Quelques aspects de la cryptographie et du codage - partie 3

Claude Carlet
(en collaboration avec S. Mesnager)

Les codes correcteurs d'erreurs

→ Un outil visant à améliorer la fiabilité des transmissions sur un canal bruité.
Lors de la transmission sur un canal bruité :

- à l'émission : ajouter une redondance à un message.
- à la réception : détecter les erreurs et à les corriger.

→ En théorie des codes, on étudie comment :

- corriger un nombre maximum d'erreurs pour un taux de transmission donné.
- coder et décoder à moindre coût.
- s'adapter à des formes d'erreurs particulières.

Utilisation des codes correcteurs d'erreurs

- Tous les réseaux : la généralisation des satellites de télécommunications augmente le niveau de bruit.
- Supports numériques : CD, DVD (code de Reed-Salomon)
- Pour la protection de la mémoire des ordinateurs : une mémoire peut être sujette à des erreurs. La mémoire est un composant électronique sensible aux variations de courant, au champ électromagnétique ou à la chaleur.
- En cryptographie (codes de Goppa, codes de Reed-Muller ...)

Une des grandes familles de codes : Codes en blocs

L'information formée par des mots d'un alphabet fini $\mathcal{A}$, $|\mathcal{A}| = q$, est coupée en blocs $(u_1, \ldots, u_k)$ de taille constante et traitée bloc par bloc.

Définition

Un (n, k)-code est un sous-ensemble non vide formé par q^k éléments (mots) de $\mathcal{A}^n = \mathcal{A} \times \cdots \times \mathcal{A}$.

Généralement, $\mathcal{A} = \mathbb{F}_q$ (corps fini)
En pratique, $\mathcal{A} = \mathbb{F}_2 = \{0, 1\}$
dans la suite, on prendra $\mathcal{A} = \mathbb{F}_2$ (code binaire)

Une des grandes familles de codes : Codes en blocs

Schématiquement, le problème de transmission sur un canal bruité :

$$\text{Source} \to \underbrace{(u_1, \ldots, u_k)}_{\text{mot transmis}} \to \text{Encodeur} \to \underbrace{(x_1, \ldots, x_n)}_{\text{mot du code}}, n > k$$

$$\downarrow \text{canal bruité}$$

$$\underbrace{(y_1, \ldots, y_n)}_{\text{mot reçu}} \to \text{Décodeur} \to (v_1, \ldots, v_k)$$

- Détecter une erreur : savoir si $(y_1, \ldots, y_n) \stackrel{?}{=} (x_1, \ldots, x_n)$.
- Corriger cette erreur : après détection, obtenir par décodage $(v_1, \ldots, v_k) = (u_1, \ldots, u_k)$.

Que signifie décoder ?

Soit C un code sur $\mathbb{F}_2^n$.

- C’est associer au mot reçu, un mot du code.
  On cherche le plus souvent à décoder en associant à un mot, le mot du code le “*plus proche*”.

Que signifie décoder ?

Soit C un code sur $\mathbb{F}_2^n$.

- C'est associer au mot reçu, un mot du code.
  On cherche le plus souvent à décoder en associant à un mot, le mot du code le "*plus proche*".
- **Maximum de vraisemblance** : trouver le mot du code ayant la plus grande probabilité d'avoir été émis par le canal.

Que signifie décoder ?

Soit C un code sur $\mathbb{F}_2^n$.

- C'est associer au mot reçu, un mot du code.
  On cherche le plus souvent à décoder en associant à un mot, le mot du code le "*plus proche*".
- **Maximum de vraisemblance** : trouver le mot du code ayant la plus grande probabilité d'avoir été émis par le canal.

- Dans un canal binaire symétrique sans mémoire,

Que signifie décoder ?

Soit C un code sur $\mathbb{F}_2^n$.

- C'est associer au mot reçu, un mot du code.
  On cherche le plus souvent à décoder en associant à un mot, le mot du code le "*plus proche*".
- **Maximum de vraisemblance** : trouver le mot du code ayant la plus grande probabilité d'avoir été émis par le canal.

- Dans un canal binaire symétrique sans mémoire, cela revient à trouver le mot du code qui est le plus proche au sens de la distance de Hamming d_H définie par :
  $d_H(x,y) = \#\{i \text{ tel que } x_i \neq y_i\}, x, y \in \mathbb{F}_2^n$.
  Mais un décodage complet (de n'importe quel mot de $\mathbb{F}_2^n$) à maximum de vraisemblance est un problème très difficile !

Que signifie décoder ?

Soit C un code sur $\mathbb{F}_2^n$.

- C'est associer au mot reçu, un mot du code.
  On cherche le plus souvent à décoder en associant à un mot, le mot du code le "*plus proche*".
- **Maximum de vraisemblance** : trouver le mot du code ayant la plus grande probabilité d'avoir été émis par le canal.
- On effectue un décodage borné : décodage par un mot quelconque du code qui se trouve à une distance inférieure à une borne fixée r.
  la valeur minimale de r pour laquelle l'espace $\mathbb{F}_2^n$ est entièrement décodable est appelé le rayon de recouvrement ρ de $\mathcal{C}$.

Définitions

- Boule de Hamming :

$$x \in \mathbb{F}_2^n, \quad B(x, r) = \{y \in \mathbb{F}_2^n \mid d_H(x, y) \leq r\}$$

- Rayon de recouvrement d'un code binaire $\mathcal{C}$

$$\rho = \min\{r \in \mathbb{N} \mid \bigcup_{x \in C} B(x, r) = \mathbb{F}_2^n\}$$

On a : $\rho = \max_{x \in \mathbb{F}_2^n} \min_{y \in C} d_H(x, y)$.
ρ mesure la distance maximale entre le code $\mathcal{C}$ et l'ensemble des vecteurs de $\mathbb{F}_2^n$.
Décodage borné jusqu'à ρ : décodage complet
De plus, le calcul de ρ est un problème difficile !

