UNIVERSITÉ DE LIMOGES, 2008-09
IREM, IUFM DU LIMOUSIN
Formation continue second degré **Mathématiques actuelles**

Borne de SERRE et codes de REED-MÜLLER projectifs

Stéphane VINATIER

Soit $d \geq 2$ un entier, quel est l'arrangement de d droites du plan sans parallèles qui a « le plus grand nombre de points », autrement dit le moins de points d'intersection, ceux-ci étant comptés autant de fois qu'il y a de droites passant par le point moins 1 ? Plus généralement, quel est l'arrangement de d hyperplans d'un espace affine sans parallèles qui a « le plus grand nombre de points », autrement dit « la plus petite intersection » ? L'hypersurface de degré d qui a « le plus grand nombre de points » ?

Nous allons dans ce qui suit donner un sens précis à ces questions, une réponse (et sa preuve !) à chacune — c'est la borne de SERRE[1], et voir comment elles interviennent dans un problème « pratique » de théorie des codes. C'est d'ailleurs de là qu'elles viennent : lors des *Journées Arithmétiques* de Luminy en 1989 (rassemblement international bisannuel des chercheurs en théorie des nombres), M. TSFASMAN a posé ces questions lors d'un exposé sur la théorie des codes ; dans le train qui le ramenait à Paris, J.-P. SERRE a rédigé sa réponse sous forme de lettre au conférencier, publiée plus tard dans les Actes du colloque [Se]. A.B. SØRENSEN, doctorant danois travaillant sur les codes projectifs et ayant aussi assisté à la conférence, a prouvé en parallèle un résultat équivalent, voir [Sø].

1 Droites du plan

Dans cette section, $d \geq 2$ est un entier naturel fixé, p est un nombre premier et $q = p^\alpha$ est une puissance ($\alpha \in \mathbb{N}^*$) de p. On note $\mathbb{F}_q$ le corps fini à q éléments, c'est l'unique — à isomorphisme près — extension de degré α de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. On peut tout à fait supposer que $\alpha = 1$ (donc $q = p$) si on le souhaite.

1.1 Arrangements de droites projectives

Soit $n \in \mathbb{N}$, on considère l'espace vectoriel $\mathbb{F}_q{}^n$ de dimension n sur $\mathbb{F}_q$. Un élément de $\mathbb{F}_q{}^n$ est donc un n-uplet $(x_1, \ldots, x_n)$ d'éléments de $\mathbb{F}_q$. Une *droite vectorielle* est l'ensemble des multiples d'un vecteur non nul, c'est-à-dire $\{(\lambda x_1, \ldots, \lambda x_n),\ \lambda \in \mathbb{F}_q\}$ avec $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$. Un *plan vectoriel* est l'ensemble des combinaisons linéaires de deux vecteurs indépendants, c'est-à-dire $\{(\lambda x_1 + \mu y_1, \ldots, \lambda x_n + \mu y_n),\ \lambda, \mu \in \mathbb{F}_q\}$ avec (x, y) libre.

[1] appelée aussi borne de SERRE-SØRENSEN

Une droite vectorielle est isomorphe à $\mathbb{F}_q$, un plan vectoriel à $\mathbb{F}_q{}^2$.

Exercice 1 *Vérifier que le nombre de droites vectorielles contenues dans $\mathbb{F}_q{}^n$ est égal à*

$$\frac{q^n-1}{q-1} = 1+q+\cdots+q^{n-1} = \pi_{n-1} \ .$$

En déduire que le nombre de :

a) droites vectorielles contenues dans un plan vectoriel est égal à $\pi_1 = 1+q$;

b) droites vectorielles contenues dans $\mathbb{F}_q{}^3$ est égal à $\pi_2 = 1+q+q^2$;

c) plans vectoriels contenus dans $\mathbb{F}_q{}^3$ est égal à $\pi_2 = 1+q+q^2$.

On appelle *plan projectif* sur $\mathbb{F}_q$ et on note $\mathbb{P}_2(\mathbb{F}_q)$ l'ensemble des droites vectorielles de $\mathbb{F}_q{}^3$; autrement dit, $\mathbb{P}_2(\mathbb{F}_q)$ est l'espace quotient de $\mathbb{F}_q{}^3 \setminus \{(0,0,0)\}$ par la relation de *colinéarité*. On appelle :

- *point (projectif)* de $\mathbb{P}_2(\mathbb{F}_q)$ un de ses éléments, c'est-à-dire une droite vectorielle de $\mathbb{F}_q{}^3$ (ou plus précisément la classe définie par les vecteurs d'une droite vectorielle de $\mathbb{F}_q{}^3$) ;
- *droite (projective)* de $\mathbb{P}_2(\mathbb{F}_q)$ l'ensemble des droites d'un plan vectoriel de $\mathbb{F}_q{}^3$ (ou plus précisément l'ensemble des classes définies par les vecteurs d'un plan vectoriel de $\mathbb{F}_q{}^3$).

