CODES MDS, PLAN PROJECTIF ET MOLS (INCOMPLETE DRAFT VERSION)

PAVLE MICHKO

Résumé. L'objet de cette note est de faire un point sur les conjectures concernants les configurations combinatoires associées aux codes MDS de dimension deux.

1. Introduction

Soit K un corps fini de cardinal q et de caractéristique p. Un $[n, k, d]$ code linéaire est un sous espace de K^n de dimension k de poids minimal supérieur ou égal à d :

$$d \leq d(C) = \min_{0 \neq x \in C} \mathrm{wt}(x)$$

où $\mathrm{wt}(x)$ est le poids de Hamming de x. Le code est dit MDS quand l'égalité est réalisée dans la borne de Singleton i.e. :

$$d(C) = n - k + 1.$$

La matrice génératrice d'un code MDS est complètement systématique : toute matrice $k \times k$ formée de k colonnes est inversible. Il en résulte que la classe des codes MDS est stable par orthogonalisation. Dans la suite, nous laissons de côté les cas triviaux correspondant à $k \leq 1$ et $k \geq n - 1$.

$$M(k, q) := \text{longueur maximal d'un code MDS de dimension } k$$

Conjecture 1 (main MDS)**.** *Pour $q \leq k$,*

$$M(k, q) = k + 1.$$

Pour $q > k$,

$$M(k, q) = \begin{cases} q + 2, & q > 2, p = 2, k = 3; \\ q + 2, & q > 2, p = 2, k = q - 1; \\ q + 1, & \textit{sinon.} \end{cases}$$

Il s'agit là d'une des conjectures des plus passionantes formuler dans le domaine des mathématiques discrètes. Les déclinaisons font légions : cas non linéaire, alphabet arbitraire etc. . . .

Date: Printemps 2014, dernière compilation 23 mai 2014.

2. Code de Reed-Solomon

L'exibition de code MDS par des méthodes informatiques est rapidement impossible. Dans ce contexte combinatoire, les corps finis offrent des codes MDS sans effort.

On considère l'espace des polynômes de degré strictement inférieurs à k à coefficients dans K, c'est un espace de dimension k et tout élément non nul possède au plus k racines. Notons x_1, x_2, n éléments distincts dans K. L'évaluation des polynômes de degré inférieur à k sur ces points fournit un code MDS $[n, k]$.

$$K[X]_k \ni p(X) \mapsto \big(p(x_1), p(x_2), \dots, p(x_n)\big) \in K^n$$

En effet, le copoids d'un polynôme non nul est au plus $k-1$ i.e. $d(C) \geq n-k+1$. Le code de Reed-Solomon obtenu peut-être prolongé par une évaluation à l'infini en un code $[n+1, k]$ MDS. Quand q est une puissance de 2 une nouvelle extension est possible lorsque $k = 3$.

3. Matrice

Sans perdre en généralité, une matrice génératrice d'un $[n, k]$ s'écrit

$$G = [I_k : A]$$

où A est une matrice $k \times (n-k)$. Le code est MDS si et seulement si toutes les matrices carrés extraites de A sont inversibles. On peut supposer A bordée par l'unité à gauche.

Lemme 1. *La dimension d'un code linéaire MDS vérifie $k \leq (q-1)$, ou encore*

$$n \leq q - 1 + k$$

Remarque 1. *Un code linéaire sur un anneau vérifie une borne similaire.*

4. Enumérateur des poids

L'énumérateur de poids de C est

$$W_C(X, Y) = \sum_{i=0}^{n} A_i X^{n-i} Y^i, \quad A_i = \sharp\{x \in C \mid \mathrm{wt}(x) = i\}.$$

La formule de MacWilliams [8]

$$W_{C^\perp}(X, Y) = q^{-k} W_C(X - Y, X + (q-1)Y)$$

permet alors de déterminer la distribution de poids d'un code MDS.

$$A_w = (q-1)\binom{n}{w} \sum_{i=0}^{w-d} (-1)^j \binom{w-1}{j} q^{w-d-j} \tag{1}$$

La même formule vaut dans le cas non-linéaire.