Distance minimale

Distance minimale de $\mathcal{C}$: d_{min}

$$d_{min} = \min\{d_H(x,y) \mid x,y \in \mathcal{C}\}$$

$\mathcal{C}$ est un code $(d_{min}-1)$-détecteur d'erreurs et un code $e = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$-correcteur d'erreurs.
e est la capacité de correction de $\mathcal{C}$.
$(e = \max\{r \mid \bigcap_{x\in\mathcal{C}} B(x,r) = \emptyset\})$
Décodage borné jusqu'à $\left\lfloor \frac{d_{min}-1}{2} \right\rfloor$: décodage (unique) à maximum de vraisemblance.

Distance minimale et rayon de recouvrement

- Inégalité de Hamming : si $\mathcal{C}$ est de longueur n et de cardinal 2^k alors on a $1 + \binom{n}{1} + \cdots + \binom{n}{e} \leq 2^{n-k}$.
- $e \leq \rho$ et $d_{min} \leq 2\rho + 1$.
- $\mathcal{C}$ est dit *parfait* si $e = \rho$. Dans ce cas, on a un décodage complet à maximum de vraisemblance.

Les codes linéaires

C'est la plus grande sous-famille de codes correcteurs d'erreurs en blocs :

- Un code $\mathcal{C} \subseteq \mathbb{F}_2^n$ est dit *linéaire* si $\mathcal{C}$ est un sous-espace vectoriel de $\mathbb{F}_2^n$.
  matrice génératrice

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

$00 \rightarrow 00000$ $01 \rightarrow 01011$	$10 \rightarrow 10110$ $11 \rightarrow 11101$

Le code $\mathcal{C}$ défini par $\mathcal{G}$ est $\{u\mathcal{G}, u \in \mathbb{F}_2^2\}$

Les codes linéaires

C'est la plus grande sous-famille de codes correcteurs d'erreurs en blocs :

- Un code $\mathcal{C} \subseteq \mathbb{F}_2^n$ est dit *linéaire* si $\mathcal{C}$ est un sous-espace vectoriel de $\mathbb{F}_2^n$.
  matrice génératrice

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

$$\mathrm{a} = 01100011$$

$$01|10|00|11 \longrightarrow 01011|10110|00000|11101$$

Les codes linéaires : terminologie

- Le code $\mathcal{C}$: espace vectoriel engendré par $\mathcal{G}$.
- La dimension k : dimension de $\mathcal{C}$.
- La longueur n : nombre de colonnes de $\mathcal{G}$.
- Le poids de Hamming, noté wt : nombre de coordonnées non nulles d'un mot.
- La distance minimale d_{min} : distance de Hamming minimale entre deux mots du code.

On dit que $\mathcal{C}$ est un code binaire de paramètres $[n, k, d_{min}]$.

Codes de Reed-Muller (binaires) d'ordre r et de longueur 2^n : $\mathcal{RM}(r,n)$

➔ peut être défini en termes de fonctions booléennes :
$f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$.
f peut être representée par sa table de vérité ou par sa forme algébrique normale : $f(x_1,\ldots,x_n) = \bigoplus_{I\subseteq\{1\ldots,n\}} a_I \prod_{i\in I} x_i$,
$a_I \in \mathbb{F}_2$, $\deg(f) = \max\{|I| \text{ tel que } a_I \neq 0\}$

$$f(x) = x_1x_2x_3 + x_1x_4 + x_2$$

x_1	x_2	x_3	x_4	$x_1x_2x_3$	x_1x_4	$f(x)$	$(-1)^{f(x)}$				$\widehat{\chi_f}(x)$
0	0	0	0	0	0	0	1	2	4	0	0
1	0	0	0	0	0	0	1	0	0	0	0
0	1	0	0	0	0	1	-1	-2	-4	8	8
1	1	0	0	0	0	1	-1	0	0	0	8
0	0	1	0	0	0	0	1	2	0	0	0
1	0	1	0	0	0	0	1	0	0	0	0
0	1	1	0	0	0	1	-1	-2	0	0	0
1	1	1	0	1	0	0	1	0	0	0	0
0	0	0	1	0	0	0	1	0	0	0	4
1	0	0	1	0	1	1	-1	2	4	4	-4
0	1	0	1	0	0	1	-1	0	0	0	4
1	1	0	1	0	1	0	1	-2	0	4	-4
0	0	1	1	0	0	0	1	0	0	0	-4
1	0	1	1	0	1	1	-1	2	0	-4	4
0	1	1	1	0	0	1	-1	0	0	0	4
1	1	1	1	1	1	1	-1	2	-4	4	-4

TAB.: table de vérité de f (equilibrée optimale)

Définitions

- $\mathcal{B}_n$=ensemble des fonctions booléennes de $\mathbb{F}_2^n$ dans $\mathbb{F}_2$.
- $\mathcal{RM}(r,n)$=ensemble des fonctions booléennes de $\mathcal{B}_n$ de degré algébrique au plus r.
- $\mathcal{RM}(r,n)$ est un code linéaire de paramètres $\left[2^n, \sum_{i=0}^{r}\binom{2^n}{i}, 2^{n-r}\right]$.
- $d_H(f,g) = \#\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\}$

Définition

$$\rho(r,n) = \max_{f\in\mathcal{B}_n} \min_{g\in\mathcal{RM}(r,n)} \mathrm{d_H}(f,g)$$

Valeurs exactes sur le rayon de recouvrement pour $n \leq 9$

$r \backslash n$	1	2	3	4	5	6	7	8	9
1	0	1	2	6	12	28	56	120	
2		0	1	2	6	18			
3			0	1	2	8			
4				0	1	2	8		
5					0	1	2	10	
6						0	1	2	10
7							0	1	2
8								0	1
9									0

Bornes supérieures sur le rayon de recouvrement obtenues par Hou

$r \backslash n$	1	2	3	4	5	6	7	8	9
1	0	1	2	6	12	28	56	120	
2		0	1	2	6	18	44		
3			0	1	2	8	23		
4				0	1	2	8		
5					0	1	2	10	
6						0	1	2	10
7							0	1	2
8								0	1
9									0