Exercice 2 *Donner le nombre de points de $\mathbb{P}_2(\mathbb{F}_q)$, le nombre de points d'une droite projective, le nombre de droites projectives dans $\mathbb{P}_2(\mathbb{F}_q)$.*

On se donne un *arrangement* (c'est-à-dire une réunion) $\mathscr{D}$ de d droites projectives de $\mathbb{P}_2(\mathbb{F}_q)$. La borne de SERRE majore le nombre $\mathrm{N}_{\mathscr{D}}$ de points projectifs de l'arrangement $\mathscr{D}$:

$$\mathrm{N}_{\mathscr{D}} \leq dq+1 \ ,$$

avec égalité si et seulement si $d \leq q+1$ et toutes les droites de $\mathscr{D}$ passent par un même point de $\mathbb{P}_2(\mathbb{F}_q)$. Noter que $d = q+1$ est la plus grande valeur de d pour laquelle la borne est pertinente ; en effet, pour $d = q+1$, on trouve $(q+1)q+1 = q^2+q+1$, qui est égal au nombre total de points de $\mathbb{P}_2(\mathbb{F}_q)$.

Une façon de compter les points de $\mathscr{D}$ est la suivante :

$$\begin{gathered}(\text{nombre de points sur une droite}) \times (\text{nombre de droites}) \\ -(\text{les points comptés plusieurs fois})\end{gathered}$$

Pour cela, si l'on désigne par $\mathrm{P}_1, \ldots, \mathrm{P}_m$ les points d'intersection des droites de $\mathscr{D}$, on va noter a_i le nombre de droites de $\mathscr{D}$ passant par P_i pour chaque $1 \leq i \leq m$. Chaque P_i est compté a_i fois dans la première étape du calcul ci-dessus, donc

$$\mathrm{N}_{\mathscr{D}} = d(q+1) - \sum_{i=1}^{m} (a_i - 1) \ .$$

Il s'ensuit que majorer $N_{\mathscr{D}}$ revient à minorer $\sum_{i=1}^{m}(a_i - 1)$. Pour avoir une meilleure intuition de la situation (et pouvoir dessiner !), on va commencer par étudier ce problème dans le plan euclidien ; on vérifiera ensuite que le raisonnement mis en œuvre se transpose à l'identique au plan projectif. Avant cela, pour que l'analogie soit correcte, notons la propriété suivante de $\mathbb{P}_2(\mathbb{F}_q)$.

Exercice 3 *Justifier que deux droites distinctes de $\mathbb{P}_2(\mathbb{F}_q)$ ont toujours exactement un point d'intersection.*

1.2 Le plan euclidien

On se place dans le plan euclidien $\mathbb{R}^2$ et on se donne un arrangement $\mathscr{D}$ de d droites sans parallèles. Soient $P_1, \ldots, P_m$ les points d'intersection de l'arrangement ; comme ci-dessus, on note a_i le nombre de droites de l'arrangement passant par P_i, pour $1 \leq i \leq m$. On a donc $a_i \geq 2$ pour tout $1 \leq i \leq m$. On va montrer la propriété :

$$\sum_{i=1}^{m}(a_i - 1) \geq d - 1 \ , \quad \text{avec égalité si et seulement si } m = 1 \ . \tag{1}$$

Il est clair qu'il y a égalité lorsque $m = 1$. Considérons les autres cas.

Exercice 4 *On suppose $m \geq d$, montrer que $\sum_{i=1}^{m}(a_i - 1) \geq d$.*

Supposons maintenant que $2 \leq m \leq d$. Noter qu'alors $\mathscr{D}$ contient trois droites D_1, D_2, D_3 qui se coupent deux à deux en trois points distincts. Soient $T = D_1 \cup D_2 \cup D_3$ et $\mathscr{T} \subseteq \{1, \ldots, m\}$ l'ensemble des entiers $1 \leq i \leq m$ tels que $P_i \in T$.

