Journées mathématiques X-UPS

Année 1993

Codes géométriques algébriques et arithmétique sur les corps finis

Mireille MARTIN-DESCHAMPS

Codes géométriques

Journées mathématiques X-UPS (1993), p. 1-9.
https://doi.org/10.5802/xups.1993-01

Les Éditions de l'École polytechnique
Route de Saclay
F-91128 PALAISEAU CEDEX
https://www.editions.polytechnique.fr

Centre de mathématiques Laurent Schwartz
CMLS, École polytechnique, CNRS,
Institut polytechnique de Paris
F-91128 PALAISEAU CEDEX
https://portail.polytechnique.edu/cmls/

Publication membre du
Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org

Journées mathématiques X-UPS
1993, p. 1–9 doi: 10.5802/xups.1993-01

CODES GÉOMÉTRIQUES

par

Mireille Martin-Deschamps

Table des matières

Les théorèmes généraux de théorie des codes qui ont été montrés par Shannon assurent l'existence de codes très performants (en ce sens qu'ils atteignent la borne de Varshamov-Gilbert

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

où R et δ sont les paramètres asymptotiques du code).

Malheureusement, ces théorèmes ne fournissent aucune indication sur la manière effective de construire de tels codes. Un pas important dans cette direction a été fait avec la construction des codes géométriques, construction qui utilise les objets et les méthodes de la géométrie algébrique, et qui permet de retrouver les résultats prédits par la théorie.

Publication originelle dans Journées X-UPS 1993. Codes géométriques algébriques et arithmétique sur les corps finis. Prépublication du Centre de mathématique de l'École polytechnique, 1993.

1. Exemple : Code de Reed-Solomon sur $\mathbb{F}_q$, $q = p^m$

On note $(0, \alpha_1, \ldots, \alpha_{q-1})$ les éléments de $\mathbb{F}_q$. Par exemple, si α est un élément primitif, on pourra choisir $\alpha_i = \alpha^{i-1}$ pour $i = 1, \ldots, q-1$.

Soit δ un entier compris entre 2 et $q-1$. Le code de Reed-Solomon sur $\mathbb{F}_q$ de paramètre δ est défini par la matrice de contrôle de parité :

$$H = \begin{pmatrix} \alpha_1 & \cdots & \alpha_{q-1} \\ \vdots & & \vdots \\ \alpha_1^{\delta-1} & \cdots & \alpha_{q-1}^{\delta-1} \end{pmatrix}$$

Autrement dit, les mots du code sont les $q-1$-uples $(a_1, \ldots, a_{q-1})$ de $\mathbb{F}_q^{q-1}$ tels que

$$\sum_{i=1}^{q-1} \alpha_i^j a_i = 0$$

pour $j = 1, \ldots, \delta - 1$. C'est un code de longueur $n = q - 1$, de dimension $k = n - \delta + 1$.

Un encodeur peut être défini de la manière suivante : on considère l'espace vectoriel $\mathbb{F}_q[x]_{k-1}$ des polynômes en une variable de degré $\leqslant k-1$ sur $\mathbb{F}_q$, et l'application linéaire d'« évaluation : »

$$\begin{aligned} \mathbb{F}_q[x]_{k-1} &\longrightarrow \mathbb{F}_q^n \qquad n = q-1 \\ f &\longmapsto (f(\alpha_1), \ldots, f(\alpha_n)). \end{aligned}$$

En effet, on vérifie que c'est une injection, que l'image est contenue dans le code, donc lui est égale pour des raisons de dimension. On peut alors calculer facilement la distance minimale d : un polynôme de degré $\leqslant k-1$ ayant au plus $(k-1)$ zéros, le poids d'un mot du code est $\geqslant n - k + 1 = \delta$, donc on a : $d = \delta$.

Remarque. Ces codes sont effectivement utilisés dans la pratique, par exemple on utilise un Reed-Solomon sur $\mathbb{F}_{64}$ pour corriger les informations contenues dans les disques numériques audio.

