Nombre de fonctions courbes en 8 variables

Philippe Langevin
Institut de Mathmatiques de Toulon

Paris, Décembre 2008.

Résumé

L'objectif de cet exposé est de vous présenter le résultat d'une expérience numérique effectuée au cours de l'année 2007 ayant pour objet le comptage du nombre de fonctions courbes en 8 variables. Un travail en collaboration avec Gregor Leander

Notations

- $\mathbb{F}_2$ le corps à 2 éléments
- n un entier, le plus souvent pair, $n = 2t$.
- $\mathbb{F}_2^n$ l'espace de dimension sur $\mathbb{F}_2$.
- $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ fonction booléenne.
- S une partie de $\{1, 2, \ldots, n\}$.
- monôme X_S

$$X_S(x) = \prod_{s \in S} x_s$$

- u vecteur de $\mathbb{F}_2^n$

$$X^u(x) = \prod_{i=1}^{n} x_i^{u_i}$$

Représentation polynômiale

$$X_{\{1,2,\ldots,n\}}(x) = \prod_s x_s = \begin{cases} 1 & \text{si } x = (1,1,\ldots,1); \\ 0 & \text{sinon.} \end{cases}$$

L'indicatrice de $(1,1,\ldots,1)$ est polynomiale. Par conséquent, toute *fonction booléenne* $f : \mathbb{F}_2^n \to \mathbb{F}_2$ possède une représentation polynomiale :

$$f = \sum_{S \subseteq \{1,\ldots,n\}} a_S X_S$$

où $a_S \in \mathbb{F}_2$. Il s'agit d'une représentation unique, en terme de *polynôme réduit* i.e. $\deg_{X_i}(f) \leq 1$, (ANF).

$$\deg(f) = \sup\{|S| \mid a_S \neq 0\}$$

Coefficient de Fourier

$$\widehat{f}(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\langle a,x \rangle}.$$

$$\mathrm{spec}\,(f) = \{\widehat{f}(a) \ : \ a \in \mathbb{F}_2^n\}.$$

La distance de Hamming entre f et la fonction affine $x \mapsto ax + b$ est donnée par

$$d_H(f, ax + b) = 2^{m-1} + (-1)^b \hat{f}(a)$$

La *non-linéarité* de f

$$2^{m-1} - \frac{1}{2} \sup_{a \in \mathbb{F}_2^n} |\hat{f}(a)|$$

Fonction courbe

Une fonction de non-linéarité maximale i.e. d'amplitude spectrale minimale est une *fonction courbe*.

$$\sum_{a \in \mathbb{F}_2^n} \hat{f}(a)^2 = 2^{2n} \quad \text{(Parseval)}$$

$$|\hat{f}|_\infty \geq \sqrt{2^n}$$

En dimension paire,

$$\text{courbe} \iff \operatorname{spec}(f) = \{\pm 2^{n/2}\}$$

On définit la fonction courbe *duale* $\hat{f}(a) = (-1)^{\tilde{f}(a)} 2^t$

Invariance

Soient $\alpha \in \mathbb{F}_2^{n*}$, $u \in \mathbb{F}_2^n$ et $A \in \mathrm{GL}(2, n)$.
Si f est courbe alors

- $f(x) + 1$,
- $f(x) + \alpha(x)$,
- $f(x + u)$,
- $f \circ A(x)$,

sont courbes.
L'ensemble des fonctions courbes est invariant sous l'action du groupe affine, et même un peu plus:

$$\mathbb{F}_2 \times \mathrm{GA}(2, n) \dot{\times} \mathbb{F}_2^n$$

Action du groupe linéaire

Le groupe linéaire $\mathrm{GL}(2, n)$ agit sur les fonctions booléennes. Du point de vue fonctionnel, l'action de A sur f est la composée de f par A. Du point de vue polynomial,

$$f^A(x_1, x_2, \ldots, x_n) = f((x_1, x_2, \ldots, x_n)A)$$

Le cardinal du groupe linéaire

$$|\mathrm{GL}(2, n)| = \prod_{k=0}^{n-1} (2^n - 2^k) \sim 0.27 \times 2^{n^2}$$

est modeste comparé au nombre total (2^{2^n}) de fonctions booléennes. Le rang de cette action (nombre d'orbites) est doublement exponentiel en n.