Exercice 5 *Montrer que chaque droite de $\mathscr{D}$ coupe* T *en au moins deux points ; en déduire que l'on a : $\sum_{i \in \mathscr{T}} a_i \geq 2d$.*

De là, on obtient aisément la propriété (1).

Remarque : on peut montrer que

$$\sum_{i=1}^{m} \frac{a_i(a_i - 1)}{2} = \frac{d(d-1)}{2} \ .$$

En effet, on voit facilement par récurrence sur $a \in \mathbb{N}$ que le nombre de points d'intersection d'un arrangement de a droites en position *générique* (pas de parallèles, aucun point commun à plus de 2 droites) est :

$$\binom{a}{2} = \frac{a(a-1)}{2} = \sum_{k=0}^{a-1} k \ .$$

Il s'ensuit que si P_i est un point *multiple* ($a_i \geq 3$), on peut en modifiant légèrement l'arrangement le faire « éclater » en $\frac{a_i(a_i-1)}{2}$ points *simples* (contenus dans exactement 2 droites). Ceci justifie qu'on

appelle *multiplicité d'intersection* de P_i le nombre $\binom{a_i}{2} = \frac{a_i(a_i-1)}{2}$. Ainsi, la somme des multiplicités d'intersection des points de d droites non parallèles ne dépend pas des positions des droites.

1.3 Le plan projectif

Revenons au plan projectif $\mathbb{P}_2(\mathbb{F}_q)$, muni d'un arrangement $\mathcal{D}$ de d droites projectives, de points d'intersection $P_1, \ldots, P_m$; pour chaque $1 \leq i \leq m$, on note a_i le nombre de droites de $\mathcal{D}$ passant par P_i.

Exercice 6 *Vérifier que le raisonnement tenu dans la section 1.2 pour établir l'assertion (1) est encore valable pour l'arrangement $\mathcal{D}$ du plan projectif. En déduire que $N_{\mathcal{D}} \leq dq+1$, avec égalité si et seulement si toutes les droites de $\mathcal{D}$ passent par un même point de $\mathbb{P}_2(\mathbb{F}_q)$.*

Exercice 7 *Déterminer le nombre de droites passant par un même point de $\mathbb{P}_2(\mathbb{F}_q)$. Un arrangement de $d \leq q+1$ droites peut-il contenir tous les points de $\mathbb{P}_2(\mathbb{F}_q)$?*

On a ainsi retrouvé la borne de SERRE en dimension 2 (pour les droites, c'est-à-dire sans considérer les courbes algébriques de degré au moins 2). On va maintenant considérer ...

2 Le cas général

Soit n un entier naturel. L'*espace projectif* $\mathbb{P}_n(\mathbb{F}_q)$ de dimension n est l'espace quotient de $\mathbb{F}_q{}^{n+1} \setminus \{0\}$ par la relation de colinéarité, autrement dit chaque élément de $\mathbb{P}_n(\mathbb{F}_q)$ est la classe des vecteurs d'une droite vectorielle de $\mathbb{F}_q{}^{n+1}$.

Exercice 8 *Vérifier que le cardinal de $\mathbb{P}_n(\mathbb{F}_q)$ est $\pi_n = 1 + q + \cdots + q^n$.*

2.1 Coordonnées projectives et équations

Notons $(x_0, x_1, \ldots, x_n)$ les $n+1$ coordonnées de $x \in \mathbb{F}_q{}^{n+1} \setminus \{0\}$; les éléments de la droite vectorielle engendrée par x ont pour coordonnées $(\lambda x_0, \lambda x_1, \ldots, \lambda x_n)$ pour $\lambda \in \mathbb{F}_q$ et on appelle *coordonnées projectives* de la classe de x dans $\mathbb{P}_n(\mathbb{F}_q)$ le « système » :

$$(x_0 : x_1 : \ldots : x_n) \ .$$

Ces coordonnées projectives ne sont définies *qu'à multiplication par $\mathbb{F}_q^*$ près* : pour tout $\lambda \in \mathbb{F}_q^*$, on a $(\lambda x_0 : \lambda x_1 : \ldots : \lambda x_n) = (x_0 : x_1 : \ldots : x_n)$ puisque x et λx ont la même classe dans l'espace projectif. Comme $x \neq 0$, l'un des x_i est non nul ; si par exemple $x_0 \neq 0$, alors $(x_0 : x_1 : \ldots : x_n) = (1 : \frac{x_1}{x_0} : \ldots : \frac{x_n}{x_0})$ et l'application $x \mapsto (\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})$ permet d'identifier les classes des vecteurs de première coordonnée non nulle à $\mathbb{F}_q{}^n$. Sa réciproque permet d'injecter l'espace affine $\mathbb{F}_q{}^n$ dans l'espace projectif de même dimension, donc de voir celui-ci comme la réunion de $\mathbb{F}_q{}^n$ et des classes des vecteurs de première coordonnée nulle, sous-ensemble qu'on appelle habituellement l'hyperplan « à l'infini ».

