset \mathbf{F}_q^{\times \mathbf{l}}$.

Proof : This is a consequence of lemma 11 with $S = \mathbf{F}_q$, $E = \{(x,y) \in \mathbf{F}_q^{\,2} \,;\, x - y \in \mathbf{F}_q^{\times \mathbf{l}}\}$, and $m = \dfrac{q-1}{\mathbf{l}}$. The inequality

$$b(q) \binom{q}{a(q)} \leq q \binom{m}{a(q)}$$

holds for q sufficiently large if $1 - \varepsilon - d_1 \log \mathbf{l} > 0$. One can see that by using Stirling formulae.

Next, theorem 9 is an easy consequence of lemma 10 and corollary 12.

Remarks : 1) If q is odd, $q \geq 13$, then $A(q) \geq \alpha \log q$, with $\alpha = 0{,}08734.. > \frac{1}{12}$. If q is even, $q \geq 32$, then $A(q) > \beta \log q$, with $\beta = 0{,}02727.. > \frac{1}{37}$. In order to compute the constant c of theorem 9, it is enough to minore A(3), A(5), ..., A(11), and A(2), A(4), A(8), and A(16). For example, Serre showed that $A(2) > \frac{8}{39}$.

2) Since

$$\log_q \frac{2q-1}{q} \sim \frac{\log 2}{\log q} \ ,$$

the existence of excellent families of codes over $\mathbf{F}_q$ for q large enough would result from corollary 5 and theorem 9 if we could show that $c > \frac{1}{\log 2}$. Unfortunately, this bound has not been obtened yet.

3. The main theorems.

a) The first is the following :

Theorem 13. Let $\mathbf{l}$ be a prime number, and suppose that $q > 4\mathbf{l} + 1$. Let k be a positive integer. If q is a primitive k-root of the unity in $\mathbf{F}_\mathbf{l}$, then :

$$A(q^{\mathbf{l}}) \geq \frac{\sqrt{\mathbf{l}} \ \ -2\mathbf{l}}{\mathbf{l}-1} \qquad \text{if } k = 1 \text{ (e.g. if } q \equiv 1 \ (\text{mod } \mathbf{l}\ )),$$

and

$$A(q^k) \geq \frac{\sqrt{\mathbf{l}} \ \ -2\mathbf{l}}{\mathbf{l}-1} \qquad \text{if } k \geq 2 \ .$$

For example : 1) If $q \equiv 1$ (mod 3), or if $q \equiv 2$ or 4 (mod 7), and if $q > 13$, then :

$$A(q^3) \geq \frac{\sqrt{3}}{2}\sqrt{q-1} - 3.$$

2) If $q \equiv 1$ (mod 5), and if $q > 21$, then :

$$A(q^5) \geq \frac{\sqrt{5}}{4}\sqrt{q-1} - \frac{5}{2} \ .$$

Theorem 13 will be a consequence of the following lemma :

Lemma 14 : If Q is a power of q, $q > 4\mathbf{l} + 1$, $Q \equiv 1 \pmod{\mathbf{l}}$, and if all elements of $\mathbf{F}_q$ are $\mathbf{l}$ -power in $\mathbf{F}_Q$, then :

$$A(Q) \geq \frac{\sqrt{\mathbf{l}} - 2\mathbf{l}}{\mathbf{l} - 1} .$$

This lemma imply theorem 13 thank to the following remarks :
-If $q \equiv 1 \pmod{\mathbf{l}}$, then all elements of $\mathbf{F}_q$ is a $\mathbf{l}$ -power in $\mathbf{F}_{q^{\mathbf{l}}}$.
-If $(\mathbf{l}, q-1) = 1$, then all elements of $\mathbf{F}_q$ is a $\mathbf{l}$ -power in $\mathbf{F}_q$, hence in $\mathbf{F}_{q^k}$.
Then one can apply lemma 10, with $Q = q^{\mathbf{l}}$ (resp. q^k), since in the first case $q^{\mathbf{l}} \equiv 1 \pmod{\mathbf{l}}$, and in the second case $q^k \equiv 1 \pmod{\mathbf{l}}$, which is a fundamental hypothesis of lemma 14.

We have now to give a demonstration of lemma 14. we choose as a pair A,B of lemma 10 a partition of $\mathbf{F}_q$.The condition b) of lemma 10, together with a + b = q, enable us to calculate a and b as better as possible. Taking few precautions so that $(a, \mathbf{l}) = 1$, the lower bound of lemma 10 gives the lower bound of lemma 14.

b) Finally, theorem 13, together with corollary 5, shows that :

Theorem 15. Under the assumptions and notations of theorem 13, if

$$\frac{\mathbf{l} - 1}{\sqrt{\mathbf{l}} - 2\mathbf{l}} < \log_{q^{\mathbf{l}}} \frac{2q^{\mathbf{l}} - 1}{q^{\mathbf{l}}} ,$$

(resp. if

$$\frac{\mathbf{l} - 1}{\sqrt{\mathbf{l}} - 2\mathbf{l}} < \log_{q^k} \frac{2q^k - 1}{q^k}),$$

then there exist excellent families of codes over $\mathbf{F}_{q^{\mathbf{l}}}$ (resp. $\mathbf{F}_{q^k}$).

For example, our construction shows the existence of excellent families of $\mathbf{F}_{q^{\mathbf{l}}}$ - codes in the following cases :
1) $\mathbf{l} = 2$, $q \geq 191$ and q odd, which is not as good as the result of corollary 8.
1) $\mathbf{l} = 3$, $q \geq 1657$, and $q \equiv 1 \pmod 3$ or $q \equiv 2$ or $4 \pmod 7$;

2) **l** = 5, q ≥ 16981 , and q ≡ 1 (mod 5).

Références :

- [1] Lachaud, G. : "Les codes géométriques de Goppa", Séminaire Bourbaki, 1984-85, exposé n° 641, Astérisque 133-134, 1986.

- [2] Manin, Yu, I. : "What is the maximum number of points of a curve over $\mathbf{F}_2$?", J. Fac. Sci. Tokyo, I., A., 28, 1981, p. 715-720.

- [3] Manin, Vladut : "Linear codes and modular curves", English translation in J.of Soviet Maths, Vol. 30, n° 6, p. 2611 - 2643.

- [4] Michon, J.F. : "Geométrie algébrique et codes ", p. 301 - 318 in poli, A., Huguet, Li., Codes Correcteurs, Paris Masson, 1989.

- [5] Perret, M. : "Sur le nombre de points d'une courbe sur un corps fini - Application aux codes correcteurs d'erreurs", C.R. Acad. Sci. Paris, à paraître.

- [6] Tsfasman, M.A. : "Goppa codes that are better thant the Varshamov-Gilbert bound", Prob-Peredatchi Inform, 18, 1982, p. 3-6, Traduction anglaise : Prob. Inform. Trans., 18, 1982, p. 163-166.

- [7] Tsfasman, Vladut & Zink : "Modular curves, Shimura curves, and Goppa codes that are better than the Varshamov-Gilbert bound", Math-Nachr, 109, 1982, p. 163-166.

❖❖❖❖❖❖❖