Amplitude spectrale d'une forme quadratique

Soit Q une forme quadratique i.e. un polynôme réduit de degré deux sans terme constant.

$$Q(x+y) = Q(x) + Q(y) + (x,y)$$

où $(.,.)$ est une forme bilinéaire, forcément symétrique et symplectique.

$$\mathrm{rad}(Q) = \{y \in \mathbb{F}_2^n \mid (x,y) \equiv 0\}.$$

Un calcul direct montre que

$$\hat{Q}(a)^2 = 0 \quad \text{ou} \quad 2^{n+\dim \mathrm{rad}(Q)}$$

Pour une forme quadratique,

courbe $\iff$ non dégénérée.

Groupe orthogonaux en dimension paire

Le coefficient de Fourier en phase d'une forme quadratique non dégénérée Q vérifie,

$$\hat{Q}(0) = -\epsilon 2^t.$$

Le groupe linéaire agit sur les formes quadratiques non-dégénérées. Il y a exactement deux classes :

$$\begin{aligned} x_1x_{t+1} + x_2x_{t+2} + \ldots + x_tx_n & \quad \text{Elliptique } \epsilon = -1 \\ x_1x_{t+1} + x_2x_{t+2} + \ldots + x_tx_n + x_1 + y_1 & \quad \text{Hyperbolique } \epsilon = +1 \end{aligned}$$

$$\mathrm{fix}\,(Q) = \{A \in \mathrm{GL}(2, n) \mid Q^A = Q\}$$

est un *groupe orthogonal* son cardinal est bien connu :

$$\mathrm{O}^\epsilon(2t) = 2 \times N \times 2^{t(t-1)}(2^t - \epsilon)$$

où $N = \prod_{i=1}^{t-1}(2^{2i} - 1)$.

Nombre de fonctions courbes quadratiques

$$\mathrm{NB}_2(n) = 2 \times \sum_{\epsilon} \frac{\mathrm{GL}(2,n)}{\mathrm{O}^{\epsilon}(n)}$$

$$\overline{\mathrm{NB}}_2(n) = 2^{-n} \times \sum_{\epsilon} \frac{\mathrm{GL}(2,n)}{\mathrm{O}^{\epsilon}(n)}$$

Par exemple,

$$\mathrm{GL}(2,4) = 2^6 \times 3^2 \times 5 \times 7 \quad \mathrm{O}^{\epsilon}(4) = 2 \times 3 \times 2^2(2^2 - \epsilon)$$

$$\begin{aligned} \mathrm{NB}_2(4) &= 2\Big(\frac{2^6 \times 3^2 \times 5 \times 7}{2^3 \times 3 \times 5} + \frac{2^6 \times 3^2 \times 5 \times 7}{2^3 \times 3^2}\Big) \\ &= 2\big(2^3 \times 3 \times 7 + 2^3 \times 5 \times 7\big) = 2^5 \times 28 \end{aligned}$$

Et donc, $\overline{\mathrm{NB}}_2(4) = 28$.

Classe de Maiorana-MacFarland

On peut construire des fonctions courbes de degré 2, 3, ... t.

- identification $\mathbb{F}_2^n \simeq \mathbb{F}_2^t \times \mathbb{F}_2^t$.
- Ψ une permutation de $\mathbb{F}_2^t$.
- $g : \mathbb{F}_2^t \longrightarrow \mathbb{F}_2$.

$$f(x, y) = \langle x, \Psi(y) \rangle + g(y)$$

Un calcul direct donne

$$\begin{aligned}
\hat{f}(a, b) &= \sum_{x,y} (-1)^{\langle x,\Psi(y)\rangle + g(y) + \langle a,x\rangle + \langle b,y\rangle} \\
&= \sum_{y} (-1)^{g(y)+\langle b,y\rangle} \times \sum_{x} (-1)^{\langle x,\Psi(y)+a\rangle} \\
&= 2^t \sum_{\Psi(y)=a} (-1)^{g(y)+\langle b,y\rangle} \\
&= 2^t (-1)^{g(\Psi^{-1}(a))+\langle b,\Psi^{-1}(a)\rangle}
\end{aligned}$$

Degré d'une fonction courbe

- inclusion $u \leq v : \forall\ i, \quad u_i \leq v_i$.
- complément $\bar{u} = (1, 1, \ldots, 1) + u$.