Un sous-espace de dimension $0 \leq k \leq n$ de $\mathbb{P}_n(\mathbb{F}_q)$ est l'ensemble des classes des vecteurs d'un sous-espace vectoriel de dimension $k+1$ de $\mathbb{F}_q{}^{n+1}$. En particulier, si $n \geq 1$, une *droite projective* est l'ensemble des classes des vecteurs d'un plan vectoriel, un *hyperplan projectif* est l'ensemble des classes des vecteurs d'un hyperplan vectoriel.

Tout hyperplan vectoriel H est le noyau d'une forme linéaire $\mathbb{F}_q{}^{n+1} \to \mathbb{F}_q$, autrement dit l'ensemble des $x = (x_0, \ldots, x_n)$ tels que

$$a_0 x_0 + \cdots + a_n x_n = 0 \ ,$$

pour certains $a_i \in \mathbb{F}_q$ non tous nuls. Comme $a_0 x_0 + \cdots + a_n x_n = 0 \Leftrightarrow a_0 \lambda x_0 + \cdots + \lambda a_n x_n = 0$, pour tout $\lambda \in \mathbb{F}_q^*$, on voit que l'hyperplan projectif $\mathbb{P}(\mathrm{H})$ associé à H est donné par la même équation :

$$\mathbb{P}(\mathrm{H}) = \{(x_0 : \ldots : x_n) \in \mathbb{P}_n(\mathbb{F}_q),\ a_0 x_0 + \cdots + a_n x_n = 0\} \ .$$

Les sous-espaces vectoriels étant des intersections d'hyperplans, ils sont donnés par des systèmes d'équations, et il en va de même pour les sous-espaces projectifs associés. En particulier, une droite projective est définie par un système de n équations indépendantes.

Plus généralement, étant donné un entier naturel d et un polynôme f *homogène* de degré d à $n+1$ variables, on a $f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$ si bien que, pour $\lambda \in \mathbb{F}_q^*$:

$$f(x_0, \ldots, x_n) = 0 \Leftrightarrow f(\lambda x_0, \ldots, \lambda x_n) = 0 \ ,$$

ce qui permet de donner un sens à l'équation $f(x_0 : \ldots : x_n) = 0$. On appelle *sous-variété de* $\mathbb{P}_n(\mathbb{F}_q)$ définie par f le sous-ensemble $\mathrm{S}(f)$ de $\mathbb{P}_n(\mathbb{F}_q)$ égal à

$$\mathrm{S}(f) = \{(x_0 : \ldots : x_n),\ f(x_0 : \ldots : x_n) = 0\} \ .$$

Exercice 9 *Supposons que* $f = \prod_{i=1}^{d} g_i$, *où les* g_i *sont des polynômes homogènes de degré* 1 *à* $n+1$ *variables. Montrer que* $\mathrm{S}(f)$ *est la réunion des* d *hyperplans d'équations* $g_i = 0$.

2.2 La borne de Serre

Notons N_f le cardinal de $\mathrm{S}(f)$. La borne de SERRE est la majoration de N_f donnée par le résultat suivant.

Théorème. *Soit* $n \geq 1$ *un entier. Pour tout entier naturel* d, *pour tout polynôme homogène* f *de degré* d *à* $n+1$ *variables, on a (en convenant que* $\pi_{-1} = 0$*) :*

$$\mathrm{N}_f \leq d q^{n-1} + \pi_{n-2} \ .$$

Remarques :

— pour $n \geq 0$, on a $\pi_n = \frac{q^{n+1}-1}{q-1} = 1 + q + \cdots + q^n$, donc

$$\pi_{n+1} = \pi_n + q^{n+1} \ ;$$

la convention $\pi_{-1} = 0$ permet d'étendre cette formule de récurrence à $n \geq -1$;

