Astérisque

GILLES LACHAUD

Les codes géométriques de Goppa

Astérisque, tome 133-134 (1986), Séminaire Bourbaki,
exp. n° 641, p. 189-207

<http://www.numdam.org/item?id=SB_1984-1985__27__189_0>

Séminaire BOURBAKI Février 1985
37ème année, 1984-85, n°641

LES CODES GÉOMÉTRIQUES DE GOPPA

par Gilles LACHAUD

1. INTRODUCTION

1.1 La théorie de l'information a été créée par C.E.Shannon il y a une quarantaine d'années. Son objet est d'améliorer ou de préserver la qualité des systèmes de transmissions de données à travers l'espace (réseaux téléphoniques, communications par satellite) ou le temps (bandes magnétiques, disques optiques, etc.). Les transmissions sont en effet menacées par le bruit, les distorsions, etc. On a par ailleurs de bonnes raisons de penser aujourd'hui que les codes correcteurs interviennent dans le **code génétique.**

La théorie s'est développée suivant deux approches distinctes. Shannon a fondé l'approche probabiliste; il a démontré qu'il existe des codes dont le taux de transmission est aussi voisin que l'on veut de la capacité du canal, et qui rendent la probabilité d'erreur aussi petite que l'on veut (cf. **3.5**). Son théorème n'indique malheureusement pas comment on peut trouver de tels codes. En revanche, l'approche algébrique, amorcée par Golay et Hamming, consiste à construire explicitement des systèmes remplissant ces conditions : c'est l'objet de la théorie des codes correcteurs d'erreurs.

On a construit des codes correcteurs en utilisant un grand nombre de méthodes, issues notamment de l'algèbre et de la géométrie sur les corps finis, ou de la combinatoire (réseaux, empilement de sphères). On trouvera dans [Bl] une réimpression commentée des principaux articles sur ce sujet publiés entre 1949 et 1972; le livre [MW-S] et ses 1478 références joue le rôle de bible. Des exemples de codes utilisés dans les mémoires à semi-conducteurs figurent dans [Ch-Hs].

Les travaux récents de Goppa ([Go 3],[Go 4]), en établissant un dictionnaire entre la théorie des codes et l'arithmétique des courbes algébriques sur un corps fini, ont amené une refonte partielle de la théorie et une unification des procédés de construction de codes : c'est ce qu'on verra dans la deuxième partie de cet exposé.

Ce travail a été rédigé au sein de l'A.T.P. du C.N.R.S. "Applications des Mathématiques Pures" n°399 (Y.Colombé, Y.Driencourt, J.F.Michon).

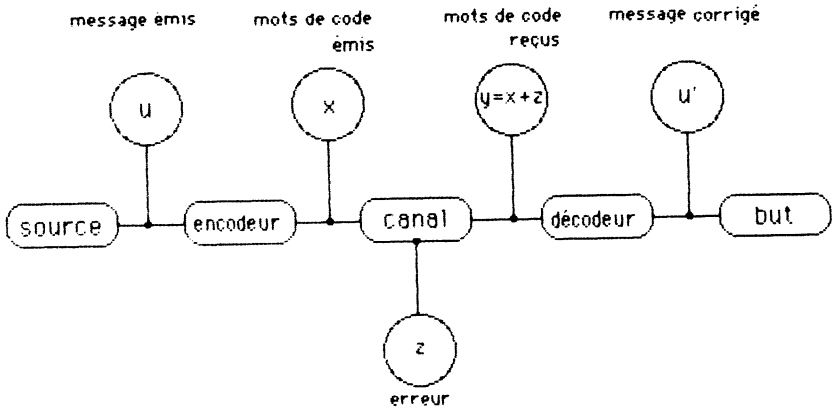

Figure 1.

1.2 Le modèle général d'un système de transmission comportant une protection contre les erreurs est indiqué dans la figure 1. On va maintenant examiner ce processus plus en détail.

Soit p un nombre premier, e un entier naturel et $q = p^e$. On veut transmettre des **messages**, qui sont des mots (vecteurs à 1 ligne) de longueur k dont les lettres sont dans le corps fini $\underline{F}_q$; ce sont donc des éléments de l'espace vectoriel $\underline{F}_q^k$. Le cas le plus courant est celui où q est une puissance de 2. On passe d'abord ces messages dans un **encodeur**, qui est une application injective

$$\underline{E} : \underline{F}_q^k \longrightarrow \underline{F}_q^n ;$$

l'image de $\underline{E}$ s'appelle le **code** utilisé; il est dit linéaire si l'encodeur l'est lui-même; ainsi un **code linéaire** C sur le corps fini à q éléments $\underline{F}_q$ n'est pas autre chose qu'un sous-espace vectoriel de $\underline{F}_q$. Les éléments x de C sont les **mots de code**; la dimension k de C sur $\underline{F}_q$ est la **dimension** du code, l'entier n est la **longueur** du code, et l'entier n-k est sa **redondance**. On transmet ensuite les mots de code à travers un **canal**, supposé **discret** (le canal transmet un signal par unité de temps), **sans mémoire** (la transmission d'un signal n'a aucun effet sur les transmissions suivantes), et **sans effacement** (un signal est reçu pour tout signal émis). Le signal émis est alors perturbé et c'est un vecteur y qui est en fait reçu : la différence $z = y-x$ est l'erreur commise. Le message reçu est alors envoyé dans un **décodeur**

$$\underline{D} : \underline{F}_q^n \longrightarrow \underline{F}_q^k$$

qui est une section de l'encodeur $\underline{E}$, et qui fait correspondre à tout vecteur reçu y de $\underline{F}_q^n$ un vecteur corrigé qui soit l'un des mots de code **le plus vraisemblablement émis** (maximum likehood decision), à savoir un vecteur u' de $\underline{F}_q^k$ pour lequel $\underline{E}(u')$ et y aient le moins de coordonnées différentes possibles : on suppose toujours que l'erreur de transmission est minimum.

2. GÉNÉRALITÉS SUR LES CODES LINÉAIRES

2.1 Soit C un code de longueur n et de dimension k. Si on choisit des bases de $\underline{F}_q^k$ et de $\underline{F}_q^n$, un encodeur dont C est l'image est donné par une matrice G à k lignes et n colonnes à éléments dans $\underline{F}_q$ de rang maximum k, et s'écrit comme l'application linéaire

$$\underline{E}_G(u) = uG \ ;$$

on dit que G est une **matrice génératrice** de C. Autrement dit, les lignes de G forment une base de C. On dit que G est **sous forme standard** si

$$G = (I_k \ B) \ ,$$

où I_k est la matrice carrée identité de type (k,k) et où B est une matrice à k lignes et n-k colonnes. Si G est une matrice génératrice du code C qui est sous forme standard, il est naturel d'appeler les k premières coordonnées d'un vecteur de C les **symboles d'information**, et les n-k suivantes les **symboles de contrôle.**

2.2 On dit que deux codes sont équivalents si l'un se déduit de l'autre par permutation des coordonnées. Il s'ensuit que tout code est équivalent à un code qui a une matrice génératrice sous forme standard.