Le coefficient de $x^u = \prod_{i=1}^{n} x_i^{u_i}$ est

$$a_u(f) = \sum_{x \leq u} f(x)$$

La formule de Poisson

$$\sum_{x \leq u} (-1)^{f(x)} = \frac{1}{2^{\mathrm{wt}\,(\bar{u})}} \sum_{a \leq \bar{u}} \hat{f}(a)$$

montre que

le degré d'une fonction courbe est $\leq t$

Problème

$\mathrm{NB}(n) :=$ nombre de fonctions courbes

$\overline{\mathrm{NB}}(n) :=$ nombre de fonctions courbes modulo $\mathrm{RM}(1, n)$

$\mathrm{NB}(n) = 2^{n+1} \times \overline{\mathrm{NB}}(n)$

n	$\overline{\mathrm{NB}}(n)$
2	1
4	28
6	42386176
8	$2^{61} \leq ? \leq 2^{111} < 2^{134} < 2^{154}$

- Classification de $\mathrm{RM}(6,6)/\mathrm{RM}(1,6)$ par Maiorana (1991)
- Minoration de S. Agievich (2005).
- Majorations de LLRVZ (2006), Carlet-Klapper (2002).

Code de Reed-Müller

$$\mathrm{RM}(k, n) = \{f \mid \deg(f) \leq k\}$$

- $\dim \mathrm{RM}(k, n) = \sum_{i=0}^{k} \binom{n}{i}$.
- $\mathrm{GL}(2, n)$ agit sur $\mathrm{RM}(k, n)$.

Forme booléenne

$$\mathrm{RM}^*(k,n) = \mathrm{RM}(k,n)/\mathrm{RM}(k-1,n)$$

On introduit le projecteur Π_k

$$\begin{array}{rcl} \Pi_k : \mathrm{RM}(n,n) & \to & \mathrm{RM}^*(k,n) \\ \displaystyle\sum_{S\subseteq\{1,\ldots,n\}} a_S X_S & \to & \displaystyle\sum_{\substack{S\subseteq\{1,\ldots,n\} \\ |S|=k}} a_S X_S. \end{array}$$

- $\dim \mathrm{RM}^*(k,n) = \binom{n}{k}$.
- $\mathrm{GL}(2,n)$ agit sur $\mathrm{RM}^*(k,n)$.

Action de $\mathrm{GL}(2, n)$ sur les formes

Deux formes g et h de degrés k sont équivalentes

$$h \sim g \iff \exists A \in \mathrm{GL}(2, n), \quad h^A(x) = h(xA) = g(x) + f(x)$$

avec $\deg f < k$. En d'autres termes:

$$\Pi_k(h(xA)) = \Pi_k(g(x))$$

L'action de A sur $\mathrm{RM}^*(k, n)$ est linéaire, la matrice de cette opération dans la base monomiale, est une *matrice composée* d'ordre k.

Matrice composée

L'action de $A \in \mathrm{GL}(2, n)$ sur le monôme X_S est donné par :

$$\begin{aligned} {X_S}^A(x) &= \prod_{i \in S} (\sum_{j=1}^{m} a_{ij} x_j) \\ &= \sum_{|T|=k} \sum_{j\,:\, S \to T} \prod_{i \in S} a_{ij(i)} X_T \\ &= \sum_{|T|=k} \det A_{S,T} X_T \end{aligned}$$

La composée d'ordre k de A.

$$C^k(A) = \left(\det A_{S,T}\right)$$

où $A_{S,T}$ est la matrice carrée d'ordre k obtenue par extraction des lignes indices $i \in S$ et des colonnes $j \in T$.

Un petit exemple

On considère la transvection :

$$T = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

dans la base (yz, xz, xy)

$$C^2(T) = \begin{pmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \\ \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \\ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} & \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{pmatrix}$$

Classification et comptage

$$\mathrm{RM}(k,m) \ni f \text{ courbe} \Longleftrightarrow \mathrm{RM}(k,m) \ni f^A \text{ courbe}$$

Pour compter, les fonctions courbes de degré k, on détermine un ensemble de représentants Ω de l'action de $\mathrm{GL}(k,n)$ sur $\mathrm{RM}^*(k,n)$, puis on énumère et calcule le spectre des fonctions

$$\omega + f, \quad \omega \in \Omega, \quad f \in \mathrm{RM}(k-1,m)$$

Le facteur de travail est

$$N(k,n) \times 2^{\dim \mathrm{RM}(k-1,m)} \times 2^m \times m$$

$+$ le temps de calcul de la classification !