— comme pour $n = 2$, la majoration est triviale pour $d \geq q+1$ puisque $(q+1)q^{n-1} + \pi_{n-2} = q^n + q^{n-1} + q^{n-2} + \cdots + 1 = \pi_n$ est le cardinal de $\mathbb{P}_n(\mathbb{F}_q)$. Elle l'est aussi pour $d = 0$, on supposera donc $1 \leq d \leq q$ pour la preuve ;

— dans le cas particulier $n = 2$ et $f = \prod_{i=1}^{d} g_i$ avec $\deg(g_i) = 1$, $S(f)$ est la réunion de d droites projectives et on retrouve la majoration $N_f \leq dq+1$ établie dans la section 1 pour les arrangements de droites (mais pas pour les sous-variétés de degré ≥ 2).

Dans cette section, on présente la preuve du Théorème donnée par SERRE dans [Se]. Commençons par prouver le résultat dans le cas $n = 1$. Soit $(x_0 : x_1) \in \mathbb{P}_1(\mathbb{F}_q)$, écrivons

$$f(X_0, X_1) = \sum_{i=0}^{d} a_i X_0^i X_1^{d-i} \quad .$$

Exercice 10 *Montrer que, si $x_0 \neq 0$, $f(x_0 : x_1) = 0$ est possible pour au plus d valeurs de $\frac{x_1}{x_0}$ si $a_0 \neq 0$, et pour au plus $d-1$ valeurs de $\frac{x_1}{x_0}$ si $a_0 = 0$.*

On en déduit que $N_f \leq d$, ce qui est le résultat souhaité pour $n = 1$.

Pour le cas général, soient $g_1, \ldots, g_\delta$ les différents (à multiplication par $\mathbb{F}_q^*$ près) polynômes homogènes de degré 1 à cœfficients dans $\mathbb{F}_q$ qui divisent f ; les $S(g_i)$, $1 \leq i \leq \delta$, sont des hyperplans distincts de $\mathbb{P}_n(\mathbb{F}_q)$, contenus dans $S(f)$.

2.3 Cas des unions d'hyperplans

On suppose ici que $S(f) = \bigcup_{i=1}^{\delta} S(g_i) = S(g_1 \ldots g_\delta)$, c'est-à-dire $S(f)$ est une union d'hyperplans. Montrons par récurrence sur $0 \leq m \leq \delta$ que

$$N_{g_1 \cdots g_m} \leq mq^{n-1} + \pi_{n-2} \quad . \tag{2}$$

Si $m = 0$, $g_1 \ldots g_m = 1$ donc c'est clair ; si $m = 1$, $S(g_1)$ est un hyperplan donc $N_{g_1} = \pi_{n-1} = q^{n-1} + \pi_{n-2}$. Supposons donc la propriété vraie pour un $1 \leq m \leq \delta - 1$.

Exercice 11 *Vérifier que $S(g_{m+1}) \cap (S(g_1) \cup \cdots \cup S(g_m))$ contient au moins π_{n-2} points ; en déduire que (2) est vraie pour $m+1$.*

D'après notre hypothèse, on a $N_f = N_{g_1 \cdots g_\delta} \leq \delta q^{n-1} + \pi_{n-2} \leq dq^{n-1} + \pi_{n-2}$, donc le théorème est prouvé dans le cas des réunions d'hyperplans.

Remarque : la preuve donnée par SERRE pour les unions d'hyperplans en toute dimension est beaucoup plus simple que celle pour les unions de droites qu'on a présentée dans la section 1.

2.4 Cas où $S(f)$ n'est pas une réunion d'hyperplans

On va raisonner ici par récurrence sur $n \geq 1$; le cas $n = 1$ a été établi plus haut. On a maintenant $\bigcup_{i=1}^{\delta} S(g_i) \subset S(f)$ et l'inclusion est stricte.

Soit $P \in S(f) \setminus \bigcup_{i=1}^{\delta} S(g_i)$. Pour H hyperplan de $\mathbb{P}_n(\mathbb{F}_q)$ passant par P, la restriction $f_{|H}$ de f à H n'est pas identiquement nulle (sinon $H \subset S(f)$ donc $H = S(g_i)$ pour un $1 \leq i \leq \delta$, ce qui est impossible car $P \in H$) ; de plus on peut écrire $f_{|H}$ comme un polynôme homogène de degré d en n variables : si $a_0 x_0 + \cdots + a_n x_n = 0$ est l'équation de H, alors l'un des a_i est non nul (disons a_n), donc $x_n = -\frac{1}{a_n}(a_0 x_0 + \cdots + a_{n-1} x_{n-1})$ pour tout $(x_0 : x_1 : \ldots : x_n) \in H$ et $f_{|H}$ s'exprime en fonction de $x_0, \ldots, x_{n-1}$. On peut donc appliquer l'hypothèse de récurrence à $f_{|H}$, ce qui donne :