Soit maintenant H une matrice à n-k lignes et n colonnes, de rang n-k. On lui associe l'application linéaire

$$\underline{S}_H(x) = H\,{}^t x$$

de $\underline{F}_q^n$ dans $\underline{F}_q^{n-k}$. Si le code C est égal au noyau de $\underline{S}_H$, on dit que H est une **matrice de contrôle** de C. Si on se donne un code C de matrice génératrice G et de matrice de contrôle H, on a donc une suite exacte

$$0 \longrightarrow \underline{F}_q^k \xrightarrow{\underline{E}_G} \underline{F}_q^n \xrightarrow{\underline{S}_H} \underline{F}_q^{n-k} \longrightarrow 0 \ .$$

Si la matrice génératrice G est sous forme standard, on peut prendre comme matrice de contrôle la matrice

$$H = (-{}^t B \ I_{n-k}).$$

2.3 Le **dual** $C^\perp$ d'un code C est le sous-espace orthogonal de C pour la forme bilinéaire symétrique non dégénérée

$$(x \mid y) = \Sigma x_j y_j \ ;$$

on déduit immédiatement de la suite exacte de **2.2** que la matrice génératrice d'un code est une matrice de contrôle pour son orthogonal, et vice versa.

2.4 Si x est dans $\underline{F}_q^n$, le **poids** w(x) de x est le nombre de ses coordonnées non nulles. Si x et y sont dans $\underline{F}_q^n$, le nombre

$$d(x,y) = w(x-y)$$

est une distance sur $\underline{F}_q^n$, appelée la **distance de Hamming.** Si C est un code, la **distance minimale** de C est le nombre :

$$d = \text{Min}\{ d(x,y) \mid (x,y) \in C \times C \text{ et } x \neq y \}$$
$$= \text{Min}\{ w(x) \mid x \in C - \{0\} \}.$$

2.5 Si C est un code, on peut construire un décodeur de la façon suivante :
- pour tout vecteur reçu y, on cherche un élément z de poids minimal dans l'ensemble y + C, et on déclare alors que z est l'erreur commise : le mot x = y - z est celui qui a été le plus vraisemblablement émis.

Soit [a] la partie entière du nombre réel a; si un code C est de distance minimale d, les boules centrées en les points de C et de rayon $t = [(d-1)/2]$ sont disjointes; par suite le code C admet un décodeur qui corrige t erreurs, en faisant correspondre à tout vecteur reçu y qui est à distance $\leqslant t$ de C le seul élément x de C tel que $d(x,y) \leqslant t$.

2.6 Signalons en passant que le polynôme des poids d'un code C de longueur n est

$$P_C(X,Y) = \sum_{u \in C} X^{n-w(u)} Y^{w(u)} ;$$

il y a un pont entre la théorie des codes et la géométrie des nombres (théorie des réseaux) dans lequel le polynôme des poids joue le rôle des séries thêta; à la formule de Poisson correspond la formule de Mac-Williams

$$P_{C^\perp}(X,Y) = (\text{Card } C)^{-1} P_C(X + (q-1)Y, X-Y);$$

on renvoie à [Br] pour un exposé détaillé en caractéristique 2.

2.7 Si C est un code de longueur n, de dimension k et de distance minimale d, on dit que C **est un code de type** [n, k, d] ; les **paramètres asymptotiques** de C sont

$$R(C) = k/n , \quad \delta(C) = d/n ;$$

le rapport R(C) est appelé **taux de transmission** (ou efficacité) du code C , et le rapport $\delta(C)$ sa **distance relative.**

3. FAMILLES DE SHANNON

3.1 Dans le **modèle algébrique** d'un système de transmission (cf. [Go 4]), on se donne, pour tout entier n, une partie V_n de F_q^n, et on fait l'hypothèse suivante:

(H) **pour tout mot de F_q^n émis, l'erreur commise est dans V_n.**

Lorsqu'il existe, le nombre

$$\mu = \lim_{n\infty} (n^{-1} \log_q(\text{Card } V_n))$$

est appelé **l'entropie de Hartley** du système, et le nombre

$$ß = 1 - \mu$$

sa **capacité.**

3.2 Par exemple, le **modèle de Hamming** est le cas d'un canal satisfaisant à la condition (H) en prenant $V_n = B_n(cn)$ (avec $0 < c < 1$), où $B_n(T)$ est la boule de

centre 0 et de rayon T de $\underline{F}_q^n$:

$$B_n(T) = \{x \in \underline{F}_q^n \mid w(x) \leqslant T\}.$$

On a

$$\text{Card } B_n(T) = \Sigma_{0 \leqslant i \leqslant T} \binom{n}{i} (q-1)^i ;$$

et un calcul simple (cf.[VL],p.55) montre que l'on a dans ce cas

$$\mu = \lim_{n \infty} (n^{-1} \text{Card } B_n(cn)) = H_q(c),$$

avec

$$H_q(c) = c \log_q(q-1) - c \log_q c - (1-c) \log_q(1-c).$$

3.2 Soient H une matrice de type (n-k,n),

$$\underline{S}_H : \underline{F}_q^n \longrightarrow \underline{F}_q^{n-k}$$

l'application linéaire définie par H, et C le code noyau de $\underline{S}_H$. Le vecteur $s = \underline{S}_H(y) = H^t y$ est appelé le **syndrome** du vecteur y. Les mots de C sont de syndrome nul, et le syndrome de tout vecteur reçu est égal au syndrome de l'erreur z. On pose

$$V_n' = \{z \in V_n \mid \underline{S}_H^{-1}(\underline{S}_H(z)) = \{z\}\};$$

ainsi, l'ensemble V_n' est la plus grande partie de V_n telle que la restriction de $\underline{S}_H$ à la-dite partie soit injective. Si l'erreur commise est dans V_n', il y a une seule façon de décoder, puisque dans ce cas le syndrome détermine l'erreur; en revanche, si l'erreur commise est dans $V_n - V_n'$, plusieurs vecteurs d'erreur correspondent à un même syndrome, et l'erreur est incorrigible. Le nombre

$$e = \text{Card}(V_n - V_n')/\text{Card } V_n = 1 - (\text{Card } V_n'/\text{Card } V_n)$$

s'appelle le **taux d'erreur** du code C.

3.4 Soit $\underline{C}$ une famille de codes sur $\underline{F}_q$. On dit que $\underline{C}$ est une **famille de Shannon** (pour un canal de capacité ß) si elle vérifie la condition suivante :

(S) **Quels que soient** $\varepsilon_1 > 0$ **et** $\varepsilon_2 > 0$ **, si** n **est assez grand, il existe un code de la famille** $\underline{C}$ **de longueur** n **, de taux de transmission** $R > ß - \varepsilon_1$ **et de taux d'erreur** $e < \varepsilon_2$.

3.5 Dans le **modèle probabiliste** de Shannon (cf. par ex. [ME]), les vecteurs émis sont présentés comme des variables aléatoires discrètes; on a aussi, dans ce modèle, une notion de capacité et de taux d'erreur; par exemple, le cas du **canal symétrique binaire** avec probabilité d'erreur de transmission p (qu'on peut toujours supposer $\leqslant 1/2$!) est donné par la figure 2.