Afin de généraliser cette construction, on va en donner une interprétation un peu différente :

Soit $X = \mathbb{P}^1_{\mathbb{F}_q}$ la droite projective sur $\mathbb{F}_q$. On peut regarder $(\alpha_1, \ldots, \alpha_{q-1})$ non plus comme des éléments de $\mathbb{F}_q$, mais comme des

points rationnels de X. On note $P_i = (\alpha_i, 1)$ pour $i = 1, \ldots, q-1$ et $P_\infty = (1, 0)$.

Un polynôme de $\mathbb{F}_q[x]$ définit une fonction rationnelle sur X, ayant en P_∞ un pôle d'ordre égal à son degré. En particulier, on identifie ainsi l'ensemble $\mathbb{F}_q[x]_{k-1} - \{0\}$ avec l'ensemble des fonctions rationnelles f non nulles sur X telles que le diviseur $(f) + (k-1)P_\infty$ soit positif. Autrement dit, on a un isomorphisme linéaire :

$$\mathbb{F}_q[x]_{k-1} \xrightarrow{\sim} H^0(X, \mathcal{O}_X((k-1)P_\infty)).$$

On va alors pouvoir définir les codes géométriques.

2. Codes géométriques de Goppa

Soient X une courbe lisse et projective sur $\mathbb{F}_q$, de genre g, (D, G) un couple de diviseurs sur X satisfaisant les conditions suivantes :

$$(*) \quad \begin{cases} D = P_1 + \cdots + P_n \quad \text{où } P_1, \ldots, P_n \text{ sont} \\ \qquad\qquad\qquad\qquad\qquad n \text{ points distincts de } X(\mathbb{F}_q) \\ G > 0 \\ \operatorname{Supp} D \cap \operatorname{Supp} G = \varnothing. \end{cases}$$

On considère l'application linéaire d'« évaluation » :

$$\begin{aligned} H^0(X, \mathcal{O}_X(G)) &\xrightarrow{\varphi} \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \ldots, f(P_n)). \end{aligned}$$

Elle est bien définie car toute fonction rationnelle $f \neq 0$ qui vérifie $(f) + G \geqslant 0$ n'a pas de pôle en $P_1, \ldots, P_n$. L'image de φ est un code sur $\mathbb{F}_q$, noté C_L, dont on va calculer les paramètres asymptotiques en utilisant des résultats de géométrie algébrique.

Proposition 2.1. *Soit $[n, k, d]$ le type de C_L. Si $\deg G < n$, on a :*

- $k \geqslant \deg G + 1 - g$ *avec égalité si* $\deg G > 2g - 2$,
- $d \geqslant n - \deg G$.

Démonstration. Soit $f \neq 0$ qui vérifie les conditions :

$$(f) + G \geqslant 0 \qquad f(P_i) = 0 \qquad i = 1, \ldots, n.$$

Alors, puisque les supports de D et G sont distincts, on a aussi

$$(f) + G - D \geqslant 0 \quad \text{donc} \quad \deg G \geqslant \deg D = n$$

donc si on a $\deg G < n$, φ est injective.

D'après le théorème de Riemann-Roch, on a :

$$h^0(\mathcal{O}_X(G)) = \deg G + 1 - g + h^0(\omega_X \otimes \mathcal{O}_X(-G))$$

où ω_X est le faisceau des formes différentielles sur X,

$$\deg(\omega_X \otimes \mathcal{O}_X(-G)) = 2g - 2 - \deg G$$

d'où l'assertion sur k.