$$N_{f_{|H}} = |S(f) \cap H| \leq d q^{n-2} + \pi_{n-3} \ .$$

Soit X l'ensemble des couples (P', H), où P' est un point de $S(f) \setminus \{P\}$ et H un hyperplan passant par P et par P'. Si l'on fixe P', il y a π_{n-2} hyperplans passant par P et P', d'où :

$$|X| = (N_f - 1)\pi_{n-2} \ ;$$

si au contraire on fixe un hyperplan H passant par P, le nombre de points $P' \in S(f) \setminus \{P\}$ contenus dans H est $N_{f_{|H}} - 1 \leq d q^{n-2} + \pi_{n-3} - 1$, d'où l'on tire que :

$$|X| \leq \pi_{n-1}(d q^{n-2} + \pi_{n-3} - 1) \ .$$

En combinant les deux formules précédentes, on obtient :

$$N_f \leq 1 + \frac{\pi_{n-1}}{\pi_{n-2}}(d q^{n-2} + \pi_{n-3} - 1) \ .$$

Exercice 12 *Vérifier que :*

$$d q^{n-1} + \pi_{n-2} - \frac{q^{n-2}}{\pi_{n-2}}(q + 1 - d) = 1 + \frac{\pi_{n-1}}{\pi_{n-2}}(d q^{n-2} + \pi_{n-3} - 1) \ .$$

Or on a supposé $d \leq q$ donc $q + 1 - d > 0$ et $N_f < d q^{n-1} + \pi_{n-2}$, ce qui entraîne le résultat du théorème, dont la preuve est donc terminée.

Exercice 13 *Dans le cas où $S(f)$ est une réunion d'hyperplans, vérifier qu'il y a égalité dans la formule du théorème si et seulement si $S(f)$ est réunion de d hyperplans contenant tous le même sous-espace de codimension 2.*

3 Codes de Reed-Müller projectifs

On va maintenant introduire une famille de codes pour lesquels la borne de SERRE donne la distance minimale. Ils seront constitués par les « images » sur les points d'un espace projectif des polynômes homogènes de degré fixé d.

Un *code* est simplement un sous-espace d'un espace vectoriel sur un corps fini (notons celui-ci $\mathbb{F}_q$). Les codes intéressants pour les applications pratiques sont souvent construits de manière algébrique ; dans le cas des codes de REED-MÜLLER projectifs, la construction à partir des polynômes homogènes de degré fixé permet de calculer les principaux paramètres du code (voir en fin de section). Pour utiliser un code C, on en détermine une base ; autrement dit, on fixe un isomorphisme (appelé *encodeur*) : ${\mathbb{F}_q}^k \to \mathrm{C}$, où $k = \dim_{\mathbb{F}_q} \mathrm{C}$, ce qui permet d'*encoder* n'importe quel k-uplet d'éléments de $\mathbb{F}_q$ en un vecteur du code.

Pour construire les codes de REED-MÜLLER projectifs, on associe à chaque polynôme homogène P le vecteur dont les composantes sont les « images » par P des points de l'espace projectif. Les coordonnées de ces points n'étant connues qu'à multiplication par $\mathbb{F}_q^*$ près, on ne peut pas évaluer directement P sur celles-ci. Nous allons voir une manière de découper l'espace projectif en parties disjointes sur lesquelles on aura un moyen « naturel » d'évaluer P.

On suit ici la présentation de [L]. Dans $\mathbb{P}_n(\mathbb{F}_q)$ notons V_i pour $0 \leq i \leq n$ le sous-ensemble constitué des éléments dont la i-ème coordonnée est non nulle, puis :

$$\mathrm{W}_0 = \mathrm{V}_0\,, \quad \mathrm{W}_1 = \mathrm{V}_1 \setminus \mathrm{V}_0\,, \quad \mathrm{W}_2 = \mathrm{V}_2 \setminus (\mathrm{V}_0 \cup \mathrm{V}_1)\,, \ldots$$

Exercice 14 *Montrer que* $x = (x_0 : \ldots : x_n) \in \mathrm{W}_i$ *si et seulement si* $x_0 = \ldots = x_{i-1} = 0$ *et* $x_i \neq 0$.