Dans [7], une généralisation est introduite. A une partition T de {1,2,. . . ,n} en s sous ensembles T_i de cardinal n_i, est associé un énumérateur :

$$\mathrm{wt}_T(c) = (w_1, w_2, \ldots, w_r), \quad w_i = |\mathrm{supp}c \cap T_i|$$

$$A_w^T = (q-1) \prod_{i=1}^{s} \binom{n_i}{w_i} \sum_{i=0}^{w-d} (-1)^j \binom{w-1}{j} q^{w-d-j} \tag{2}$$

5. Borne de Singleton

Un code non linéaire de paramètre (n, k, d) sur un alphabet A de cardinal q est une partie de A^n de cardinal q^k et de distance minimale d, dans ce con :texte la borne de Singleton

$$d(C) \leq n - \lceil k \rceil + 1 \quad \text{(Singleton)}$$

La preuve est immédiate. Notons d est la distance minimale entre les mots de C. Enumérons tous les mots de C, et observons t colonnes. Si $|C| > q^t$ alors $d \leq n - t$.

Remarque 2. *Le raisonnement ci-dessus fait apparaître en filigrane la notion de tableau orthogonal.*

Dans la littérature, un code vérifiant l'égalité de Singleton dit MDS quand k est entier. Pour k non entier, nous parlerons de code MDS au sens large. La conjecture MDS se prolonge aux codes non linéaire.

Le produit en couronne $S(A) \wr S(n)$ agit sur les codes sans changer les distances. Tout code MDS est équivalent à un code MDS contenant le mot nul pour lequel la formule (1) est encore valide.

On dit qu'un code C' est une extension de C lorsque les mots de C' sont des prolongements des mots de C et $d(C') > d(C)$. Un code MDS est toujours une extension d'un code MDS. Le résultat suivant montre que les codes linéaires MDS sont localement optimaux.

Théorème 1. *Si un code linéaire MDS (sur un corps) possède une extension MDS alors il possède une extension linéaire MDS.*

Lemme 2. *L'existence d'un code MDS* (n, k) *entraine l'existence d'un* $(n-1, k-1)$.

Démonstration. (**??**) □

Problème 1. *Que dire dans le cas des groupes, des modules ?*

6. Résultats connus

Dans le cas linéaire, la conjecture MDS est prouvée pour $k \leq 5$ (Casse,Segre), $q \leq 11$ (Maneri, Silverlman, Jurick), $q > (4k-9)^2$ (Thas) , et $k \leq 2p-2$ [4].

Nous reproduisons ici la liste des résultats proposée par Alderson et Huntemannn dans [**?**] concernant l'existence d'un code MDS non linéaire de paramètres $(n,k)_q$:

(1) $k+1 \leq M(k,q) \leq q+k-1$;
(2) si $k \geq q$ alors $M(k,q) = k+1$;
(3) si q est impair et $k \geq 3$ alors $M(k,q) \leq q+k-2$;
(4) si $q = 2 \mod 4$ et $k \geq 3$ alors $M(k,q) \leq q+k-3$;
(5) si $36 \not| q$ pair et $k \geq 4$ alors $M(k,q) \leq q+k-3$;
(6) si $q = 1,2 \mod 4$ et $k \geq 3$ et la partie square free de q est divisible par un entier congru à 3 modulo 4 alors $M(k,q) \leq q+k-3$;

(1) $M(2,6) = 3$;
(2) si $q \neq 2$ et $q \neq 6$ alors $4 \leq M(2,q) \leq q+1$;
(3) $M(2,10) \leq 8$;
(4) si $q \equiv 2 \mod 4$ alors $M(3,q) \leq q$.

Problème 2. *Que dire de l'énumérateur des poids complets d'un code MDS ?*

Problème 3. *Que dire dans le cas des groupes ?*

7. Définition

Un *plan projectif* d'ordre q est une configuration de q^2+q+1 points et q^2+q+1 droites tels que :
— chaque droite contient $q+1$ points ;
— par chaque point passent $q+1$ droites ;
— chaque paire de point définit une et une seule droite ;
— il existe 4 points non alignés.

