LA CONJECTURE DE PATTERSON-WIEDEMAN

PAVLE MICHKO

Résumé. Dans cette note, je décris un procédé pour construire des fonctions hautement non-linéaire à partir de la structure multiplicative d'un corps fini.

1. Introduction

Dans cette note, L désigne un corps fini de caractéristique paire et de cardinal q. Nous notons μ le caractère additif canonique de L. Le coefficient de Fourier-Hadamard d'une application complexe F en un point a de L est défini à partir d'un caractère additif non trivial μ par :

$$\widehat{F}(a) = \sum_{x \in L} F(x)\mu(ax)$$

Dans le cas d'une application booléenne $f\colon L \to \mathbb{F}_2$, la transformée de Fourier de la fonction binaire $x \mapsto (-1)^{f(x)}$ est souvent appelée transformée de Walsh de f. Dans la suite, nous utiliserons la notation

$$f^*(a) = \sum_{x \in L} (-1)^{f(x)}\mu(ax)$$

Pour une application binaire, les coefficients de Fourier sont entiers et la relation de Parseval s'écrit :

$$\sum_{a \in L} \widehat{F}(a)^2 = q^2.$$

ce qui montre sur le champ que

$$\sup_{a \in L} |\widehat{F}(a)| \geq \sqrt{q}$$

L'inégalité est réalisable si et seulement si $[L : \mathbb{F}_2]$ est pair. Par exemple, pour une forme quadratique non dégénérée q, un calcul directe donne

$$\sup_{a \in L} q^*(a)^2 = \begin{cases} 2q, & \text{si } [L : \mathbb{F}_2] \text{ est impair;} \\ q, & \text{si } [L : \mathbb{F}_2] \text{ est pair;} \end{cases}$$

Date: Hiver 2013, dernière compilation 9 janvier 2014.

2. Conjecture

Convenons de noter

$$R(q) = \frac{\inf_f \sup_a |f^*|}{\sqrt{q}}$$

Comme nous venons de le voir $1 \leq R(q) \leq \sqrt{2}$. Au début des années 90, Patterson et Wiedemann [1] on construit de manière relativement empirique une fonction d'amplitude spectrale 240 en dimension 15. Ils proposent la conjecture

$$\lim_{q\to\infty} R(q) = 1.$$

Avant de nous intéresser à cette conjecture, signalons que tout cela est généralisable au groupe fini arbitraire et pour l'heure, je ne suis pas sûr de l'existence de travaux dans cette direction.

3. construction

Comme dans la thèse de Julien Bringer, nous partons d'un sous-groupe G de $L^\times$ et considérons la fonction binaire définie par :

$$F(x) = R(x) + \sum_{\omega\in\Omega} S(\omega)G_\omega(x)$$

où G_ω est l'indicatrice de la classe ωG, R une application de support G, à valeurs binaire sur$G$ et enfin, S une application binaire sur $\Omega = L^\times/G$.

Nous appelons R la fonction noyau, et S la fonction de sélection. Cette dernière sera toujours équilibrée de sorte que le coefficient de Fourier en phase se concentre sur le noyau :

$$\widehat{F}(0) = \widehat{R}(0) + |G| \sum_{\omega\in\Omega} S(\omega) = \widehat{R}(0)$$

Pour un coefficient hors phase, avec la relation

$$\widehat{G_\omega}(a) = \sum_{x\in G} \mu(ax\omega) = \widehat{G}(a\omega)$$

on obtient

$$\begin{aligned}\widehat{F}(a) &= \widehat{R}(a) + \sum_{\omega\in\Omega} S(\omega)\widehat{G_\omega}(a)\\ &= \widehat{R}(a) + \sum_{\omega\in\Omega} S(\omega)\widehat{G}(a\omega)\\ &= \widehat{R}(a) + S \times \widehat{G}(a)\end{aligned}$$

Nous espérons alors construire une fonction hautement non linéaire, en choissant un bon groupe G, un bon noyau R pour une sélection adéquate : tout un programme.

Références

[1] Nick J. Patterson and Douglas H. Wiedemann. Correction to 'the covering radius of the (2^{15}, 16) reed-muller code is at least 16276' (may 83 354-356), 1990.