Les W_i, $0 \leq i \leq n$, forment une partition de $\mathbb{P}_n(\mathbb{F}_q)$. De plus, W_i est un isomorphe à un espace vectoriel de dimension $n-i$, donc $|\mathrm{W}_i| = q^{n-i}$. On retrouve ainsi la formule $|\mathbb{P}_n(\mathbb{F}_q)| = 1 + q + \cdots + q^n$.

Pour $d \in \mathbb{N}$, notons $\{0\} \cup \mathbb{F}_q[\mathrm{X}_0, \ldots, \mathrm{X}_n]_d^0$ l'espace vectoriel des polynômes homogènes de degré d à cœfficients dans $\mathbb{F}_q$ et à $n+1$ variables. Si $\mathrm{P} \in \mathbb{F}_q[\mathrm{X}_0, \ldots, \mathrm{X}_n]_d^0$ et $x = (x_0 : \ldots : x_n) \in \mathrm{W}_i$, on pose

$$c_x(\mathrm{P}) = \frac{\mathrm{P}(x_0, \ldots, x_n)}{x_i^d}\ .$$

On vérifie immédiatement que ceci ne dépend pas du représentant $(x_0, \ldots, x_n)$ de x choisi. On définit alors l'image de P par :

$$c(\mathrm{P}) = (c_x(\mathrm{P}))_{x \in \mathbb{P}_n(\mathbb{F}_q)}\ .$$

De plus, on pose $c(0) = 0$ et on note

$$\mathrm{R}_q(d, \mathbb{P}_n) = c(\{0\} \cup \mathbb{F}_q[\mathrm{X}_0, \ldots, \mathrm{X}_n]_d^0)\ ;$$

comme l'application c est linéaire, c'est un sous-espace vectoriel de ${\mathbb{F}_q}^{\pi_n}$, qu'on appelle le code de REED-MÜLLER projectif d'ordre d sur $\mathbb{P}_n(\mathbb{F}_q)$. La construction de $\mathrm{R}_q(d, \mathbb{P}_n)$ qu'on vient de présenter donne accès à ses principaux *paramètres* : longueur, dimension, distance minimale.

La *longueur* du code est la dimension de l'espace vectoriel qui le contient, c'est-à-dire le nombre de composantes de chaque vecteur ; ici, elle est bien sûr égale à π_n.

La *dimension* du code est sa dimension en tant qu'espace vectoriel sur le corps de base ; cette grandeur mesure la capacité d'encodage, puisque le nombre de vecteurs disponibles pour encoder l'information est le cardinal du corps de base à la puissance cette dimension. On va calculer cette dimension dans le cas où $d \leq q$, car la borne de SERRE montre qu'alors l'application c est injective. En effet, comme elle est linéaire, il suffit de vérifier que son noyau est réduit au polynôme nul ; or avec les mêmes notations que ci-dessus, $c_x(\mathrm{P}) = 0 \Leftrightarrow \mathrm{P}(x) = 0$, donc un polynôme P appartient au noyau de c si et seulement si il est identiquement nul sur $\mathbb{P}_n(\mathbb{F}_q)$. Mais $d < q+1$ entraîne que $dq^{n-1} + \pi_{n-2} < \pi_n$, si bien qu'aucun polynôme homogène de degré d à $n+1$ variables n'est identiquement nul sur $\mathbb{P}_n(\mathbb{F}_q)$.

Il s'ensuit que, si $d \leq q$, la dimension de $\mathrm{R}_q(d, \mathbb{P}_n)$ est égale à la dimension de l'espace vectoriel $\{0\} \cup \mathbb{F}_q[\mathrm{X}_0, \ldots, \mathrm{X}_n]^0_d$, lequel admet pour base la famille des monômes de degré d à $n+1$ variables. Au monôme $\mathrm{X}_0^{a_0}\mathrm{X}_1^{a_1}\ldots\mathrm{X}_n^{a_n}$, avec $a_i \in \mathbb{N}$ et $a_0 + a_1 + \cdots + a_n = d$, on peut associer le $(n+1)$-uplet $(a_0+1, a_1+1, \ldots, a_n+1)$, qui constitue une *composition* de $n+1+d$ à $n+1$ parts, c'est-à-dire un $(n+1)$-uplet d'entiers strictement positifs de somme $n+1+d$.