Nombre de cubiques courbes en 8 variables

Il existe 32 classes de formes cubiques. Pour chaque **représentant cubique** C, on énumère **toutes** les formes quadratiques Q pour calculer le spectre de Fourier de

$$C + Q.$$

Le facteur de travail est :

$$2^5 \times 2^{28} \times 2^8 \times 2^3 = 2^{44}.$$

Le nombre de cubiques courbes vaut :

$$\overline{\mathrm{NB}}_{\leq 3}(8) = \sum_{C} \overline{\mathrm{NB}}_{C}(8) \times \sharp \mathrm{orb}_8^3(C).$$

$\overline{\mathrm{NB}}_{\leq 3}(8) = 5386705781653504 = 2^{21} \times 7 \times 11 \times 31 \times 37 \times 127 \times 229.$

Nombre de Quartiques courbes en 8 variables?

Pour une forme quartique h, on énumère toutes les formes cubiques c, toutes les formes quadratiques q pour calculer le spectre de Fourier de

$$h + c + q.$$

Le facteur de travail est :

$$2^{56} \times 2^{28} \times 2^{8} \times 2^{3} = 2^{95} \quad \times \sharp\mathrm{cl}(4,8) \quad \rightarrow 2^{105}$$

Le nombre de quartiques courbes vaut :

$$\overline{\mathrm{NB}}_{\leq 4}(8) = \sum_{H} \overline{\mathrm{NB}}(H) \times \mathrm{orb}_8^4(H).$$

- Classification de $\mathrm{RM}^*(4,8)$.
- Il faut trouver des réductions !

Classification des espaces de formes

Deux formes g et h de degrés k sont équivalentes

$$h \sim g \iff \exists A \in \mathrm{GL}(2, m), \quad h^A(x) = h(xA) = g(x) + f(x)$$

avec $\deg f < k$. Faire une classification complète de $\mathrm{RM}^*(k, n)$ c'est déterminer :

1. le nombre de classes $N(k, m)$
2. un ensemble de representants $\mathrm{cl}(k, m)$
3. la taille des orbites $\mathrm{orb}_m^k(h)$, $h \in \mathrm{cl}(k, m)$
4. un système de générateurs des groupes $\mathrm{fix}(h)$

Il est impossible de procéder de façon (strictement) aléatoire à cause de l'existence d'orbites de trés petites tailles.

Classification of $\mathrm{RM}^*(3,7)$

The lift by derivation of $\mathfrak{q}$ discriminates the 12 class of $\mathrm{RM}^*(3,7)$.

orb. size	fix. size	cubic
1	163849992929280	0
11811	13872660480	123
1763776	92897280	137+237+147+247+157+267+467
2314956	70778880	145+123
45354240	3612672	123+456
59527440	2752512	123+245+346
21165312	7741440	123+145+246+356+456
238109760	688128	124+235+346+457+561+267+137
444471552	368640	712+724+134+234+135+745+146
2222357760	73728	127+123+147+245+167
13545799680	12096	127+123+234+345+456+567+617
17777862080	9216	127+234+125+457+245+167+126

By the complementary map, we get the classification of $\mathrm{RM}^*(4,7)$.

Application complémentaire

$$\mathrm{RM}^*(k,n) \ni X_S \to X_{\bar{S}} \in \mathrm{RM}^*(n-k,n)$$

$$\begin{array}{ccc} \mathrm{RM}^*(k,m) & \xrightarrow{\text{comp}} & \mathrm{RM}^*(m-k,m) \\ {\scriptstyle A}\downarrow & & \downarrow{\scriptstyle A^{-1*}} \\ \mathrm{RM}^*(k,m) & \xrightarrow{\text{comp}} & \mathrm{RM}^*(m-k,m) \end{array} \tag{1}$$

En particulier,

$$f \sim g \iff \mathrm{comp}\,(f) \sim \mathrm{comp}\,(g).$$

et donc $N(k,m) = N(m-k,m)$.

- See X.-D. Hou papers.