L'entropie de Shannon de ce canal est donnée par

$$H_2(p) = -p \log_2 p - (1-p) \log_2(1-p),$$

et sa **capacité** est

$$C_2(p) = 1 - H_2(p).$$

Le **taux (ou probabilité) d'erreur de Shannon** e d'un canal est la probabilité qu'un mot de code erroné sorte du canal.

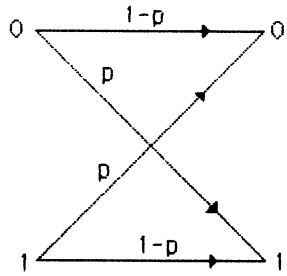

Figure 2.

Les mots ayant maintenant le sens qu'on leur a donné dans ce paragraphe-ci, le théorème de Shannon s'énonce en disant que **l'énoncé** (S) **est vrai pour la famille de tous les codes** (linéaires ou non) (cf. [ME] et [VL]).

3.6 Si on se place dans le modèle de Shannon, un nombre $\varepsilon > 0$ étant donné, on sait grâce à la loi des grands nombres que pour n assez grand il existe dans $\underline{F}_q^n$ un ensemble V(n) tel que la probabilité pour que l'erreur commise ne soit pas dans V(n) soit $< \varepsilon$. Il s'ensuit qu'une famille de Shannon dans le modèle algébrique est aussi une famille de Shannon dans le modèle probabiliste.

3.7 Le **problème principal de la théorie des codes** consiste à trouver explicitement des familles de Shannon. En pratique, le taux d'erreur d'un code est difficile à calculer; mais on peut utiliser la distance relative δ d'un code C comme une bonne mesure de qualité du code, puisque celui-ci corrige $t = [(\delta n-1)/2]$ erreurs; par suite, si H est une matrice de contrôle de C, l'application $\underline{S}_H$ est injective sur la boule de rayon t. La première étape dans la résolution du problème principal consiste à chercher des codes avec des paramètres $R(C) = k/n$ grand et $\delta(C) = d/n$ grand. Dès lors, une bonne famille de codes $\underline{C}$ sera une famille (infinie) telle que les nombres $\delta(C)$ et R(C) puissent ne pas devenir trop petits lorsque C parcourt $\underline{C}$.

4. LE DOMAINE DES CODES

4.1 On va maintenant préciser ce que l'on vient de dire en **3.7**. On note $\underline{C}_q$ l'ensemble des codes sur $\underline{F}_q$ et V_q l'image de l'application

$$F : \underline{C}_q \longrightarrow [0, 1]\times[0, 1]$$

définie par

$$F(C) = (\delta(C), R(C)).$$

Enfin, on note U_q l'ensemble **dérivé** de V_q : c'est le **domaine des codes sur** $\underline{F}_q$. (Rappelons que l'ensemble dérivé X' d'un ensemble X est l'ensemble de ses points d'accumulation). Une **bonne famille de codes** sera par définition une famille dont

le couple de paramètres a un point d'accumulation au moins situé à l'intérieur du domaine des codes.

4.2 Pendant longtemps, on ne pouvait établir l'existence de bonnes familles de codes qu'en s'appuyant sur le théorème de Shannon. Ce n'est qu'en 1970 que Justesen a construit par concaténation de bonnes familles de codes. Ce principe a été repris par Delsarte et Piret (cf. [De-Pi]) pour construire des codes de Shannon; mais cf. le § 9.

4.3 THÉORÈME (Manin). **Posons, pour** δ **dans** $[0, 1]$:

$$a_q(\delta) = \sup\{R(C) \mid C \in \underline{C}_q \text{ et } \delta(C) = \delta\}.$$

a) **la fonction** a_q **est continue et décroissante;**

b) **on a**

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

On renvoie à [Ma] et à [Ma-Vl] pour une démonstration détaillée de ce théorème, et on se contente d'indiquer les principales étapes :

(1) si on dispose d'un code de type $[n, k, d]$, et si $1 \leqslant k$, on peut construire un code de type $[n-1, k-1, d]$.

(2) on déduit de (1) que si le point (δ_o, R_o) est dans U_q, le segment de la droite d'équation $\delta_o R - R_o \delta = \delta_o - \delta$ compris dans la bande $0 \leqslant R \leqslant R_o$ est contenu dans U_q.

(3) si on dispose d'un code de type $[n, k, d]$, et si $1 \leqslant k$, on peut construire un code de type $[n-1, k, d-1]$.

(4) on déduit de (3) que si le point (δ_o, R_o) est dans U_q, le segment de la droite d'équation $R - \delta = R_o - \delta_o$ compris dans la bande $0 \leqslant \delta \leqslant \delta_o$ est contenu dans U_q.

On déduit alors les conclusions du théorème des assertions (2) et (4).

Question : la fonction a_q est-elle dérivable ?

4.4 On va maintenant donner des bornes pour le domaine des codes. Tout d'abord, il est facile de voir que pour tout code de type $[n, k, d]$, on a $d \leqslant n - k + 1$, autrement dit

$$\delta + R \leqslant 1 + 1/n ;$$

c'est la **borne de Singleton**; pour (δ, R) dans U_q, on a donc

$$\delta + R \leqslant 1.$$

4.5 On peut préciser **4.4** : on a en effet

$$a_q(\delta) \leqslant \mathrm{Max}(1 - (q\delta/(q-1)), 0) ;$$

c'est la **borne de Plotkin.**

4.6 On sait aussi que

$$a_q(\delta) \geqslant 1 - H_q(\delta)$$

où la fonction H_q est celle définie en **3.2**; c'est la **borne de Varshamov-Gilbert.**

Une **excellente famille de codes** est par définition une famille dont les paramètres ont un point d'accumulation situé au-dessus de la borne de Varshamov-Gilbert.

4.7 Remarque. La fonction $1-H_q$ est convexe; on a $(dH_q/d\delta)(\delta_o) = 1$ pour $\delta_o = (q-1)/(2q-1)$; en ce point on a

$$\delta_o - H_q(\delta_o) = 1 - \log_q(2q-1).$$

Par suite, la tangente à la courbe $R = 1 - H_q(\delta)$ au point $\delta = \delta_o$ a pour équation $R + \delta = 1 - S_o$, avec $S_o = \log_q((2q-1)/q)$; la droite d'équation $R + \delta = 1 - c$ aura un segment au-dessus de la courbe de Varshamov-Gilbert dès que $c < S_o$.

4.8 Pour les bornes supérieures, on dispose de la borne d'Elias et lorsque $q = 2$, de la borne $a_2(\delta) \leqslant g_2(\delta)$ de Mc Eliece-Rodemich-Rumsey-Welch, où g_2 est une fonction explicite; on trouvera ces bornes dans [MW-S], Ch.17,§7. Il nous suffira ici de dire que la droite d'équation

$$R + \delta = 1 - 0.525$$

est tangente à la courbe $R = g_2(\delta)$.