Exercice 15 *Soit $m \in \mathbb{N} \setminus \{0\}$; en utilisant le fait qu'une composition de m est le choix entre un signe $+$ et une virgule dans chacun des $m-1$ intervalles séparant m copies de l'entier 1 :*

$$(1 \quad 1 \quad 1 \quad \ldots \quad 1 \quad 1) \ ,$$

montrer que le nombre total de compositions de m est 2^{m-1} et que, pour $1 \leq k \leq m$, le nombre de compositions de m à k parts est $\binom{m-1}{k-1}$.

Comme l'application des monômes de degré d à $n+1$ variables vers les compositions de $n+1+d$ à $n+1$ parts considérée ci-dessus est clairement une bijection, on en déduit que, pour $d \leq q$, la dimension de $\mathrm{R}_q(d, \mathbb{P}_n)$ est

$$\binom{n+d}{d} = \frac{(n+d)!}{n!\,d!} \ .$$

Le rapport des deux paramètres précédents, dimension sur longueur, est l'*efficacité* du code.

Remarque : on a dit plus haut que pour utiliser le code, il fallait en choisir une base ; lorsque $d \leq q$, on peut donc choisir la base image par c de la famille des monômes de degré d.

Enfin, la *distance minimale* d'un code est le minimum du nombre de coordonnées non nulles de ses vecteurs non nuls. Ce dernier paramètre est souvent le plus difficile à déterminer. Ici, la borne de SERRE avec son cas d'égalité (voir exercice 13) nous permet de le faire. Supposons encore $d \leq q$ et soit P un polynôme homogène de degré d à $n+1$ variables qui atteint la borne :

$$\mathrm{N_P} = dq^{n-1} + \pi_{n-2} \ .$$

Ceci signifie que le nombre de coordonnées nulles de $c(\mathrm{P})$ est maximal et vaut $dq^{n-1} + \pi_{n-2}$; il s'ensuit que le nombre de coordonnées non nulles de $c(\mathrm{P})$ est minimal et vaut $\pi_n - (dq^{n-1} + \pi_{n-2})$, c'est-à-dire que la distance minimale de $\mathrm{R}_q(d, \mathbb{P}_n)$ est :

$$\Delta = (q+1-d)q^{n-1} \ .$$

Pour tout vecteur x de $\mathbb{F}_q{}^{\pi_n}$, il y a au plus un vecteur du code à *distance* (nombre de coordonnées distinctes[2]) inférieure à $\frac{\Delta-1}{2}$ de x. On peut donc décoder sans erreur si l'on sait que le nombre de coordonnées susceptibles d'être modifiées lors de la transmission est au plus $\frac{\Delta-1}{2}$.

Remarques :

— lorsque $d \geq q+1$, on peut trouver P homogène de degré d à $n+1$ variables, identiquement nul sur $\mathbb{P}_n(\mathbb{F}_q)$ (voir l'exercice 7 pour le cas limite quand $n=2$) ; il semble alors moins aisé de calculer la distance minimale du code obtenu, puisque cela nécessiterait de connaître le maximum du nombre de zéros des polynômes homogènes de degré d non identiquement nuls sur $\mathbb{P}_n(\mathbb{F}_q)$.

— On vérifie facilement que, à n et q fixés et en imposant $1 \leq d \leq q$, l'efficacité de $\mathrm{R}_q(d, \mathbb{P}_n)$ est maximale pour $d = q$, tandis que la distance minimale Δ est maximale (ce qui est souhaitable pour pouvoir corriger le plus possible d'erreurs de transmission) pour $d = 1$; on ne peut donc pas avoir, ici encore, à la fois le beurre et l'argent du beurre !

Références

[L] Lachaud G., The parameters of projective Reed-Müller codes, *Discrete Math. 81* (1990), no. 2, 217–221.

[Se] Serre J.-P., Lettre à M. Tsfasman, Journées Arithmétiques (Luminy, 1989), *Astérisque No. 198-200* (1991), *11*, 351–353 (1992).

[Sø] Sørensen A.B., Projective Reed-Muller codes, *IEEE Trans. Inform. Theory 37* (1991), no. 6, 1567–1576.

XLIM UMR 6172 CNRS / UNIVERSITÉ DE LIMOGES — Faculté des Sciences et Techniques de Limoges, 123 avenue Albert Thomas, 87060 Limoges cedex, France — stephane.vinatier@unilim.fr

[2] il s'agit de la distance de HAMMING