PARITÉ MODULAIRE

PAVLE MICHKO

Résumé. Dans cette note, je met en place quelques faits sur la fonction de parité de domaine modulaire, en vue d'obtenir des résultats sur une bien curieuse conjecture.

1. Motivation

Soit m un entier positif, $n := 2^m - 1$, pour tout éléments z de $\mathbb{Z}/(n)$, on note $\mathrm{wt}\,(z)$ le poids binaire du résidu z. Notre travail est motivé par une curieuse conjecture proposée par Deng et Tu [1] :

Conjecture 1. *Soit t un élément non nul de $\mathbb{Z}/(n)$, le nombre de solutions du système*

$$x + y = t, \quad \mathrm{wt}\,(x) + \mathrm{wt}\,(y) < m;$$

est toujours inférieur à 2^{m-1}.

Comme $\mathrm{wt}\,(x) + \mathrm{wt}\,(-x) = m$, cette conjecture peut-être formulée en faisant intervenir le nombre de solutions de

$$x + y = t, \quad \mathrm{wt}\,(x) + \mathrm{wt}\,(y) > m;$$

Au final, une conjecture plus faible :

Conjecture 2. *Soit t un élément non nul de $\mathbb{Z}/(n)$, le nombre de solutions du système*

$$x + y = t, \quad \mathrm{wt}\,(x) + \mathrm{wt}\,(y) = m;$$

est strictement positif.

Cette dernière hypothèse paraît assez raisonnable vu que le nombre de paires d'entiers (x, y) vérifiant $\mathrm{wt}\,(x) + \mathrm{wt}\,(y) = m$ s'estime par

$$\sum_{r=0}^{m} \binom{m}{r}^2 = \binom{2m}{m} \sim \frac{1}{\sqrt{\pi m}}\, 2^{2m}$$

Date: 19 mars, dernière compilation 11 octobre 2015.

TAB. 1. Les différents énumérateurs pour $m = 6$.

X	0	1	2	3	4	5	6	7	8	9	10	11
6	0	0	0	0	0	32	16	8	4	2	1	0
3	0	0	0	0	16	16	12	4	9	4	2	0
6	0	0	0	0	16	16	8	12	5	4	2	0
6	0	0	0	0	16	8	20	10	5	2	2	0
2	0	0	0	8	12	6	13	6	12	6	0	0
6	0	0	0	8	4	10	21	10	4	6	0	0
12	0	0	0	8	8	12	9	12	8	6	0	0
6	0	0	4	2	5	10	20	8	14	0	0	0
6	0	0	4	4	5	12	8	16	14	0	0	0
3	0	0	4	4	9	4	12	16	14	0	0	0
6	0	2	1	2	4	8	16	30	0	0	0	0
1	1	0	0	0	0	0	62	0	0	0	0	0

2. PARITÉ

On commence par étudier la parité sur le domaine modulaire :

$$\pi(z) = \begin{cases} 1 & z_0 = 0; \\ 0, & \text{sinon.} \end{cases} \qquad \pi_i(z) = \begin{cases} 1 & z_i = 0; \\ 0, & \text{sinon.} \end{cases}$$

En opérant modulo m sur les indices, on remarque que

$$\sum_{i=1}^{m} \pi_i(x) = m - \operatorname{wt}(x), \quad \pi_i(x) = \pi(2^{-i}).$$

Le coefficient de Fourier en phase :

$$\widehat{\pi}(0) = 2^{m-1} = \frac{1}{2}(n+1), \widehat{\operatorname{wt}}(0) = m2^{m-1} - m.$$

La transformée de Fourier hors phase :

$$\begin{aligned} \widehat{\pi}(\zeta) = \sum_{z} \pi(z)\zeta^z &= \sum_{k=0}^{(n-1)/2} \zeta^{2k} \\ &= \frac{\zeta^{(n+1)} - 1}{\zeta^2 - 1} = \frac{\zeta - 1}{\zeta^2 - 1} = \frac{1}{\zeta + 1} \end{aligned}$$

En notant K le corps des invariants par σ_2, on obtient :

$$\widehat{\operatorname{wt}}(\zeta) = \operatorname{trace}_K(\zeta).$$

Et quand m est premier, le poids modulo m peut prendre la forme

$$\operatorname{wt}(k) \equiv \sum_{\zeta \neq 1} \operatorname{trace}_K(\zeta)\bar{\zeta}^k.$$

Références

[1] Ziran Tu and Yingpu Deng. A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity. *Des. Codes Cryptogr.*, 60(1) :1–14, 2011.