5. LES CODES GÉOMETRIQUES

5.1 On va d'abord rappeler quelques résultats sur les courbes algébriques. Soient X une courbe algébrique complète, absolument irréductible et non singulière de genre g définie sur $\underline{F}_q$; si $\underline{F}$ est une extension de $\underline{F}_q$ on note $X(\underline{F})$ l'ensemble des points de X qui sont définis sur $\underline{F}$. On note encore $R(X,\underline{F})$, ou simplement $R(X)$ lorsque $\underline{F} = \underline{F}_q$ le corps des fonctions rationnelles sur X définies sur $\underline{F}$, et $Div(X,\underline{F})$ le groupe des diviseurs sur X définis sur $\underline{F}$; c'est le groupe abélien libre engendré par l'ensemble des **places** du corps $R(X,\underline{F}_q)$; il revient au même de dire, en notant $\underline{F}_q^a$ la clôture algébrique de $\underline{F}_q$, qu'un élément de $Div(X,\underline{F}_q)$ est un élément du groupe libre $Div(X,\underline{F}_q^a)$ engendré par l'ensemble $X(\underline{F}_q^a)$ des **points algébriques** de X, qui est invariant sous l'action de $Gal(\underline{F}_q^a/\underline{F}_q)$. Si f est dans $R(X,\underline{F})$, le diviseur (f) de f est dans $Div(X, \underline{F})$.
Pour tout élément T de $Div(X, \underline{F}_q)$, on note L(T) l'espace vectoriel des fonctions f dans R(X) telles que f = 0 ou bien $(f) \geqslant -T$.

Les formes différentielles d'ordre 1 qui sont rationnelles sur X et définies sur $\underline{F}_q$ sont les éléments de l'espace vectoriel $\Omega(X)$ des différentielles de Kähler du corps R(X); l'espace $\Omega(X)$ est de dimension 1 sur R(X). On note (ω) le diviseur d'une forme différentielle ω, et pour tout élément T de $Div(X, \underline{F}_q)$, on note $\Omega(T)$ l'espace vectoriel des formes ω dans $\Omega(X)$ telles que $\omega = 0$ ou bien $(\omega) \geqslant T$; en particulier, l'espace $\Omega(0)$, que l'on note aussi $\Omega[X]$, n'est autre que l'espace vectoriel de dimension g sur $\underline{F}_q$ des différentielles de première espèce.

A toute forme différentielle ω on sait associer son **résidu** Rés(ω, P)

en chaque point P de $X(\underline{F}_q^a)$; et la somme des résidus d'une forme différentielle est nulle.

Pour toutes ces notions, on renvoie à la section 1 de la bibliographie.

5.2 Soit (D,G) un couple de diviseurs de Div(X, $\underline{F}_q$), sur lesquels on fait les hypothèses suivantes :

a) le diviseur D est positif et s'écrit

$$D = P_1 + \ldots + P_n ,$$

avec des points $P_1, \ldots, P_n$ tous distincts et dans $X(\underline{F}_q)$;

b) le diviseur G est positif ;

c) les supports de D et de G sont disjoints.

5.3 Les données étant celles de **5.2**, on note C_L le code de longueur n qui est l'image de l'application linéaire

$$\emptyset_L : L(G) \longrightarrow \underline{F}_q^n$$

définie par

$$\emptyset_L(f) = (f(P_1) \ \ldots \ f(P_n)) ;$$

c'est une injection si $\deg(G) < n$ (en effet, si $\emptyset_L(f) = 0$, on a $(f) \geqslant D - G$, et ce dernier diviseur est de degré > 0).

Proposition. Soit $[n, k_L, d_L]$ **le type du code** C_L**, et supposons** $\deg(G) < n$.

On a $$k_L \geqslant \deg(G) - g + 1 ;$$

avec égalité si $\deg(G) > 2g - 2$,

et $$d_L \geqslant n - \deg(G).$$

Démonstration. Le théorème de Riemann-Roch affirme que pour tout diviseur T, on a

$$\dim L(T) = \deg(T) - g + 1 + \dim \Omega(T) ,$$

et $\Omega(T)$ est réduit à {0} dès que $\deg(T) > 2g-2$, d'où l'assertion sur k_L en faisant T = G. Par ailleurs si f est dans L(G) et si le poids de $\emptyset_L(f)$ est égal à d, cela signifie que la fonction f s'annule en n-d points $P_{i(1)}, \ldots, P_{i(n-d)}$ du support de D, et on a

$$(f) \geqslant P_{i(1)} + \ldots + P_{i(n-d)} - G ;$$

en prenant les degrés il vient

$$0 \geqslant n - d - \deg(G) ,$$

d'où l'assertion sur d_L.

5.4 Posons $\dim L(G) = \ell$; si on choisit une base $(f_1, \ldots, f_\ell)$ de L(G), la matrice génératrice de C_L est la matrice à k lignes et n colonnes

$$G(C_L) = \begin{pmatrix} f_1(P_1) & \ldots & f_1(P_n) \\ f_i(P_1) & \ldots & f_i(P_n) \\ f_\ell(P_1) & \ldots & f_\ell(P_n) \end{pmatrix} ;$$

si on considère l'application rationnelle $\underline{f} = (f_1,\ldots,f_\ell)$ de X dans $\underline{A}^\ell$, les colonnes de $G(C_L)$ sont les vecteurs-colonnes ${}^t\underline{f}(P_j)$, pour $1 \leqslant j \leqslant n$.

Un pas important dans l'élaboration effective d'un algorithme de construction consiste à trouver des bases pour les espaces L(G), ce qui peut être fait en adaptant l'algorithme de Coates en caractéristique non nulle : cf. [Laz] et sa bibliographie.

5.5 On peut généraliser le procédé de construction du code C_L de la façon suivante : on prend une variété algébrique complète et non singulière X définie sur $\underline{F}_q$, un faisceau inversible $\mathscr{L}$ sur X (Cf. [Ha], [Sh]), et une partie V de $X(\underline{F}_q)$; pour tout x de V, on choisit un générateur de la fibre $\mathscr{L}_x$, ce qui fournit un isomorphisme de $\mathscr{L}_x$ sur $\underline{F}_q$, et une application

$$\emptyset_{\mathscr{L}} : \Gamma(X,\mathscr{L}) \longrightarrow \prod \mathscr{L}_x = \underline{F}_q^{\mathrm{Card}\ V}$$

on a ainsi associé au couple $(V,\mathscr{L})$ un code sur $\underline{F}_q$, à savoir l'image de $\emptyset_{\mathscr{L}}$, qui est de longueur Card(V).

Si on prend par exemple $X = \underline{P}^r$, puis $V = \underline{P}^r(\underline{F}_q)$ et $\mathscr{L} = \mathscr{O}(1)$, on obtient un code de paramètres

$$n = (q^{r+1} - 1)/(q-1)\ , \quad k = r + 1\ , \quad d = q^r.$$

5.6 En conservant toujours les données de **5.2**, on considère maintenant le code C_Ω, également de longueur n, qui est l'image de l'application

$$\emptyset_\Omega : \Omega(G-D) \longrightarrow \underline{F}_q^n$$

définie par

$$\emptyset_\Omega(\omega) = (\mathrm{Rés}(P_1, \omega), \ldots \mathrm{Rés}(P_n, \omega)\ ;$$

la noyau de $\emptyset_\Omega$ est égal à $\Omega(G)$; par suite, $\emptyset_\Omega$ est une injection dès que $\deg(G) > 2g-2$.

Proposition. Soit $[n, k_\Omega, d_\Omega]$ **le type du code** C_Ω **défini par le couple** (D,G) **de diviseurs de** X.