Soit $f \neq 0$, $f \in H^0(\mathcal{O}_X(G))$, et $w(f)$ le poids de $\varphi(f)$. Il existe des indices $i_1, \ldots, i_{n-w(f)}$ tels que :

$$f(P_{i_1}) = \cdots = f(P_{i_{n-w(f)}}) = 0$$

donc le diviseur $(f) + G - (P_{i_1} + \cdots + P_{i_{n-w(f)}})$ est $\geqslant 0$, ainsi que son degré, d'où :

$$\begin{aligned} \deg G &\geqslant n - w(f), \\ w(f) &\geqslant n - \deg G. \end{aligned}$$

Pour obtenir une matrice génératrice, on choisit une base $(f_1, \ldots, f_\ell)$ de $H^0(\mathcal{O}_X(G))$, et on obtient :

$$\begin{pmatrix} f_1(P_1) & \cdots & f_1(P_n) \\ \vdots & & \vdots \\ f_\ell(P_1) & \cdots & f_\ell(P_n) \end{pmatrix}. \qquad \square$$

Exemple. Code sur la cubique d'équation :

$$X^3 + Y^3 + Z^3 = 0 \quad \text{sur} \quad \mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}.$$

Elle est lisse de genre 1, elle a 9 points rationnels, dont 3 à l'infini.

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9
X	0	0	0	α^2	α	1	α^2	α	1
Y	α^2	α	1	0	0	0	1	1	1
Z	1	1	1	1	1	1	0	0	0

On considère alors les diviseurs :

$$D = P_1 + \cdots + P_8,$$
$$G = 3P_9.$$

Puisque $0 < \deg G < 8$, on a $h^0(\mathcal{O}_X(G)) = 3$, donc il faut trouver 3 éléments indépendants de $H^0(\mathcal{O}_X(G))$. On choisit

$$\begin{aligned} f &= 1 && (f) = 0 \\ g &= \frac{X}{X+Y} && (g) = P_1 + P_2 + P_3 - 3P_9 \\ h &= \frac{X}{X+Y} && (h) = P_1 + P_2 + P_3 - 3P_9. \end{aligned}$$

On obtient alors la matrice génératrice :

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \alpha & \alpha^2 & 1 & \alpha & \alpha^2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & \alpha & \alpha^2 \end{pmatrix}$$

C'est un code de type [8,3,5] sur $\mathbb{F}_4$.

Remarque. La courbe elliptique considérée est un cas particulier de « courbe d'Hermite » sur $\mathbb{F}_q$. Lorsque q est un carré et $d = \sqrt{q} + 1$, la courbe d'Hermite est la courbe X d'équation : $X^d + Y^d + Z^d = 0$. C'est une courbe lisse de genre

$$g = \frac{(d-1)(d-2)}{2} = \frac{q - \sqrt{q}}{2}.$$

Il est facile de voir qu'une telle courbe a $q\sqrt{q} + 1$ points rationnels, donc qu'elle atteint la borne de Weil :

$$\#X(\mathbb{F}_q) \leqslant q + 1 + 2g\sqrt{q}.$$

Il existe une deuxième manière d'associer à un couple de diviseurs (D, G) qui vérifie les conditions $(*)$ un code linéaire sur $\mathbb{F}_q$. On considère l'application linéaire « résidu » :

$$\begin{aligned} H^0(\omega_X \otimes \mathcal{O}_X(D-G)) &\xrightarrow{\psi} \mathbb{F}_q^n \\ \omega &\longmapsto (\mathrm{Rés}_{P_1}(\omega), \ldots, \mathrm{Rés}_{P_n}(\omega)). \end{aligned}$$

L'image de ψ est un code sur $\mathbb{F}_q$, noté C_Ω.

Proposition 2.2. *Soit $[n, k', d']$ le type de C_Ω. Si $2g-2 < \deg G$, on a :*

- $k' \geqslant n - \deg G - 1 + g$ *avec égalité si* $\deg G < n$,
- $d' \geqslant \deg G - 2g + 2$.

Démonstration. Soit $\omega \neq 0$ qui vérifie les conditions :

$$(\omega) + D - G \geqslant 0 \quad \text{et} \quad \text{Rés}_{P_i}\,\omega = 0 \qquad i - 1, \ldots, n.$$

Alors ω n'a pas de pôle en $P_1, \ldots, P_n$, donc on a aussi :

$$(\omega) - G \geqslant 0 \quad \text{et} \quad \deg G \leqslant 2g - 2.$$

Donc si on a $\deg G > 2g - 2$, ψ est injective.