Bornes connues sur le rayon de recouvrement pour $n \leq 9$

$r \backslash n$	1	2	3	4	5	6	7	8	9
1	0	1	2	6	12	28	56	120	244
2		0	1	2	6	18	44	100	220
3			0	1	2	8	23	67	167
4				0	1	2	8	31	98
5					0	1	2	10	41
6						0	1	2	10
7							0	1	2
8								0	1
9									0

$$\rho(r,n) \leq \rho(r-1,n-1) + \rho(r,n-1)$$

Bornes connues sur le rayon de recouvrement pour $n \geq 10$

Théorème

$$\rho(1, n) = 2^{n-1} - 2^{\frac{n}{2}-1} \textit{ si n est pair}$$

$$\rho(1, n) \leq 2^{n-1} - 2^{\frac{n}{2}-1} \textit{ si n est impair}$$

Bornes connues sur le rayon de recouvrement pour $n \geq 10$

Théorème

$$\rho(1,n) = 2^{n-1} - 2^{\frac{n}{2}-1} \text{ si } n \text{ est pair}$$

$$\rho(1,n) \leq 2^{n-1} - 2^{\frac{n}{2}-1} \text{ si } n \text{ est impair}$$

Théorème (Cohen, Litsyn'92)

Pour $2 \leq r \leq n$, on a

$$\rho(r,n) \leq 2^{n-1} - (1+\sqrt{2})^{r-1} \cdot 2^{\frac{n}{2}-1} + O\left(n^{r-2}\right)$$

Obtention d'une nouvelle borne sur le rayon de recouvrement de $\mathcal{RM}(2,n)$

Théorème

Pour $n \geq 15$

$$\rho(2,n) \leq \left\lfloor 2^{n-1} - \sqrt{15}\, 2^{\frac{n}{2}-1} \left(1 - \frac{40609}{21 \cdot 2^n} - \frac{25156284173}{4410 \cdot 2^{2n}}\right) \right\rfloor$$

n	6	7	8	9	10	11	12	13	14
Borne	20	47	104	236	469	1009	1961	3950	7980

Meilleurs résultats connus à ce jour sur le rayon de recouvrement de $\mathcal{RM}(2, n)$

Théorème

Pour $n \geq 15$

$$\rho(2,n) \leq \left\lfloor 2^{n-1} - \sqrt{15}\, 2^{\frac{n}{2}-1} \left(1 - \frac{40609}{21 \cdot 2^n} - \frac{25156284173}{4410 \cdot 2^{2n}}\right) \right\rfloor$$

n	6	7	8	9	10	11	12	13	14
Borne	18	44	100	220	464	960	1961	3950	7980

$$\rho(2,n) \leq \rho(1,n-1) + \rho(2,n-1)$$

Obtention d'une nouvelle borne asymptotique sur le rayon de recouvrement de $\mathcal{RM}(r, n)$

Théorème

Pour $3 \leq r \leq n$, on a

$$\rho(r, n) \leq 2^{n-1} - (1+\sqrt{2})^{r-2} \cdot \sqrt{15} \cdot 2^{\frac{n}{2}-1} + O\left(n^{r-2}\right)$$

Théorème (Cohen, Litsyn'92)

Pour $3 \leq r \leq n$, on a

$$\rho(r, n) \leq 2^{n-1} - (1+\sqrt{2})^{r-1} \cdot 2^{\frac{n}{2}-1} + O\left(n^{r-2}\right)$$

$$\rho(r, n) \leq \rho(r-1, n-1) + \rho(r, n-1)$$

Préliminaire

Définition

$$\rho(r,n) = \max_{f \in \mathcal{B}_n} \min_{g \in \mathcal{RM}(r,n)} \mathrm{d_H}(f,g)$$

Préliminaire

Définition

$$\rho(r,n) = \max_{f\in\mathcal{B}_n} \min_{g\in\mathcal{RM}(r,n)} \mathrm{d_H}(f,g)$$

La distance de Hamming entre deux fonction booléennes peut se réécrire

$$\mathrm{d_H}(f,g) = 2^{n-1} - \frac{1}{2}\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+g(x)}$$

Préliminaire

Définition

$$\rho(r,n) = \max_{f\in\mathcal{B}_n} \min_{g\in\mathcal{RM}(r,n)} \mathrm{d_H}(f,g)$$

La distance de Hamming entre deux fonction booléennes peut se réécrire

$$\mathrm{d_H}(f,g) = 2^{n-1} - \frac{1}{2}\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+g(x)}$$

$$\rho(r,n) = \max_{f\in\mathcal{B}_n}\left(2^{n-1} - \frac{1}{2}\max_{g\in\mathcal{RM}(r,n)}\left|\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+g(x)}\right|\right)$$

Remarque

Remarque

$\rho(1, n)$ coïncide avec la non-linéarité maximale des fonctions booléennes à n variables :

$$\mathrm{nlmax}(n) = \max_{f \in \mathcal{B}_n} \left(2^{n-1} - \frac{1}{2} \max_{\omega \in \mathbb{F}_2^n} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\omega \cdot x} \right| \right)$$

$\widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\omega \cdot x}$: transformée de Walsh de f en $\omega \in \mathbb{F}_2^n$.

Cas $r = 1$

Notation : $\#\mathcal{RM}(r,n)$=cardinal de $\mathcal{RM}(r,n)$

Identité de Parseval peut se réécrire : pour toute fonction booléenne $f \in \mathcal{B}_n$,

$$\sum_{l \in \mathcal{RM}(1,n)} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+l(x)} \right)^2 = 2^n \, \#\mathcal{RM}(1,n)$$

Cas $r = 1$

Notation : $\#\mathcal{RM}(r,n)$=cardinal de $\mathcal{RM}(r,n)$

Identité de Parseval peut se réécrire : pour toute fonction booléenne $f \in \mathcal{B}_n$,

$$\sum_{l \in \mathcal{RM}(1,n)} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+l(x)} \right)^2 = 2^n \, \#\mathcal{RM}(1,n)$$

Donc

$$\max_{l \in \mathcal{RM}(1,n)} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+l(x)} \right|^2 \geq 2^n$$

$$\rho(1,n) = \max_{f \in \mathcal{B}_n} \left(2^{n-1} - \frac{1}{2} \max_{l \in \mathcal{RM}(1,n)} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+l(x)} \right| \right)$$

Cas $r = 1$

Notation : $\#\mathcal{RM}(r, n)$=cardinal de $\mathcal{RM}(r, n)$

Identité de Parseval peut se réécrire : pour toute fonction booléenne $f \in \mathcal{B}_n$,

$$\sum_{l \in \mathcal{RM}(1,n)} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+l(x)} \right)^2 = 2^n \, \#\mathcal{RM}(1, n)$$

Donc

$$\max_{l \in \mathcal{RM}(1,n)} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+l(x)} \right|^2 \geq 2^n$$

dont on déduit

$$\rho(1, n) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$$

Il y a égalité quand n est pair.