Supposons $2g - 2 < \deg(G) < n + g - 1$.

On a : $$k_\Omega \geqslant n - \deg(G) + g - 1\ ;$$

avec égalité si $\deg(G) > n$,

et $$d_\Omega \geqslant \deg(G) - 2g + 2\ .$$

Démonstration. D'après le théorème de Riemann-Roch, on a, pour tout diviseur T:

$$\dim \Omega(T) = -\deg(T) + g - 1 + \dim L(T)\ ;$$

puisque $\deg(G) > 2g-2$, l'application $\emptyset_\Omega$ est injective, par suite $k_\Omega = \dim \Omega(G-D)$. Si $\deg(G) < n$, on a $L(G-D) = \{0\}$, d'où les assertions sur k_Ω.

Si ω est dans $\Omega(G-D)$ et si le poids de Hamming de $\emptyset_\Omega(\omega)$ est égal à d, cela signifie que ω a des résidus non nuls en d points $P_{i(1)},\ldots,P_{i(d)}$ du support de D, et donc

$$(\omega) \geqslant G - (P_{i(1)} + \ldots + P_{i(d)})\ ;$$

en prenant les degrés il vient :

$$2g-2 \geqslant \deg(G) - d,$$

d'où l'assertion sur d_Ω.

5.7 Voici un exemple de code C_Ω: on suppose $p > 2$ et on considère la conique

$$X : y^2 = xz$$

de $\underline{P}^2(\underline{F}_q)$; si t est dans $\underline{F}_q$, on pose $P_t = (t : t^2 : 1), P_\infty = (1 : 0 : 0)$,

$$D = \sum_{t \in \underline{F}_q} P_t \ , \quad G = 2\, P_\infty \ ;$$

l'espace $L(2\, P_\infty)$ est de dimension 3, de base $(f_1, f_2, f_3) = (1, x/z, y/z)$; en notant $t_1, \ldots, t_q$ les éléments de $\underline{F}_q$ le code C_Ω a pour matrice de contrôle

$$H = \begin{pmatrix} 1 & \ldots & 1 \\ t_1 & \ldots & t_q \\ t_1^2 & \ldots & t_q^2 \end{pmatrix};$$

le code C_Ω est de longueur q et de dimension $q-3$, et la distance minimale de C est égale à 4 : ce code corrige 1 erreur. On pourrait généraliser cet exemple en utilisant le plongement d-uple de Veronèse (cf. [Ha] pour la définition).

5.8 Proposition. **Si** $2g-2 < \deg(G) < n$ **les codes** C_L **et** C_Ω **sont duaux l'un de l'autre.**

Démonstration. Si f est dans $L(G)$ et si ω est dans $\Omega(G-D)$, on a

$$(\emptyset_L(f) \mid \emptyset_\Omega(\omega)) = \Sigma \, \text{Rés}(f\omega, P) = \Sigma f(P_j) \ \text{Rés}(\omega, P_i) = 0 \ ;$$

les espaces C_L et C_Ω sont donc orthogonaux; les hypothèse faites sur $\deg(G)$ montrent que $C_L^\perp = C_\Omega$, c.q.f.d.

La matrice $G(C_L)$ est aussi la matrice de contrôle $H(C_\Omega)$ du code C_Ω. Puisque le diviseur G est positif, la fonction 1 est dans $L(G)$, le mot $(1 \ldots 1)$ est dans le code C_L, en conséquence de quoi la somme des coordonnées de chaque vecteur de C_Ω est nulle.

5.9 Définition. **Les codes** C_Ω **et** C_L **s'appellent les codes géométriques définis par le couple de diviseurs** (D,G) **de la courbe** X.

5.10 On pourrait penser a priori que la construction des codes géométriques est tout à fait particulière. On va voir qu'il n'en est rien.

Proposition. **Soit** C **un code sur** $\underline{F}_q$; **il existe alors une courbe** X **définie sur** $\underline{F}_q$ **et deux diviseurs** D **et** G **satisfaisant aux conditions de 5.2, tels que** C **soit inclus dans le code** C_L **défini par** D **et** G.

Démonstration. Soient respectivement k la dimension et n la longueur de C. On peut voir les colonnes d'une matrice génératrice de C comme des points

$Y_1,\ldots,Y_n$ de l'espace affine $\underline{A}^k(\underline{F}_q)$; il y a une courbe complète non singulière X définie sur $\underline{F}_q$, des points $P_1,\ldots,P_n$ de $X(\underline{F}_q)$ et une application rationnelle $\underline{f} = (f_1,\ldots,f_k)$ de X dans $\underline{A}^k$, tels que l'on ait $\underline{f}(P_i) = Y_i$, ce qui est possible si on accepte que le degré de $\underline{f}(X)$ soit suffisamment élevé, comme on peut le voir facilement; prenons alors $G = \text{pgcd}((f_1),\ldots,(f_k))$; on peut compléter la famille $(f_1,\ldots,f_k)$ pour obtenir une base $(f_1,\ldots,f_k, f_{k+1},\ldots,f_\ell)$ de L(G); l'application $\emptyset_L$ de **5.3** définie par les diviseurs $D = P_1+\ldots+P_n$ et G envoie alors le sous-espace V de L(G) engendré par $f_1,\ldots,f_k$ sur le code C.

5.11 En utilisant l'opération de Cartier, on peut améliorer les inégalités des propositions **5.3** et **5.6** : le résultat dépend de la suite des sauts de Weierstrass en chaque place intervenant dans le diviseur G (Michon (non publié), généralisant les résultats de Sugiyama et al. ([SKHN])).

5.12 Les codes géométriques vérifient

$$k/n + d/n \geqslant 1 + (1 - g)/n ;$$

autrement dit, avec les notations de **3.1**, on a

$$\delta(C) + R(C) \geqslant 1 + (1 - g)/n.$$

Les codes atteignant la borne de Singleton $n = k + d - 1$ sont dits **optimaux** (maximum distance séparable ou MDS en anglais). Par suite :

Corollaire. Les codes géométriques obtenus avec des courbes de genre 0 **sont optimaux.**

5.13 Prenons maintenant pour X une courbe elliptique (cf.[Dr-Mi]). Si on prend une couple (D,G) comme en **5.2**, le diviseur D s'écrit $D = \Sigma P_i$, et le diviseur G s'écrit $G = \Sigma b_i Q_i$, où les b_i sont dans $\underline{Z}$ et où les points Q_i sont dans $X(\underline{F}_q^a)$; mais le point

$$P_G = \Sigma b_i Q_i ,$$

où on effectue cette fois-ci l'addition pour la loi de groupe de X, est en fait dans $X(\underline{F}_q)$ puisque le diviseur G est rationnel sur $\underline{F}_q$. d'après la proposition **5.6** et la borne de Singleton la distance minimale du code C_Ω est égale à deg(G) ou à deg(G) + 1.

Proposition. La distance minimale de C_Ω **est** deg(G) **si on peut trouver** deg(G) **points distincts dans le support de** D **dont la somme pour la loi de groupe de** X **est égale à** P_G**; si c'est impossible le code est optimal.**

De plus, il existe un algorithme rapide qui permet de corriger d/4 erreurs pour des codes ainsi construits.