Calcul du nombre de classes

On utilise le lemme de Burnside,

$$N(k,m) \times |\mathrm{GL}(2,m)| = \sum_{A \in \mathrm{GL}(2,m)} t(A)$$

où $t(A)$ est le nombre de formes fixées par A.

$$N(k,m) = \sum_{i=1}^{t} \frac{2^{\binom{m}{k} - \mathrm{rank}\left(C^k(A_i) - I\right)}}{\gamma(A_i)}$$

où A_i est une liste de représentants des classes de conjugaisons de $\mathrm{GL}(2,n)$, I la matrice identit 'e d'ordre $\binom{m}{k} i$ et $\gamma(A)$ l'ordre du centraliseur de A dans $\mathrm{GL}(2,n)$.
Il suffit d'enumérer tous les polynômes irrducibles de degré inférieur ou égal à m pour construire la liste des facteurs invariants.

Table numérique

Table: Number of $\mathrm{GL}(2, n)$-orbits in $\mathrm{RM}^*(k, n)$.

$k \backslash m$	6	7	8	9	10
3	6	12	32	349	3691561
4	3	12	999	$\sim 10^{15}$	$\sim 10^{34}$

- Hou, Sugita, Kasami and Fujiwara classification $\mathrm{RM}^*(3, 8)$ (1996).
- Brier & PL classification de $\mathrm{RM}^*(3, 9)$ (2003).
- Rabizonni, Véron, Zanotti & PL (2006) classification partielle de $\mathrm{RM}^*(4, 8)$, 966/999.
- Leander, & PL (2007) classification complète de $\mathrm{RM}^*(4, 8)$.

Coefficients des fonctions courbes

Si f est courbe alors $\widetilde{f}$ est courbe. De plus,

$$\Pi_t(\widetilde{f}) = \mathrm{comp}\,(\Pi_t(f)),$$

- X.-D. Hou (1995)

Si f est courbe en dimension $n \geq 6$ alors

$$\sum_{\{S,T\} \mid S \cup T = V} a_S a_T = 0.$$

pour tout $V \subset \{1, \ldots, n\}$ tel que $|V| \geq n/2 + 2$.

- X.-D. Hou, PL. (1997)

Coefficients des fonctions courbes en dimension 8

Pour $V \subseteq \{1, \ldots, 8\}$ de cardinal $6, 7$ ou 8, nous obtenons un système de $1 + 8 + 28 = 37$ équations :

$$\sum_{\{S,T\} \mid S \cup T = V} a_S a_T = 0.$$

On décompose f par les degrés:

$$f = \sum_{\substack{S \subseteq \{1,\ldots,8\} \\ |S|=4}} \alpha_S X_S + \sum_{\substack{S \subseteq \{1,\ldots,8\} \\ |S|=3}} \beta_S X_S + \sum_{\substack{S \subseteq \{1,\ldots,8\} \\ |S|=2}} \gamma_S X_S.$$

Fonction courbes en dimension 8

- 1 équation sur les coefficients de degré 4

$$\sum_{\substack{S\subseteq\{1,\dots,8\}\\|S|=4}} \alpha_S\alpha_{\overline{S}} = 0.$$

- 8 équations sur les termes de degré 3, $|V| = 7$:

$$\sum_{\substack{S\subseteq V\\|S|=4}} \alpha_S\beta_{V\setminus S} + \sum_{\substack{\{S,T\}\ |\ S\cup T=V\\|S|=|T|=4}} \alpha_S\alpha_T = 0.$$

- 28 équations sur les termes de degré 2, $|V| = 6$:

$$\sum_{\substack{S\subseteq V\\|S|=4}} \alpha_S\gamma_{V\setminus S} + \sum_{\substack{S\cup T=V\\|S|=|T|=3}}{}' \beta_S\beta_T + \sum_{\substack{S\cup T=V\\|S|=4,|T|=3}} \alpha_S\beta_T + \sum_{\substack{S\cup T=V\\|S|=|T|=4}}{}' \alpha_S\alpha_T = 0.$$

Première étape

On commence par sélectionner les formes quartiques $h = \sum_{\substack{S \subset \{1,\dots,8\} \\ |S|=4}} \alpha_S X_S$ tel que

$$\mathfrak{Q}(h) = \sum_{\substack{S \subset \{1,\dots,8\} \\ |S|=4}} \alpha_S \alpha_{\overline{S}} = 0$$

	self comp.	not self comp.
$\mathfrak{Q} = 1$	294	168
$\mathfrak{Q} = 0$	300	236

- Il reste 536 cas à traiter.
- Par dualité, $300 + 236/2 = 418$.