D'après le théorème de Riemann-Roch, on a :

$$h^0(\omega_X \otimes \mathcal{O}_X(D - G)) = -\deg(G - D) + g - 1 + h^0(\mathcal{O}_X(G - D)),$$

d'où l'assertion sur k'.

Enfin, soit $\omega \neq 0$, $\omega \in H^0(\omega_X \otimes \mathcal{O}_X(D - G))$ et $w(\omega)$ le poids de $\psi(\omega)$. Il existe des indices $i_1, \ldots, i_{w(\omega)}$ tels que le diviseur $(\omega) + P_{i_1} + \cdots + P_{i_{w(\omega)}} - G$ soit positif ainsi que son degré, d'où :

$$w(\omega) \geqslant \deg G + 2 - 2g. \qquad \square$$

Le fait que les démonstrations de ces deux propositions soient très voisines n'est pas étonnant, car ces deux codes sont liés. Plus précisément, on a le résultat suivant :

Proposition 2.3. *Si $2g-2 < \deg G < n$, les codes C_L et C_Ω sont duaux l'un de l'autre.*

Démonstration. Soit $f \in H^0(\mathcal{O}_X(G))$, $\omega \in H^0(\omega_X \otimes \mathcal{O}_X(D - G))$, alors

$$f\omega \in H^0(\omega_X \otimes \mathcal{O}_X(D))$$

donc les pôles de $f\omega$ sont contenus dans le support de D. Mais on a :

$$(\varphi(f) \mid \psi(\omega)) = \sum_{i=1}^{n} f(P_i)\,\text{Rés}_{P_i}\,\omega = \sum_{i=1}^{n} \text{Rés}_{P_i}(f\omega) = 0$$

d'après la formule des résidus. Donc C_L et C_Ω sont orthogonaux. Dans le cas $2g - 2 < \deg G < n$, pour des raisons de dimension, C_Ω *est* l'orthogonal de C_L. $\square$

Definition. C_L et C_Ω sont les codes géométriques définis par le couple de diviseurs (D, G).

Remarques

(1) La dualité entre C_L et C_Ω est une traduction de la dualité de Serre sur X.

(2) Actuellement, on étudie plutôt les codes C_L. Historiquement, les codes C_Ω ont été construits d'abord, sans doute parce que Goppa, qui les a inventés, n'est pas à l'origine un géomètre, ni un algébriste. La définition de C_Ω pose moins de problèmes que celle de C_L, car le résidu d'une forme différentielle existe toujours, alors qu'il n'en est pas de même de la valeur d'une fonction rationnelle, et il faut des outils algébriques pour contrôler les domaines de définition des fonctions rationnelles.

3. Applications

On dispose maintenant d'une nouvelle famille très vaste de codes linéaires. Les problèmes qui les concernent se ramènent à des problèmes d'arithmétique et de géométrie algébrique (arithmétique en ce qui concerne les points rationnels d'une courbe sur un corps fini, géométrique pour la construction des systèmes linéaires de diviseurs).

Nous allons montrer que la famille des codes géométriques a de bonnes propriétés asymptotiques.

Soit X une courbe projective et lisse de genre g sur $\mathbb{F}_q$, C_L un code obtenu en considérant un couple (D, G) tel que D contienne tous les points rationnels de $X(\mathbb{F}_q)$, $[n, k, d]$ son type. On a :

- $k \geqslant \deg G + 1 - g$,
- $d \geqslant n - \deg G$,

d'où

$$\frac{k}{n} + \frac{d}{n} \geqslant 1 + \frac{1-g}{n}$$

avec $n = \#X(\mathbb{F}_q) = N_q(x)$.