6. DESCENTE DU CORPS DE BASE

Soit m un entier $\geqslant 1$, et posons $Q = q^m$.

6.1 Descente par intersection. A partir d'un code C de type [n, k, d] sur $\underline{F}_Q$, on construit un code noté $C|\underline{F}_q$ sur $\underline{F}_q$ en posant

$$C \mid \underline{F}_q = C \cap (\underline{F}_q)^n ;$$

on a

$$\begin{aligned} \text{longueur } (C \mid \underline{F}_q) &= n \\ \text{dimension } (C \mid \underline{F}_q) &\leqslant km , \\ \text{distance } (C \mid \underline{F}_q) &\geqslant d . \end{aligned}$$

la deuxième inégalité est assez mauvaise, mais on a en fait :

Proposition. Si C_Ω est le code géométrique associé au couple (D,G) de diviseurs de la courbe X on a

$$\dim (C \mid \underline{F}_q) \geqslant n - m(\deg(G) - g(X)) - 1.$$

6.2 Soient $T = \{t_1,\ldots,t_n\}$ une partie finie de $\underline{F}_Q$ et g un polynôme de $\underline{F}_Q[X]$ qui ne s'annule pas sur T; tout élément t_i de T définit un point $P_i = (1 : t_i)$ de la droite projective $X = \underline{P}^1$; on pose

$$D = P_1 + \ldots + P_n \quad , \quad G = (g).$$

Les diviseurs D et G ainsi définis sont dans $\mathrm{Div}(X,\underline{F}_Q)$, et le couple de diviseurs (D,G) satisfait aux conditions de **5.2**, où l'on remplace $\underline{F}_q$ par $\underline{F}_Q$; l'espace $\Omega(G-D)$ s'identifie aux formes différentielles qui s'écrivent sous la forme R(z) dz sur la droite affine, où

$$R(z) = \sum_{1 \leqslant i < n} c_i/(z-t_i)$$

est une fonction dans $R(X,\underline{F}_Q)$ dont l'image dans le quotient $\underline{F}_Q[X]/(g)$ est nulle; et un élément du code géométrique C_Ω défini par D et G ne sera pas autre chose que la suite des résidus $(c_1,\ldots,c_n)$ de l'une des fonctions R(z) ci-dessus, par définition même de C_Ω; les codes $C|\underline{F}_q$ ainsi construits sur la droite projective $\underline{P}_1$ sont **les codes de Goppa classiques** (cf. [Go 1], [MW-S], [VL]); il est a souligner que de tels codes admettent un **algorithme de décodage rapide** (cf. [Go 2]), basé sur l'algorithme de Berlekamp.

6.3 Voici un autre exemple de descente par intersection, qui permet d'obtenir une nouvelle présentation, due à Michon, des **codes BCH** (pour R.C.Bose, D.K.Ray-Chaudhury et A.Hocquenghem) : soient n un entier > 0, m le plus petit entier > 0 tel que $n|q^m - 1$, et $Q = q^m$; notons $\underline{C}$ la famille des codes géométriques C_L ou C_Ω sur $\underline{F}_Q$, avec $X = \underline{P}^1$, associés au couple (D,G) de diviseurs suivants sur X :

$$D = \Sigma_{P \in M} (P),$$

où M est un sous-groupe d'ordre n de $\underline{F}_Q{}^*$, et

$$G = A.(0) + B(\infty),$$

avec des entiers naturels A et B convenablement choisis. Les codes BCH sont

les codes $(C|\underline{F}_q)$, où C parcourt $\underline{C}$. Lorsque n = q-1, il n'y a pas de descente à faire et on obtient ainsi les **codes de Reed-Solomon**, qui sont donc optimaux, vu **5.8.**

Il convient de signaler ici que la famille des codes BCH n'est pas une bonne famille de codes au sens de **4.1** (cf. [MW-S], p.269); ils sont néanmoins fréquemment utilisés dans l'industrie.

6.4 Descente par trace . La trace est une application linéaire surjective :

$$T_m : \underline{F}_Q \longrightarrow \underline{F}_q ;$$

Si C est un code de type n, k, d , l'image $T_m(C)$ est un code de paramètres

$$\text{longueur } T_m(C) = n ,$$
$$\text{dimension } T_m(C) \leqslant km ,$$
$$\text{distance } T_m(C) \geqslant d .$$

La descente par trace est duale de la descente par intersection; on a en effet :

$$(C \mid \underline{F}_q) = T_m(C^{\perp}).$$

Ce résultat est dû à Delsarte ; cf. [MW-S], p.208 .

6.5 Descente par changement de base. En prenant une base de $\underline{F}_Q$ sur $\underline{F}_q$, on obtient un isomomorphisme de $\underline{F}_Q$ sur $\underline{F}_q^m$, puis un isomorphisme de changement de base :

$$R_m : \underline{F}_Q^n \longrightarrow \underline{F}_q^{mn}.$$

Tout code C sur $\underline{F}_Q$ définit donc un code $R_m(C)$ sur $\underline{F}_q$.

6.6 Soit maintenant X une courbe algébrique définie sur $\underline{F}_q$. Un procédé de construction de codes est le suivant :

a) on construit un code C_Ω sur $\underline{F}_Q$ associé à un couple (D_m, G_m) de diviseurs sur X comme en **5.2** mais on demande seulement que les diviseurs D_m et G_m appartiennent à $\mathrm{Div}(X, \underline{F}_Q)$.

b) on prend le code $R_m(C_\Omega)$ obtenu par changement de base de $\underline{F}_Q$ à $\underline{F}_q$.

Comme illustration de ce procédé, prenons pour X la droite projective $\underline{P}^1$, pour D_m le diviseur somme des $q^m - 1$ points à distance finie de $\underline{P}^1(\underline{F}_Q)$, et pour G_m le diviseur (0) - (∞); le code $R_m(C_\Omega)$ obtenu est le **code de Hamming d'indice** m.

L'ensemble des codes sur $\underline{F}_q$ obtenus en faisant varier le couple (D_m, G_m), puis l'entier m est la famille des codes géométriques construits sur X étendue par changement de base.

7. PERFORMANCES DES CODES GÉOMETRIQUES

7.1 En utilisant le modèle algébrique, Goppa (cf.[GO 4], §7) a établi le résultat suivant :

THÉORÈME. **La famille des codes linéaires est une famille de Shannon.**

Plus précisément, il a montré que pour toute courbe X, la famille des codes géométriques construits sur X étendue par changement de base est une famille de Shannon. Ce résultat montre que la famille des codes géométriques est très performante : on va préciser cette assertion.