Utilisation d'un algorithme de test d'équivalence.

Seconde étape

Pour $0 \neq h \in \mathrm{RM}^*(4,8)$ satisfaisant $\mathfrak{Q}(h) = 0$, on détermine une cubique s vérifiant les équations de niveau II.

- 8 équations sur les termes de degré 3, $|V| = 7$:

$$\sum_{\substack{S \subseteq V \\ |S|=4}} \alpha_S \beta_{V \setminus S} + \sum_{\substack{\{S,T\} \mid S \cup T = V \\ |S|=|T|=4}} \alpha_S \alpha_T = 0.$$

L'ensemble des cubiques solutions s'écrit

$$\mathcal{C} + s$$

où $\mathcal{C}$ est le noyau de la multiplication par h

$$\begin{array}{ccc} \mathrm{RM}^*(3,8) & \xrightarrow{\times h} & \mathrm{RM}^*(7,8) \\ c & \longrightarrow & hc \end{array} \tag{2}$$

Le noyau est donné par 8 équations, comme $\dim \mathrm{RM}^*(3,8) = 56$, on obtient :

$$48 \leq \dim \mathcal{C} \leq 56.$$

Troisième étape

Pour chaque cubique $c + s$, on détermine les solutions de niveau III.

- 28 équations sur les termes de degré 2, $|V| = 6$:

$$\sum_{\substack{S \subseteq V \\ |S|=4}} \alpha_S \gamma_{V \setminus S} + \sum_{\substack{S \cup T = V \\ |S|=|T|=3}}' \beta_S \beta_T + \sum_{\substack{S \cup T = V \\ |S|=4, |T|=3}}' \alpha_S \beta_T + \sum_{\substack{S \cup T = V \\ |S|=|T|=4}}' \alpha_S \alpha_T = 0.$$

Elles sont données par un système de 28 équations dans $\mathrm{RM}^*(2, 8)$ qui est de dimension 28. En moyenne, on s'attend à une solution. Pour une solution q, on calcule le spectre de Fourier de

$$h + s + c + q.$$

Pour h fixée, le facteur de travail est de l'ordre de

$$2^{48} \times 2^{10} \times 2^{11} = 2^{69}.$$

Réduction par les dérivées

Supposons f courbe, notons $h = \Pi_4(f), \quad c = \Pi_3(f)$. Pour $a \in \mathbb{F}_2^8$, $f'(x) = f(x+a)$ est courbe, de plus :

$$\begin{aligned} \Pi_4(f') &= \Pi_4(f) = h \\ \Pi_3(f') &= c + \Pi_3(h(x) + h(x+a)). \end{aligned}$$

Notons

$$D_a(h) = \Pi_3(h(x) + h(x+a))$$

et considérons le sous-espace

$$\mathcal{D} = \{D_a(h) \mid a \in \mathbb{F}_2^8\}, \quad \dim \mathcal{D} = \mathrm{var}\,(h)$$

On vérifie que $\mathcal{D} \subseteq \mathcal{C}$. On décompose alors

$$\mathcal{C} = D \oplus \mathcal{C}'\,.$$

Il suffit alors de compter les fonctions courbes de la forme :

$$h + s + c + q, \quad c \in \mathcal{C}'$$

Le facteur de travail est divisé par $2^{\mathrm{var}\,(h)} \sim 256$.

Cas $\mathrm{fix}\,(h)$ trivial

Il s'agit des instances favorables pour la procédure. Le traitement d'une telle forme quartique demande de l'ordre de 18 jours.

$$\mathrm{NB}\,(h) = \sharp\mathrm{GL}(2,8) \times 2^8 \times B(h)$$

1204440	1207840	1208048	1214024	1227312
1269888	1270048	1271008	1271784	1272504
1273808	1277872	1280960	1281032	1281568
1281816	1282136	1282792	1284328	1293024
1296616				

Table: Valeurs de $B(h)$, $\sharp\mathrm{fix}\,(h) = 1$.