Cas $r = 2$

On pose, pour $f \in \mathcal{B}_n$ et $k \in \mathbb{N}$,

$$\mathcal{S}_k(f) = \sum_{g \in \mathcal{RM}(2,n)} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right)^{2k}$$

Cas $r = 2$

On pose, pour $f \in \mathcal{B}_n$ et $k \in \mathbb{N}$,

$$\mathcal{S}_k(f) = \sum_{g \in \mathcal{RM}(2,n)} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right)^{2k}$$

$$\begin{aligned}\rho(2,n) &= \max_{f \in \mathcal{B}_n} \left(2^{n-1} - \frac{1}{2} \max_{g \in \mathcal{RM}(2,n)} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right| \right) \\ &= 2^{n-1} - \frac{1}{2} \min_{f \in \mathcal{B}_n} \max_{g \in \mathcal{RM}(2,n)} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right|\end{aligned}$$

Cas $r = 2$

On pose, pour $f \in \mathcal{B}_n$ et $k \in \mathbb{N}$,

$$\mathcal{S}_k(f) = \sum_{g \in \mathcal{RM}(2,n)} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right)^{2k}$$

On a, pour toute fonction booléenne $f \in \mathcal{B}_n$ et pour tout entier $k \in \mathbb{N}$,

$$\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)} \leq \max_{g \in \mathcal{RM}(2,n)} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right|^2$$

$$\rho(2, n) = 2^{n-1} - \frac{1}{2} \min_{f \in \mathcal{B}_n} \max_{g \in \mathcal{RM}(2,n)} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right|$$

Cas $r = 2$

On pose, pour $f \in \mathcal{B}_n$ et $k \in \mathbb{N}$,

$$\mathcal{S}_k(f) = \sum_{g \in \mathcal{RM}(2,n)} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right)^{2k}$$

On a, pour toute fonction booléenne $f \in \mathcal{B}_n$ et pour tout entier $k \in \mathbb{N}$,

$$\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)} \leq \max_{g \in \mathcal{RM}(2,n)} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right|^2$$

$$\boxed{\rho(2,n) \leq 2^{n-1} - \frac{1}{2} \min_{f \in \mathcal{B}_n} \sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}}}$$

Cas $r = 2$

On pose, pour $f \in \mathcal{B}_n$ et $k \in \mathbb{N}$,

$$\mathcal{S}_k(f) = \sum_{g \in \mathcal{RM}(2,n)} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right)^{2k}$$

On a, pour toute fonction booléenne $f \in \mathcal{B}_n$ et pour tout entier $k \in \mathbb{N}$,

$$\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)} \leq \max_{g \in \mathcal{RM}(2,n)} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right|^2$$

$$\forall f \in \mathcal{B}_n, \forall k \in \mathbb{N}, \quad \frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)} \leq \frac{\mathcal{S}_{k+2}(f)}{\mathcal{S}_{k+1}(f)}$$

Cas $r = 2$

On pose, pour $f \in \mathcal{B}_n$ et $k \in \mathbb{N}$,

$$\mathcal{S}_k(f) = \sum_{g \in \mathcal{RM}(2,n)} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right)^{2k}$$

On a, pour toute fonction booléenne $f \in \mathcal{B}_n$ et pour tout entier $k \in \mathbb{N}$,

$$\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)} \leq \max_{g \in \mathcal{RM}(2,n)} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right|^2$$

$$\lim_{k \to +\infty} \sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}} = \max_{g \in \mathcal{RM}(2,n)} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right|$$

Grandes lignes de la preuve

$$\boxed{\rho(2,n) \leq 2^{n-1} - \frac{1}{2}\min_{f\in\mathcal{B}_n}\sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}}}$$

Pour obtenir une borne supérieure sur $\rho(2,n)$, on cherche une borne inférieure sur $\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}$ uniforme en $f \in \mathcal{B}_n$.

1. Décomposition de $\mathcal{S}_k(f)$ en sommes de caractère.
2. Minoration des termes de cette décomposition à l'aide de la caractérisation des mots des codes de Reed-Muller donnée par Kazami, Tokura et Azumi : $\forall f \in \mathcal{B}_n$, $\mathcal{S}_k(f) \geq \mathcal{S}_k^{min}$.
3. On obtient la borne supérieure $\rho(2,n) \leq 2^{n-1} - \frac{1}{2}\sqrt{\frac{\mathcal{S}_{k+1}^{min}}{\mathcal{S}_k^{min}}}$ pour $k \leq \mathrm{k}_n$ où k_n varie selon la valeur de n.

Grandes lignes de la preuve

$$\boxed{\rho(2,n) \leq 2^{n-1} - \frac{1}{2} \min_{f \in \mathcal{B}_n} \sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}}}$$

Pour obtenir une borne supérieure sur $\rho(2,n)$, on cherche une borne inférieure sur $\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}$ uniforme en $f \in \mathcal{B}_n$.

1. Décomposition de $\mathcal{S}_k(f)$ en sommes de caractère.
2. Minoration des termes de cette décomposition à l'aide de la caractérisation des mots des codes de Reed-Muller donnée par Kazami, Tokura et Azumi : $\forall f \in \mathcal{B}_n$, $\mathcal{S}_k(f) \geq \mathcal{S}_k^{min}$.
3. On obtient la borne supérieure $\rho(2,n) \leq 2^{n-1} - \frac{1}{2}\sqrt{\frac{\mathcal{S}_{k+1}^{min}}{\mathcal{S}_k^{min}}}$

   pour $k \leq \mathrm{k}_n$ où k_n varie selon la valeur de n.