7.2 Soit X une courbe algébrique comme en **5.1**, et posons

$$X(\underline{F}_q) = \{P_1,\dots,P_n\} \quad , \quad N_Q(X) = \mathrm{Card}(X(\underline{F}_q)) = n \ ;$$

comme cas particulier de couple (D,G), prenons

$$D = P_1 + \dots + P_{n-1} \quad , \quad G = BP_n \ ,$$

où B est un entier positif avec $2g - 2 < B < n + g - 1$; vu **5.7**, le code C_Ω correspondant a pour dimension et pour distance :

$$k_\Omega \geqslant N_q(X) - B + g - 2 \ ,$$
$$d_\Omega \geqslant B - 2g + 2 \ ;$$
$$n_\Omega = N_q(X) - 1 \ ;$$

en posant

$$S_q(X) = (g-1)/(N_q(X) - 1) \ ,$$
$$b = B/(N_q(X) - 1) \ ,$$

de telle sorte que $2S_q(X) < b < 1 + S_q(X)$, il vient

$$R_\Omega \geqslant 1 + S_q(X) - b,$$
$$\delta_\Omega \geqslant b - 2S_q(X) \ .$$

On pose

$$N_q(g) = \mathrm{Max}\ N_q(X),$$

lorsque X parcourt l'ensemble fini des courbes de genre g définies sur $\underline{F}_q$, et

$$S(q) = \liminf g/N_q(g) \ ,$$

pour g tendant vers l'infini (q étant fixé). Il n'est pas évident que l'on ait $S(q) < \infty$; cf. **9.4.** En attendant supposons $S(q) < 1$, soit $(X_i)_{i\geqslant 0}$ une famille de courbes telle que $S_q(X_i)$ tende vers S(q), et prenons sur les courbes X_i des diviseurs $G_i = B_i P_n$ avec $B_i/(N_q(X) - 1)$ tendant vers b ; la famille de codes correspondante aura des paramètres qui tendront vers

$$R = 1 + S(q) - b \quad , \quad \delta = b - 2S(q) \ ;$$

dans ce qui précède, on peut choisir b arbitrairement, pourvu que $2S(q) < b < 1 + S(q)$; on a démontré le

THÉORÈME (Tsfasman). **L'intersection de la droite**

$$R + \delta = 1 - S(q),$$

avec le carré $[0, 1]\times[0, 1]$ **est incluse dans le domaine des codes** U_q.

Remarquons que cette intersection est non vide si et seulement si $S(q) \leqslant 1$.

7.3 Le théorème précédent montre que toute majoration

$$S(q) \leqslant S_0(q)$$

donne une minoration de a_q , i.e.

$$a_q(\delta) \geqslant 1 - S_0(q) - \delta \ ;$$

si

$$S_0(q) \leqslant \log_q((2q-1)/q),$$

cette minoration est meilleure que la borne de Varshamov-Gilbert, vu **4.7**, et on aura donc trouvé d'excellentes familles de codes au sens de **4.6.** Ainsi, il résulte du théorème **8.3** ci-dessous que l'on a

$$S(q) = 1/(q^{\frac{1}{2}} - 1) \quad \text{si } q \text{ est un carré ;}$$

par conséquent :

THÉORÈME. **Il existe des familles de codes pour** q **carré et** $q \geqslant 49$ **qui dépassent la borne de Varshamov-Gilbert.**

Par une autre méthode, et pour q quelconque, Goppa a établi que la famille des codes géométriques étendue par intersection atteignait cette même borne (cf.[GO 4], §7).

7.4 On peut préciser le résultat précédent : on dit qu'un code a une **construction polynômiale** s'il y a un algorithme pour construire le code (par exemple pour construire la matrice génératrice) qui est de complexité polynômiale en la longueur n. Katsman, Manin, Tsfasman et Vladut (cf. [K-T-V] et [Ma-Vl]) ont obtenu le résultat suivant en utilisant les courbes modulaires de Drinfeld :

THÉORÈME. **Si** q **est un carré et si** $q \geqslant 49$**, il existe des familles de codes géométriques qui ont une construction polynômiale et qui dépassent la borne de Varshamov-Gilbert.**

Par contre, le problème du décodage pour des codes construits sur des courbes de genre élevé reste ouvert. Si C est un code quelconque de type [n, k, d] sur $\underline{F}_q$, la méthode de décodage indiquée en **2.5** impose le stockage d'une table de q^{n-k} erreurs possibles; en fait, on peut montrer que le problème du décodage de tous les codes de type [n, k, d] sur $\underline{F}_q$ est **NP-complet.**

7.5 Dans le sens inverse de **7.3**, toute borne supérieure $a_q(\delta) \leqslant a_q^0(\delta)$ donne une borne inférieure pour S(q); si la droite d'équation

$$R + \delta = 1 - S_1(q)$$

est tangente à la courbe d'équation $R = a_q^0(\delta)$, on aura

$$S(q) \geqslant S_1(q) \ ;$$

ainsi on déduit de la borne de Plotkin **4.5** que l'on a $S(q) \geqslant q^{-1}$, en particulier

$$S(2) \geqslant 1/2 \quad , \quad S(3) \geqslant 1/3 \ ,$$

et on déduit de **4.8** que l'on a

$$S(2) \geqslant 0,525\ldots$$

8. LE NOMBRE A(q)

On pose

$$A(q) = \text{lim. sup } N_q(g)/g = S(q)^{-1} .$$

8.1 L'inégalité de Weil s'écrit :

$$|\text{Card}(X(\underline{F}_q)) - (q+1)| \leqslant 2g(X)\, q^{\frac{1}{2}} .$$

On trouvera dans [Bo] une démonstration de cette inégalité par la méthode de Stepanov, qui est basée essentiellement sur le théorème de Riemann-Roch.

On en déduit :

$$N_q(g)/g \leqslant 2\, q^{\frac{1}{2}} ;$$

par suite

$$A(q) \leqslant 2\, q^{\frac{1}{2}} .$$

8.2 En fait, Serre (cf. [Se 2], [Se 3], [Se 4]) a montré qu'on peut améliorer l'inégalité de Weil :

$$|\ \text{Card}\ X(\underline{F}_q) - (q+1)| \leqslant g(X)\ [2\, q^{\frac{1}{2}}] ,$$

d'où

$$A(q) \leqslant [2\, q^{\frac{1}{2}}] .$$

On trouvera dans Serre (loc. cit.), de nombreux autres résultats sur les valeurs des nombres $N_q(g)$, ainsi que des tables.

8.3 THÉORÈME. a) **on a**

$$A(q) \leqslant q^{\frac{1}{2}} - 1 ;$$

b) **si** q **est un carré on a**

$$A(q) = q^{\frac{1}{2}} - 1 .$$

La partie a) a été démontrée par Drinfeld et Vladut (cf. [Dr-Vl]). La démonstration de la partie b) s'est faite en plusieurs étapes. En utilisant des familles de courbes modulaires ou de courbes de Shimura "réduites modulo q", Ihara (cf. [Ih]), puis indépendamment Tsfasman, Vladut et Zink (cf. [Ts-Vl-Zi]), ont établi que si q est un carré, on a

$$A(q) \geqslant q^{\frac{1}{2}} - 1 ;$$

ce qui implique le théorème, avec le résultat de a). Signalons à ce propos que Manin et Vladut (cf. [Ma-Vl]) utilisent des familles (X_i) de modules de Drinfeld pour lesquelles on a

$$\lim_{i\,\infty} N(X_i)/g(X_i) = q^{\frac{1}{2}} - 1 .$$

Par exemple, pour q = 2, la borne de Weil **8.1** donne $A(2) \leqslant 2\sqrt{2} = 2{,}828\ldots$; la borne de Serre **8.2** et la borne de Plotkin **7.4** donnent $A(2) \leqslant 2$; la deuxième borne obtenue en **7.4** donne $A(2) \leqslant 1{,}904\ldots$, et la borne de Drinfeld-Vladut **8.3** donne $A(2) \leqslant \sqrt{2}-1 = 0{,}414\ldots$

8.4 Lorsque q n'est pas un carré, on n'a pas encore de minoration de A(q) comme en (8.3); le seul résultat dont on dispose est le suivant :

THÉORÈME. (Serre). **On a**

$$A(q) > 0 \ ;$$

plus précisément, on a

$$A(2) \geqslant 8/39 = 0{,}205\ldots$$

$$A(q) \geqslant c \log q \ ,$$

avec une constante absolue $c > 0$.