Idée clé pour $\mathrm{fix}\,(h)$ non trivial

Soit G un sous-groupe de Fix(h). Par définition, pour tout $A \in G$, le *bord* $h^A + h$ est dans $\mathrm{RM}(3,8)$. On vérifie que $\mathcal{C}$ est G module et que $h^A + h + s^A + s \in \mathcal{C}$. Supposons une décomposition

$$\mathcal{C} = \mathcal{W} \oplus \mathcal{R}$$

tel que

1. $\mathcal{W}$ est un G-module,
2. $\forall A \in G, \quad h^A + h + s^A + s \in \mathcal{W}$,

L'action de $A \in G$ sur $f = h + s + w + r + q$ se décompose

$$\begin{aligned} f^A &= (h + s + w + r + q)^A \\ &= h^A + s^A + w^A + r^A + q^A \\ &= h + s + (h^A + h) + (s^A + s) + w^A + r^A \mod \mathrm{RM}^*(2,8) \\ &= h + s + w' + r^A \mod \mathrm{RM}^*(2,8) \end{aligned}$$

Réduction par le fixateur

Comme $\mathcal{W}$ est un G-module, le groupe G agit sur $\mathcal{R} \simeq \mathcal{C} \,/\, \mathcal{W}$.
Pour $r \in \mathcal{R}$, on note $\mathrm{NB}\,(r, W)$ le nombre de fonctions courbes de la forme

$$f = h + s + w + r + q$$

avec $q \in \mathrm{RM}^*(2, 8)$ et $w \in W$.

$$\mathrm{NB}\,(r, W) = \mathrm{NB}\,(\Pi_{\mathcal{R}}(\Pi_3(r^A)), W).$$

Si Ω désigne un système de représentants de $\mathcal{R}$ pour la "trace" des actions de G sur $\mathcal{R}$ alors

$$\mathrm{NB}(h) = \sum_{\omega \in \Omega} \sharp\omega \times \mathrm{NB}\,(\omega, W).$$

Choix de G et $\mathcal{W}$

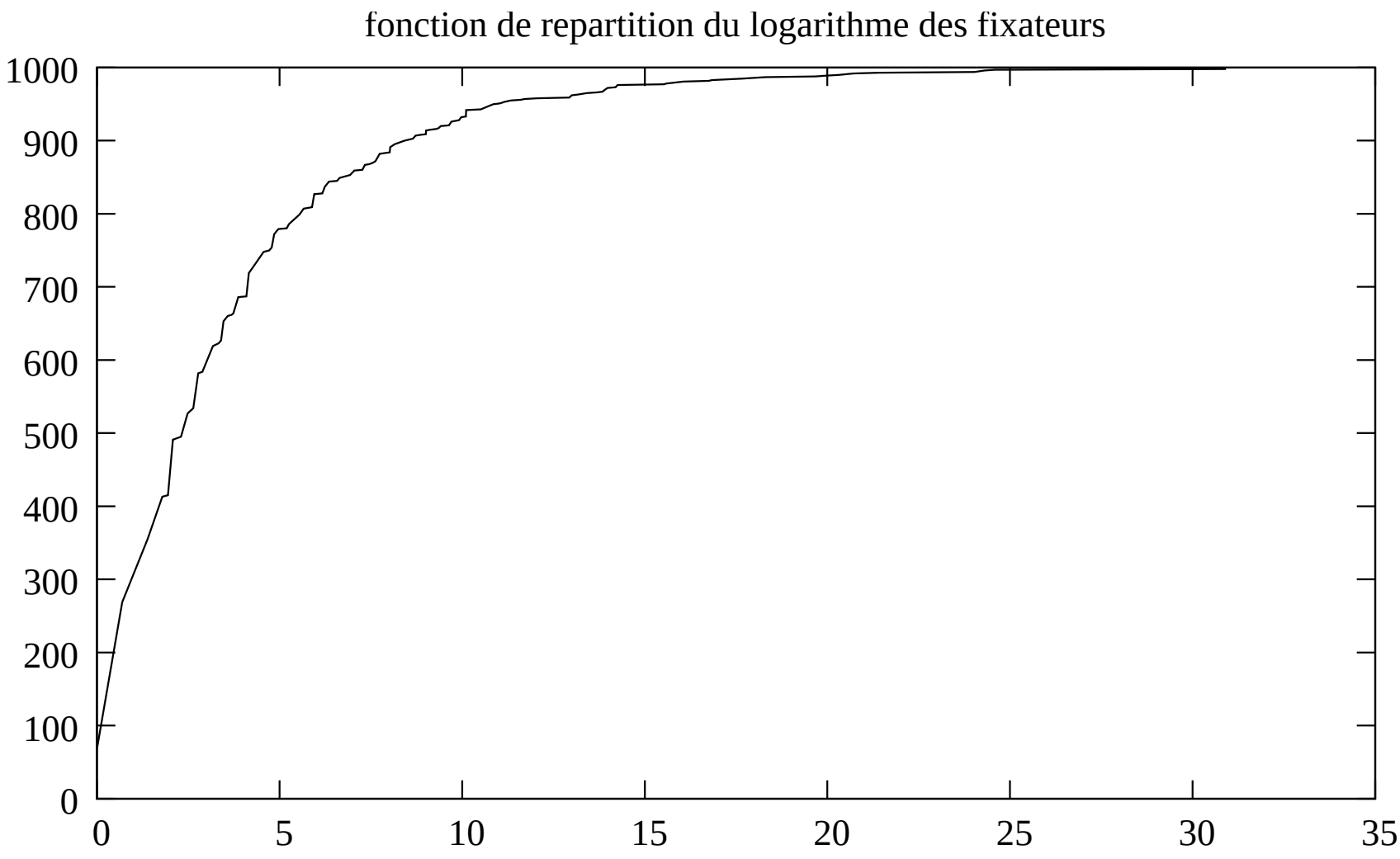
On prend $G = \mathrm{Fix}(h)$. On construit un G-module au "hasard" de co-dimension proche de 24 (dans $\mathcal{C}$), contenant les bords de $h + s$, ainsi que les dérivées de h.