Grandes lignes de la preuve

$$\boxed{\rho(2,n) \leq 2^{n-1} - \frac{1}{2} \min_{f \in \mathcal{B}_n} \sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}}}$$

Pour obtenir une borne supérieure sur $\rho(2,n)$, on cherche une borne inférieure sur $\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}$ uniforme en $f \in \mathcal{B}_n$.

1. Décomposition de $\mathcal{S}_k(f)$ en sommes de caractère.
2. Minoration des termes de cette décomposition à l'aide de la caractérisation des mots des codes de Reed-Muller donnée par Kazami, Tokura et Azumi : $\forall f \in \mathcal{B}_n$, $\mathcal{S}_k(f) \geq \mathcal{S}_k^{min}$.
3. On obtient la borne supérieure $\rho(2,n) \leq 2^{n-1} - \frac{1}{2}\sqrt{\frac{\mathcal{S}_{k+1}^{min}}{\mathcal{S}_k^{min}}}$ pour $k \leq \mathrm{k}_n$ où k_n varie selon la valeur de n.

Décomposition de $\mathcal{S}_k(f)$ en sommes de caractère

$$\boxed{\mathcal{S}_k(f) = \sum_{g \in \mathcal{RM}(2,n)} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right)^{2k}}$$

$$\left(\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right)^{2k} = \sum_{(x_1,\dots,x_{2k}) \in \left(\mathbb{F}_2^n\right)^{2k}} (-1)^{\langle f, \sum_{i=1}^{2k} 1_{x_i} \rangle + \langle g, \sum_{i=1}^{2k} 1_{x_i} \rangle}$$

$< f, g >= \sum_{x \in \mathbb{F}_2^n} f(x)g(x)$, 1_x désigne la fonction Booléenne de support $\{x\}$

Décomposition de $\mathcal{S}_k(f)$ en sommes de caractère

$$\mathcal{S}_k(f) = \sum_{g\in\mathcal{RM}(2,n)} \sum_{(x_1,\ldots,x_{2k})\in\left(\mathbb{F}_2^n\right)^{2k}} (-1)^{\langle f,\sum_{i=1}^{2k} 1_{x_i}\rangle + \langle g,\sum_{i=1}^{2k} 1_{x_i}\rangle}$$

Décomposition de $\mathcal{S}_k(f)$ en sommes de caractère

$$\mathcal{S}_k(f) = \sum_{g \in \mathcal{RM}(2,n)} \sum_{(x_1,\dots,x_{2k}) \in \left(\mathbb{F}_2^n\right)^{2k}} (-1)^{\langle f, \sum_{i=1}^{2k} 1_{x_i} \rangle + \langle g, \sum_{i=1}^{2k} 1_{x_i} \rangle}$$

Lemme

$$\sum_{g \in \mathcal{RM}(2,n)} (-1)^{\langle g,h \rangle} = \begin{cases} \#\mathcal{RM}(2,n) & si\ h \in \mathcal{RM}(n-3,n) \\ 0 & sinon \end{cases}$$

$h \in \mathcal{B}_n$, $g \in \mathcal{B}_n \mapsto (-1)^{\langle g,h \rangle}$ caractère de $\mathcal{B}_n$ muni de l'addition $\oplus$.

Décomposition de $\mathcal{S}_k(f)$ en sommes de caractère

$$\mathcal{S}_k(f) = \#\mathcal{RM}(2,n) \sum_{\substack{(x_1,\ldots,x_{2k})\in\left(\mathbb{F}_2^n\right)^{2k} \\ \sum_{i=1}^{2k} 1_{x_i}\in\mathcal{RM}(n-3,n)}} (-1)^{\langle f, \sum_{i=1}^{2k} 1_{x_i}\rangle}$$

Décomposition de $\mathcal{S}_k(f)$ en sommes de caractère

$$\mathcal{S}_k(f) = \#\mathcal{RM}(2,n) \sum_{g \in \mathcal{RM}(n-3,n)} (-1)^{\langle f,g \rangle} N_k^{(g)}$$

- $N_k^{(g)}$ désigne le nombre de $2k$-uplets $(x_1,\ldots,x_{2k})$ de vecteurs de $\mathbb{F}_2^n$ tels que $\sum_{i=1}^{2k} 1_{x_i} = g$
- $N_k^{(g)}$ ne dépend que du poids de Hamming de g

Décomposition de $\mathcal{S}_k(f)$ en sommes de caractère

- Tous les poids des éléments de $\mathcal{RM}(n-3,n)$ sont pairs : $w = 0, 2, \ldots$
- La distance minimale de $\mathcal{RM}(n-3,n)$ est 8 : $w = 0, 8, \ldots$
- Il n'y a pas de mot de poids de Hamming égal à 10 : $w = 0, 8, 12, \ldots$

Décomposition de $\mathcal{S}_k(f)$ en sommes de caractère

- Tous les poids des éléments de $\mathcal{RM}(n-3,n)$ sont pairs : $w = 0, 2, \ldots$
- La distance minimale de $\mathcal{RM}(n-3,n)$ est 8 : $w = 0, 8, \ldots$
- Il n'y a pas de mot de poids de Hamming égal à 10 : $w = 0, 8, 12, \ldots$

Décomposition de $\mathcal{S}_k(f)$ en sommes de caractère

- Tous les poids des éléments de $\mathcal{RM}(n-3,n)$ sont pairs : $w = 0, 2, \ldots$
- La distance minimale de $\mathcal{RM}(n-3,n)$ est 8 : $w = 0, 8, \ldots$
- Il n'y a pas de mot de poids de Hamming égal à 10 : $w = 0, 8, 12, \ldots$

Décomposition de $\mathcal{S}_k(f)$ en sommes de caractère

$g = 0$:
Un $2k$-uplet $(x_1, \ldots, x_{2k})$ tel que $\sum_{i=1}^{2k} 1_{x_i} = 0$ est formé avec k paires de vecteurs de $\mathbb{F}_2^n$.

- Les paires ne sont pas nécessairement distinctes.