Ce théorème se démontre par une construction de tours de corps de classes.

BIBLIOGRAPHIE

1. Livres de géométrie algébrique

[Ch] CHEVALLEY,C., Introduction to the theory of algebraic functions of one variable, Math. Surveys, VI, Providence, A.M.S., 1951

[Ha] HARTSHORNE,R., Algebraic Geometry, Graduate texts in Math., n°52, Springer, New York, 1977

[Lan] LANG,S., Introduction to Algebraic and Abelian functions, 2d ed., Graduate texts in Math., n°89, Springer, New York, 1982

[Se 1] SERRE, J.P., Groupes algébriques et corps de classes, A.S.I. 1254, Pub. Math. Univ. Nancago VII, Hermann, Paris, 1959

[Sh] SHAFAREVICH,I.R., Basic Algebraic Geometry, Springer, Berlin, 1977

[We] WEIL,A., Basic Number Theory, 3rd edition, Grund. der Math. Wiss., Bd.144, Springer, New York, 1974.

2. Livres sur la théorie des codes

[Bl] BLAKE,I.F., Algebraic coding Theory : History and Development, Dowden, Hutchinson & Ross, Stroudsburg, 1973

[ME] McELIECE,R.J., The theory of information and coding, Encyclopedia of Math., vol.3, Reading, Addison-Wesley, 1977

[MW-S] MACWILLIAMS,F.J., SLOANE,N.J.A., The theory of Error-Correcting codes, North-Holland, Amsterdam, 1977

[VL] Van LINT,J.H., Introduction to Coding Theory, Graduate texts in Math. 86, Springer, Berlin, 1982.

3. Articles sur les courbes algébriques

[Bo] BOMBIERI,E., Counting points on curves over finite fields (d'après S.A. Stepanov), Séminaire BOURBAKI, 25e année, 1972/73, n°430, Lect.Notes in Math. n°383, Springer, 1974

[Ih] IHARA,Y., Some remarks on the number of rational points of algebraic curves over finite fields, J.Fac.Sci. Univ. Tokyo, I A, 28 (1981), 721-724

[Laz] LAZARD,D., Primitives des fonctions élémentaires (d'après Risch et Davenport), Séminaire BOURBAKI, 36e annnée, 1983/84, n°627, Astérisque, S.M.F., Paris, 1984

[Se 2] SERRE,J.P., Sur le nombre des point rationnels d'une courbe algébrique sur un corps fini, C.R.Acad.Sc. Paris, 296, (1983), 397-402

[Se 3] SERRE,J.P., Nombre de points des courbes algébriques sur F_q, Sém.Th. Nombres, Bordeaux, (1982-1983), exp.n°22

[Se 4] SERRE,J.P., Résumé du cours de l'année 1984/1984, Annuaire du Collège de France, Paris, 1985

[Ta] TATE,J., Residues of differentials on curves, Ann.Sc. Ec.Norm.Sup. (4), 1 (1966), 149-159.

4. Articles sur la théorie des codes

[Br] BROUÉ,M., Codes Correcteurs d'Erreurs Auto-orthogonaux sur le Corps à Deux Eléments et Formes Quadratiques Entières Définies Positives à discriminant + 1, Discrete Math.17 (1977), 247-269

[Ch-Hs] CHEN,C.L., HSIAO,M.V., Error-Correcting Codes for Semiconductor Memory, I.B.M. J.Res. Develop.28 (1984), 124-134

[De-Pi] DELSARTE,P., PIRET,P., Algebraic constructions of Shannon codes for regular channels, I.E.E.E. Trans. Inf. Theory 28 (1982), 593-599

[Dr-Mi] DRIENCOURT,Y., MICHON,J.F., Binary Elliptic codes, prépublication, A.T.P. 399 du C.N.R.S.

[Go 1] GOPPA,V.D., A Rational Representation of Codes and (L,g)-Codes, Problemy Peredachi Informatsii 3 (1971), 41-49 ; = Probl. Inform. Transmission 3 (1971), 223-229

[Go 2] GOPPA,V.D., Decoding and Diophantine approximation, Problemy Uprav. i Teor. Informatsii 5 (1976), 195-206; = Problems of Control and Information Theory 5 (1976), 1-12

[Go 3] GOPPA,V.D., Codes on algebraic curves, Dokl. Akad. Nauk, S.S.S.R., 259 (1981), 1289-1290, = Soviet Math. Dokl. 24 (1981), 170-172

[Go 4] GOPPA,V.D., Algebraico-Geometric Codes, Izv. Akad. Nauk, S.S.S.R., 46 (1982); = Math. U.S.S.R. Izvestiya 21 (1983), 75-91

[K-T-V] KATSMAN,G.L., TSFASMAN,M.A., VLADUT,S.G., Modular Curves and Codes with a polynomial construction, I.E.E.E. Trans. Inf. Theory, 30 (1984), 353-355

[Ma] MANIN,Yu.I., What is the maximum number of points on a curve over F_2 ? , J.Fac.Sci. Univ. Tokyo,I A, 28, (1981), 715-720

[Ma-Vl] MANIN,Yu.I., VLADUT,S.G., Codes linéaires et courbes modulaires (en russe), Sovr. Prob. Mat., VINITI, Moscou, 1984

[Mi] MICHON,J.F., Les codes Géométriques de V.D.Goppa, Sém. Th. Nombres Bordeaux (1983-1984)

[SKHN] SUGIYAMA,Y., KASAHARA,M., HIRASAWA,S., NAMEKAWA,T., Further results on Goppa codes and their applications to constructing efficient binary codes, I.E.E.E. trans. Inf. Theory 22 (1976), 518-525

[Ts] TSFASMAN,M.A., Goppa codes that are better than Varshamov-Gilbert bound, Prob. Peredachi Inform. 18 (1982), 3-6 ; = Probl. Inform. Transmission, 18 (1982), 163-166

[Ts-Vl-Zi] TSFASMAN,M.A., VLADUT,S.G., ZINK,Th., Modular Curves, Shimura Curves, and Goppa codes, better than Varshamov-Gilbert bound, Math. Nachr. 109 (1982), 21-28

[Vl-Dr] VLADUT,S.G., DRINFELD,V.G., Number of Points of an Algebraic Curve, Funktsional'-nyi Analiz i Ego Prilozhenia 17 (1983), 68-69; = Functional Analysis, 17 (1983), 53-54.

Gilles LACHAUD
L.A. 168 du C.N.R.S.
& Eq. Rech. Hist. Sc
Université de Nice
Parc Valrose
F-06034 NICE CEDEX