- $\mathcal{D} \subseteq \mathcal{W}$, (réduction par dérivation).
- $\dim \mathcal{R} \approx 24$ (calcul orbital faisable).
- $\dim \mathcal{R} \approx 24$ (efficacité de la réduction).

Si G est trop gros (12 cas), la procédure échoue, on prend un sous-groupe de $\mathrm{Fix}(h)$. Dans tous les cas,

$$|\Omega| \approx |\mathcal{R}|/|G|.$$

ce qui donne une accélération d'un facteur de l'ordre de G, c.f. répartition.


fonction de repartition du logarithme des fixateurs
1000
900
800
700
600
500
400
300
200
100
0
0
5
10
15
20
25
30
35

Nombre de fonctions courbes

Finalement, 3 semaines de calculs (50 processeurs), suffisent pour obtenir :

$$\begin{aligned}\overline{\mathrm{NB}}(8) &= 193887869660028067003488010240 \\ &= 2^{22} \times 5 \times 7 \times 31 \times 89 \times 127 \times 376935697014273 7\end{aligned}$$

Est-ce correct ?

As, B. D. McKay explains in [8x8 Knight Tour paper], every computer programmers knows that errors in programming or execution can escape the most rigorous checking.
Moreover, the running time for the computation all bent functions took several weeks using several computers and communication network. It is longsome and one can get errors from miscellaneous devices.

Vérification

Pour p premier impair divisant l'ordre de $\mathrm{GL}(2,8)$, i.e

$$3, 5, 7, 17, 31, 127$$

il est possible de calculer le nombre de fonctions courbes modulo p.
On part d'un élément A d'ordre p dans $\mathrm{GL}(2,8)$, et on construit le sous-espace de $\mathrm{RM}(4,8)$ invariant par A.
On détermine le nombre β_p de fonctions courbes dans cet espace et donc :

$$\mathrm{NB}(4,8) \equiv \beta_p \pmod{p}.$$

Table: The number of bent functions modulo an odd prime p dividing the order of the general linear group $\mathrm{GL}(2,8)$.

p	3	5	7	17	31	127
N_p	2	0	0	13	0	0

Le nombre proposé vérifie ces congruences.

Problème ouvert

$$\overline{\mathrm{NB}}(8) \approx 2^{97.3}$$

Comment compter, ou estimer le nombre de fonctions courbes dans les classes connues (partial spreads de J. Dillon) afin d'avoir une idée plus précise de l'état des connaissances en matière de construction des fonctions courbes.