On pose alors

$$N_q(g) = \max\{N_q(X) \mid X \text{ proj. lisse, genre } g \text{ sur } \mathbb{F}_q\},$$

$$A(q) = \limsup \frac{N_q(g)}{g}.$$

On veut borner $A(q)$. Pour cela, on peut utiliser la borne de Weil :

$$|N_q(x) - (q+1)| \leqslant 2g\sqrt{q}$$

et on obtient $A(q) \leqslant 2\sqrt{q}$.

Mais cette borne peut être améliorée :

Théorème. *On a $A(q) \leqslant \sqrt{q} - 1$. De plus, si q est un carré, on a $A(q) = \sqrt{q} - 1$.*

L'inégalité a été montrée par Drinfeld et Vladut. L'égalité a été prouvée par Ihara, puis indépendamment par Tsfasman, Vladut et Zink, qui en ont aussi déduit, en utilisant des courbes modulaires, qu'il existe une famille de codes géométriques sur $\mathbb{F}_q$ ayant une complexité polynomiale de construction et dépassant la borne de Varshamov-Gilbert, si q est un carré $\geqslant 49$.

4. Généralisation

Cette construction peut être étendue à des variétés algébriques de dimension supérieure. Pour le moment, ces techniques n'ont pas permis de construire de « meilleurs » codes que sur les courbes, mais on a pu dans certains cas, donner ainsi une interprétation géométrique de codes déjà connus. C'est le cas des codes de Reed-Muller :

Codes de Reed-Muller projectifs. Soit $X = \mathbb{P}^r$ l'espace projectif de dimension r sur $\mathbb{F}_q$. Soient V l'ensemble des points rationnels de X, et N son cardinal. On note U_i l'ouvert de X défini par $X_i \neq 0$. On obtient ainsi un recouvrement ouvert de X : $X = \bigcup_{i=0}^{r} U_i$. On a :

$$\begin{aligned} N = \#X &= \#U_0 + \#(U_1 - U_0) + \cdots + \#\Big(U_r - \bigcup_{i=0}^{r-1} U_i\Big) \\ &= q^r + q^{r-1} + \cdots + 1 \\ &= \frac{q^{r+1} - 1}{q - 1}. \end{aligned}$$

Soit $\mathcal{L} = \mathcal{O}_P(1)$ le faisceau inversible correspondant aux diviseurs hyperplans.

Pour $m \geqslant 1$, les sections globales de $\mathcal{L}^m$ s'identifient aux polynômes homogènes de degré m en $X_0, \ldots, X_r$.

Pour tout point x de V, on peut définir une application linéaire d'évaluation en x $\varphi_x : H^0(X, \mathcal{L}^m) \to \mathbb{F}_q$ de la manière suivante :

Si $x \in U_0$, $\varphi_x(f) = f(x)/x_0^m$
Si $x \in U_1 - U_0$, $\varphi_x(f) = f(x)/x_1^m$
Si $x \in U_2 - (U_1 \cup U_0)$, $\varphi_x(f) = f(x)/x_2^m$
...

On a alors une application linéaire d'évaluation :

$$\begin{aligned} H^0(X, \mathcal{L}^m) &\xrightarrow{\psi} \mathbb{F}_q^N \\ f &\longmapsto (\varphi_{x_1}(f), \ldots, \varphi_{x_N}(f)) \end{aligned}$$

dont l'image est un code de Reed-Muller projectif.

On montre par récurrence sur r, que φ est une injection si $m < q$. Dans ce cas, puisqu'un polynôme homogène a au plus $m(q^r-1)/(q-1)$ zéros dans $\mathbb{P}^r(\mathbb{F}_q)$, les paramètres du code sont les suivants :

$$\begin{cases} n &= \dfrac{q^{r+1}-1}{q-1} \\ k &= \dbinom{r+m}{r} \\ d &\geqslant \dfrac{q^{r+1}-1-m(q^r-1)}{q-1} \quad \text{avec égalité quand } m = 1. \end{cases}$$

Mireille Martin-Deschamps, URA 762 du C.N.R.S., Département de Mathématiques et Informatique, Ecole Normale Supérieure, 45, rue d'Ulm, 75005 Paris, France