Les éléments du $2k$-uplet forment donc un multi-ensemble tel que

- La multiplicité de chaque élément est paire.
- L'ensemble des multiplicités forme une composition de $2k$.

Décomposition de $\mathcal{S}_k(f)$ en sommes de caractère

$g = 0$:
Un $2k$-uplet $(x_1,\dots,x_{2k})$ tel que $\sum_{i=1}^{2k} 1_{x_i} = 0$ est formé avec k paires de vecteurs de $\mathbb{F}_2^n$.

- Les paires ne sont pas nécessairement distinctes.

Les éléments du $2k$-uplet forment donc un multi-ensemble tel que

- La multiplicité de chaque élément est paire.
- L'ensemble des multiplicités forme une composition de $2k$.

$$N_k^{(0)} = \sum_{i=1}^{k} \binom{2^n}{i} \sum_{2p_1+\cdots+2p_i=2k} \frac{(2k)!}{\prod_{j=1}^{i}(2p_j)!}$$

Décomposition de $\mathcal{S}_k(f)$ en sommes de caractère

$g = 0$:
Un $2k$-uplet $(x_1, \ldots, x_{2k})$ tel que $\sum_{i=1}^{2k} 1_{x_i} = 0$ est formé avec k paires de vecteurs de $\mathbb{F}_2^n$.

- Les paires ne sont pas nécessairement distinctes.

Les éléments du $2k$-uplet forment donc un multi-ensemble tel que

- La multiplicité de chaque élément est paire.
- L'ensemble des multiplicités forme une composition de $2k$.

$$N_k^{(0)} = \sum_{i=1}^{k} \binom{2^n}{i} \sum_{2p_1+\cdots+2p_i=2k} \frac{(2k)!}{\prod_{j=1}^{i}(2p_j)!}$$

$N_k^{(0)}$ est le coefficient d'ordre $2k$ dans le développement en série de Taylor de $y \mapsto \cosh^{2^n}(y)$ en $y = 0$.

Décomposition de $\mathcal{S}_k(f)$ en sommes de caractère

Soit $g \in \mathcal{RM}(n-3,n)$ de poids de Hamming $2w = 8, 12, \ldots$:
Un $2k$-uplet $(x_1, \ldots, x_{2k})$ tel que $\sum_{i=1}^{2k} 1_{x_i} = g$ est formé avec

$2w$ points du support de g	$k-w$ paires de vecteurs de $\mathbb{F}_2^n$

$N_k^{(g)}$ est le coefficient d'ordre $2k$ dans le développement en série de Taylor de $y \mapsto \tanh^{2w}(y) \cosh^{2^n}(y)$ en $y = 0$.

Décomposition de $\mathcal{S}_k(f)$ en sommes de caractère

Lemme

$$\mathcal{S}_k(f) = \#\mathcal{RM}(2,n)\left(N_k^{(0)} + N_k^{(8)}M_f^{(8)} + \sum_{w=6}^{k} N_k^{(2w)}M_f^{(2w)}\right)$$

$N_k^{(2w)}$ =*coefficient d'ordre* $2k$ *dans le développement en série de Taylor de* $y \mapsto \tanh^{2w}(y)\cosh^{2^n}(y)$

$$M_f^{(2w)} = \sum_{\substack{g\in\mathcal{RM}(n-3,n)\\ \mathrm{wt}(g)=2w}} (-1)^{\langle f,g\rangle}$$

Minoration des sommes de caractère $M_f^{(2w)}$

- On utilise la caractérisation des mots des codes de Reed-Muller $\mathcal{RM}(r,n)$ donnée par Kasami, Tokura et Azumi de poids de Hamming $2w$ compris entre $d_{min} = 2^{n-r}$ (inclus) et $2.5d_{min}$ (exclu) : $r = n - 3$, $8 \leq 2w \leq 18$.
  - $2w = 8$: les mots de poids de Hamming égal à 8 sont les indicatrices 1_A des espaces affines A de $\mathbb{F}_2^n$ de dimension 3.
  - $12 \leq 2w \leq 16$: les mots de poids de Hamming égal à $2w$ sont de la forme $1_{A_1} \oplus 1_{A_2}$ où A_1 et A_2 sont deux espaces affines de $\mathbb{F}_2^n$ de dimension 3 distincts.
- La principale difficulté est d'obtenir des minorations sur $M_f^{(2w)}$ qui soient uniformes en $f \in \mathcal{B}_n$.

Minoration des sommes de caractère $M_f^{(8)}$

Les mots de poids 8 étant les indicatrices 1_A des espaces affines A de $\mathbb{F}_2^n$ de dimension 3. La somme $M_f^{(8)}$ se réécrit :

$$M_f^{(8)} = \sum_{A \in \mathcal{A}_3} (-1)^{\langle f, 1_A \rangle}$$

$\mathcal{A}_3$=ensemble des espaces affines de $\mathbb{F}_2^n$ de dimension 3

Minoration des sommes de caractère $M_f^{(8)}$

Les mots de poids 8 étant les indicatrices 1_A des espaces affines A de $\mathbb{F}_2^n$ de dimension 3. La somme $M_f^{(8)}$ se réécrit :

$$M_f^{(8)} = \sum_{A \in \mathcal{A}_3} (-1)^{\langle f, 1_A \rangle}$$

$\mathcal{A}_3$=ensemble des espaces affines de $\mathbb{F}_2^n$ de dimension 3

Idée : Tout espace affine A de dimension 3 peut s'écrire de $2(2^3 - 1)$ façons comme l'union disjointe $F_1 \cup F_2$ de deux espaces affines de dimension 2 tels que $F_1 \parallel F_2$.