Conjecture 2. *L'ordre d'un plan projectif est primaire.*

La conjecture est vérifiée pour $q = 6$ et $q = 10$.

Un *carré latin* d'ordre n est un tableau $n \times n$ à coefficients dans $\{1, 2, \ldots, n\}$ tel que chaque entier i figure 1 fois dans chaque ligne. Deux carrés latins (a) et (b) d'ordre n sont dit *mutuellement orthogonaux* si

$$a_{ij} = b_{ij} \quad \wedge \quad a_{i'j'} = b_{i'j'} \Longrightarrow i = i' \quad \wedge \quad j = j'.$$

Un *mols* de rang r est un ensemble de r carrés latins mutuellement ortogonaux.

L'existence d'un mols de rang r pour un alphabet A est équivalent à l'existence d'un code MDS $(r+2, 2)$ sur A.

En effet, un code systématique de longueur $r+2$ définit r tableaux $a^{(1)}, a^{(2)}, \ldots, a^{(r)}$ en notant

$$\left(i, j, , a_{i,j}^{(1)}, a_{i,j}^{(2)}, \ldots, a_{i,j}^{(r)}\right)$$

La distance minimale entre deux mots est au moins $r+1$ si et seulement si les tableaux sont mutuellement orthogonaux.

Dans la suite, nous notons $m(q)$ le rang maximal d'un mols sur un alphabet de taille q. La conjecture MDS se traduit en mols :

$$m(q) \leq q-1$$

Le problème qui consiste à déterminer la valeur maximale de $m(q)$. La première conjecture renvoie à Euler où il s'agissait de prouver que $m(6) = 1$ i.e. il n'existe pas de carré latin mutuellement orthogonaux à 6 valeurs.

Il s'agit du fameux probblèmes des 36 officiers, imaginé par Leonhard Euler en 1782, prouvé par Gaston Tarry en 1900. Euler n'ayant pas trouvé de solution satifaisante écrit :

Or, après toutes les peines qu'on s'est données pour résoudre ce problème, on a été obligé de reconnaître qu'un tel arrangement est absolument impossible, quoiqu'on ne puisse pas en donner de démonstration rigoureuse.

Références

[1] T. L. Aldersion and Svenja Huntemann. The partition weight enumerator and bound on MDS codes. *Altantic Electronic*, 6 :1–10, 2014.

[2] T. L. Alderson. Extending MDS codes. *Ann. Comb.*, 9(2) :125–135, 2005.

[3] T. L. Alderson. (6,3)-MDS codes over an alphabet of size 4. *Des. Codes Cryptogr.*, 38(1) :31–40, 2006.

[4] Simeon Ball and Jan De Beule. On sets of vectors of a finite vector space in which every subset of basis size is a basis II. *Des. Codes Cryptogr.*, 65(1-2) :5–14, 2012.

[5] R. C. Bose and S. S. Shrikhande. On the falsity of Euler's conjecture about the non-existence of two orthogonal Latin squares of order $4t+2$. *Proc. Nat. Acad. Sci. U.S.A.*, 45 :734–737, 1959.

[6] Aiden A. Bruen and Robert Silverman. On the nonexistence of certain M.D.S. codes and projective planes. *Math. Z.*, 183(2) :171–175, 1983.

[7] Mostafa El-Khamy and Robert J. McEliece. The partition weight enumerator of mds codes and its applications. *CoRR*, abs/cs/0505054, 2005.

[8] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. Amsterdam : North-Holland, 1983.

[9] Carl Maneri and Robert Silverman. A vector-space packing problem. *J. Algebra*, 4 :321–330, 1966.

[10] Brendan D. McKay, Alison Meynert, and Wendy Myrvold. Small Latin squares, quasigroups, and loops. *J. Combin. Des.*, 15(2) :98–119, 2007.

[11] Richard C. Singleton. Maximum distance q-nary codes. *IEEE Trans. Information Theory*, IT-10 :116–118, 1964.