Minoration des sommes de caractère $M_f^{(8)}$

La somme $M_f^{(8)}$ se réécrit :

$$M_f^{(8)} = \frac{1}{2(2^3-1)} \sum_{\substack{F_1,F_2\in\mathcal{A}_2\\ F_1\|F_2\\ F_1\neq F_2}} (-1)^{\langle f, 1_{F_1}+1_{F_2}\rangle}$$

$$= \frac{1}{2(2^3-1)} \left(\sum_{\substack{F_1,F_2\in\mathcal{A}_2\\ F_1\|F_2}} (-1)^{\langle f, 1_{F_1}+1_{F_2}\rangle} - \underbrace{\#\mathcal{A}_2}_{F_1=F_2} \right)$$

$\mathcal{A}_2$=ensemble des espaces affines de $\mathbb{F}_2^n$ de dimension 2

Deux espaces affines F_1 et F_2 de dimension 2 parallèles s'écrivent : $F_1 = u_1 + E$ et $F_2 = u_2 + E$, u_1, $u_2 \in \mathbb{F}_2^n$, E espace vectoriel de dimension 2. Il y a 2^2 façons d'écrire $F \in \mathcal{A}_2$ sous la forme $u + E$.

Minoration des sommes de caractère $M_f^{(8)}$

La somme $M_f^{(8)}$ se réécrit donc :

$$M_f^{(8)} = \frac{1}{2(2^3-1)}\left(\frac{1}{2^4}\sum_{E\in\mathcal{E}_2}\sum_{u_1,u_2\in\mathbb{F}_2^n}(-1)^{\langle f,1_{u_1+E}\rangle+\langle f,1_{u_2+E}\rangle} - \#\mathcal{A}_2\right)$$

Soit :

- $\mathcal{E}_2$=ensemble des espaces vectoriels de $\mathbb{F}_2^n$ de dimension 2
- $\#\mathcal{A}_2 = \frac{2^{n-2}(2^n-1)(2^n-2)}{(2^2-1)(2^2-2)}$

Minoration des sommes de caractère $M_f^{(8)}$

La somme $M_f^{(8)}$ se réécrit donc :

$$M_f^{(8)} = \frac{1}{2(2^3-1)}\left(\frac{1}{2^4}\sum_{E\in\mathcal{E}_2}\sum_{u_1,u_2\in\mathbb{F}_2^n}(-1)^{\langle f,1_{u_1+E}\rangle+\langle f,1_{u_2+E}\rangle} - \#\mathcal{A}_2\right)$$

Soit :

$$M_f^{(8)} = \frac{1}{2(2^3-1)}\left(\frac{1}{2^4}\sum_{E\in\mathcal{E}_2}\left(\sum_{u\in\mathbb{F}_2^n}(-1)^{\langle f,1_{u+E}\rangle}\right)^2 - \#\mathcal{A}_2\right)$$

- $\mathcal{E}_2$=ensemble des espaces vectoriels de $\mathbb{F}_2^n$ de dimension 2
- $\#\mathcal{A}_2 = \frac{2^{n-2}(2^n-1)(2^n-2)}{(2^2-1)(2^2-2)}$

Minoration des sommes de caractère $M_f^{(8)}$

La somme $M_f^{(8)}$ se réécrit donc :

$$M_f^{(8)} = \frac{1}{2(2^3-1)}\left(\frac{1}{2^4}\sum_{E\in\mathcal{E}_2}\sum_{u_1,u_2\in\mathbb{F}_2^n}(-1)^{\langle f,1_{u_1+E}\rangle+\langle f,1_{u_2+E}\rangle} - \#\mathcal{A}_2\right)$$

Soit :

$$\begin{aligned} M_f^{(8)} &= \frac{1}{2(2^3-1)}\left(\frac{1}{2^4}\sum_{E\in\mathcal{E}_2}\left(\sum_{u\in\mathbb{F}_2^n}(-1)^{\langle f,1_{u+E}\rangle}\right)^2 - \#\mathcal{A}_2\right) \\ &\geq -\frac{\#\mathcal{A}_2}{2(2^3-1)} = -\frac{2^{n-2}(2^n-1)(2^n-2)}{2(2^3-1)(2^2-1)(2^2-2)} \end{aligned}$$

- $\mathcal{E}_2$=ensemble des espaces vectoriels de $\mathbb{F}_2^n$ de dimension 2
- $\#\mathcal{A}_2 = \frac{2^{n-2}(2^n-1)(2^n-2)}{(2^2-1)(2^2-2)}$

Minoration des sommes de caractère $M_f^{(12)}$

Les mots de poids 12 s'écrivant $1_{A_1} \oplus 1_{A_2}$ où A_1 et A_2 sont deux espaces affines de dimension 3 dont l'intersection est un espace affine de dimension 1, la somme $M_f^{(12)}$ se réécrit :

$$M_f^{(12)} = \frac{1}{2} \sum_{\substack{A_1, A_2 \in \mathcal{A}_3 \\ \dim(A_1 \cap A_2) = 1}} (-1)^{\langle f, 1_{A_1} \rangle + \langle f, 1_{A_2} \rangle}$$

Si A_1 et A_2 sont deux espaces affines de dimension 3 dont l'intersection est un espace affine de dimension 1 alors ils se décomposent en : $A_1 = F + E_1$ et $A_2 = F + E_2$ où $F \in \mathcal{A}_1$, E_1 et E_2 sont deux sous-espaces vectoriels de dimension 2 d'un sous-espace vectoriel $\mathcal{E}$ donné de dimension $n-1$ en somme directe avec F tels que $E_1 \cap E_2 = \{0\}$.

Minoration des sommes de caractère $M_f^{(12)}$

La somme $M_f^{(12)}$ se réécrit donc :

$$M_f^{(12)} = \frac{1}{2} \sum_{F \in \mathcal{A}_1} \sum_{\substack{E_1, E_2 \subset \mathcal{E} \\ \dim E_1 = \dim E_2 = 2 \\ E_1 \cap E_2 = \{0\}}} (-1)^{\langle f, 1_{F+E_1} \rangle + \langle f, 1_{F+E_2} \rangle}$$

Si A_1 et A_2 sont deux espaces affines de dimension 3 dont l'intersection est un espace affine de dimension 1 alors ils se décomposent en : $A_1 = F + E_1$ et $A_2 = F + E_2$ où $F \in \mathcal{A}_1$, E_1 et E_2 sont deux sous-espaces vectoriels de dimension 2 d'un sous-espace vectoriel $\mathcal{E}$ donné de dimension $n-1$ en somme directe avec F tels que $E_1 \cap E_2 = \{0\}$.

Minoration des sommes de caractère $M_f^{(12)}$

La somme $M_f^{(12)}$ se réécrit donc :

$$M_f^{(12)} = \frac{1}{2} \sum_{F \in \mathcal{A}_1} \sum_{\substack{E_1, E_2 \subset \mathcal{E} \\ \dim E_1 = \dim E_2 = 2 \\ E_1 \cap E_2 = \{0\}}} (-1)^{\langle f, 1_{F+E_1} \rangle + \langle f, 1_{F+E_2} \rangle}$$

$$= \frac{1}{2} \sum_{F \in \mathcal{A}_1} \left(\left(\sum_{\substack{E \subset \mathcal{E} \\ \dim E = 2}} (-1)^{\langle f, 1_{F+E} \rangle} \right)^2 \right.$$

$$\left. - \sum_{\substack{E \subset \mathcal{E} \\ \dim E = 2}} 1 - \sum_{\substack{E_1, E_2 \subset \mathcal{E} \\ \dim E_1 = \dim E_2 = 2 \\ \dim(E_1 \cap E_2) = 1}} (-1)^{\langle f, 1_{F+E_1} \rangle + \langle f, 1_{F+E_2} \rangle} \right)$$

Minoration des sommes de caractère $M_f^{(12)}$

Soit :

$$M_f^{(12)} \geq -\frac{1}{2} \sum_{F \in \mathcal{A}_1} \left(\sum_{\substack{E \subset \mathcal{E} \\ \dim E = 2}} 1 + \sum_{\substack{E_1, E_2 \subset \mathcal{E} \\ \dim E_1 = \dim E_2 = 2 \\ \dim(E_1 \cap E_2) = 1}} \right)$$

$$\geq -\frac{2^{n-1}(2^n-1)}{2(2^1-1)} \left(\frac{(2^{n-1}-1)(2^{n-1}-2)}{(2^2-1)(2^2-2)} + (2^{n-1}-1)(2^{n-2}-1)(2^{n-2}-2) \right)$$

Par des arguments similaires, on minore $M_f^{(14)}$ et $M_f^{(16)}$.

Minoration des sommes de caractère $M_f^{(2w)}$

Lemme

Pour toute fonction booléenne $f \in \mathcal{B}_n$, on a

$$M_f^{(8)} \geq -\frac{2^n(2^n-1)(2^n-2)}{2^3(2^3-1)(2^2-1)(2^2-2)}$$

$$M_f^{(12)} \geq -\frac{2^n(2^n-1)(2^n-2)(2^n-4)(3\cdot 2^n-20)}{384}$$

$$M_f^{(14)} \geq -\frac{2^n\,(2^n-1)\,(2^n-2)\,(2^n-4)\,\left(7\cdot 2^{2\,n}-126\cdot 2^n+536\right)}{8064}$$

$$M_f^{(16)} \geq -\frac{2^n\,(2^n-1)\,(2^n-2)\,(2^n-4)\,K_n}{112896}$$

où $K_n = 2^{3n+1} - 63\cdot 2^{2n} + 763\cdot 2^n - 63\cdot 2^{2n} - 3054$

Conclusion

$$\mathcal{S}_k(f) = \#\mathcal{RM}(2,n)\left(N_k^{(0)} + N_k^{(8)}M_f^{(8)} + \sum_{w=6}^{k} N_k^{(2w)}M_f^{(2w)}\right)$$

On déduit des minorations sur $M_f^{(2w)}$ pour $2w = 8, 12, 14, 16$ et des valeurs exactes de $N_k^{(2w)}$ une minoration sur $\mathcal{S}_k(f)$:

$$\forall f \in \mathcal{B}_n, \quad \mathcal{S}_k(f) \geq \mathcal{S}_k^{min}$$

pour k variant de 1 à 8.

Conclusion

On déduit des minorations sur $M_f^{(2w)}$ pour $2w = 8, 12, 14, 16$ et des valeurs exactes de $N_k^{(2w)}$ une minoration sur $\mathcal{S}_k(f)$:

$$\forall f \in \mathcal{B}_n, \quad \mathcal{S}_k(f) \geq \mathcal{S}_k^{min}$$

pour k variant de 1 à 8.

Remarque

Pour $k = 9$: on ne sait pour l'instant pas minorer la somme $M_f^{(18)}$ unformément en $f \in \mathcal{B}_n$ bien qu'on connaisse la forme des mots de $\mathcal{RM}(n-3, n)$ de poids 18.
Pour $k \geq 10$: on ne connaît pas la forme des mots de poids supérieur ou égal à 20 !

Conclusion

On déduit des minorations sur $M_f^{(2w)}$ pour $2w = 8, 12, 14, 16$ et des valeurs exactes de $N_k^{(2w)}$ une minoration sur $\mathcal{S}_k(f)$:

$$\forall f \in \mathcal{B}_n, \quad \mathcal{S}_k(f) \geq \mathcal{S}_k^{min}$$

pour k variant de 1 à 8.

Remarque

Le problème est que la borne inférieure S_k^{min} ainsi obtenue peut être négative !
On montre alors que selon les valeurs de k, la borne inférieure S_k^{min} est positive si n est supérieure à une valeur n_k dont les valeurs sont donnés dans le tableau ci-dessous

k	1	2	3	4	5	6	7	8
n_k	0	0	0	1	6	9	11	13

Conclusion

On déduit des minorations sur $M_f^{(2w)}$ pour $2w = 8, 12, 14, 16$ et des valeurs exactes de $N_k^{(2w)}$ une minoration sur $\mathcal{S}_k(f)$:

$$\forall f \in \mathcal{B}_n, \quad \mathcal{S}_k(f) \geq \mathcal{S}_k^{min}$$

pour k variant de 1 à 8.

Pour minorer uniformément en $f \in \mathcal{B}_n$ le rapport $\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}$, on le considère comme une application de plusieurs variables dont les variables sont les sommes de caractère $M_f^{(2w)}$.

On utilise alors des arguments de monotonie qui nous permettent de montrer que

$$\forall f \in \mathcal{B}_n, \quad \frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)} \geq \frac{\mathcal{S}_{k+1}^{min}}{\mathcal{S}_k^{min}}$$