# Sur l'uniformité différentielle des polynômes sur les corps finis de caractéristique paire

Ali Issa

## École doctorale 548 - Mer et Sciences

## THÈSE présentée par :


## Ali Issa


Pour obtenir le grade de

### Docteur de l'Université de Toulon

**Spécialité : Mathématique**

# Sur l'uniformité différentielle des polynômes sur les corps finis de caractéristique paire

Soutenue le 17 Novembre 2022 devant le jury composé de :

| | | |
|---|---|---|
| Yves AUBRY | Maître de conférences HDR, Université de Toulon | Directeur de thèse |
| Christina BOURA | Maître de conférences, Université de Versailles | Examinatrice |
| Jean-Marc COUVEIGNES | Professeur des universités, Université de Bordeaux | Rapporteur |
| Pierre DÈBES | Professeur des universités, Université de Lille 1 | Examinateur |
| Fabien HERBAUT | Maître de conférences, Université Côte d'Azur | Co-encadrant de thèse |
| David KOHEL | Professeur des universités, Université d'Aix Marseille | Rapporteur |
| Gary MCGUIRE | Professeur des universités, University College Dublin | Examinateur |

# Table des matières

# Chapitre 1

# Introduction

### Deux questions ouvertes sur les polynômes APN exceptionnels

Depuis l'antiquité, de nombreuses méthodes de chiffrement ont été élaborées pour rendre la compréhension d'un document chiffré impossible à toute personne ne disposant pas d'une clé. Parallèlement, de nombreuses attaques ont été imaginées pour comprendre ces textes chiffrés. Parmi ces attaques on distingue les attaques différentielles qui consistent généralement à étudier l'impact de la différence entre deux entrées sur la différence entre deux sorties. Pour faire face à ces attaques, Nyberg a introduit dans [20] des polynômes qui offrent une bonne résistance contre les attaques différentielles. Elle les appelle les polynômes APN (pour *Almost Perfect Non Linear*). Avant d'énoncer leur définition, on rappelle la définition de l'uniformité différentielle. Pour un polynôme $f \in \mathbb{F}_{2^n}[x]$, Nyberg définit l'uniformité différentielle de $f$ sur $\mathbb{F}_{2^n}$ par :

$$\delta_{\mathbb{F}_{2^n}}(f) = \max_{(\alpha,\beta)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}} \mathrm{Card}\{x \in \mathbb{F}_{2^n} | f(x) + f(x+\alpha) = \beta\}.$$

Un polynôme $f$ est alors dit APN si $\delta_{\mathbb{F}_{2^n}}(f) = 2$. Parmi les polynômes APN sur $\mathbb{F}_{2^n}$, on distingue les polynômes APN exceptionnels sur $\mathbb{F}_{2^n}$. Ce sont les polynômes APN sur une infinité d'extensions de $\mathbb{F}_{2^n}$. Malgré leur importance, les polynômes APN exceptionnels sont rares. En 2010, Aubry, McGuire et Rodier ont énoncé dans [4] la conjecture suivante :

**Conjecture.** *Soit $n \in \mathbb{N}^*$. Les seuls polynômes APN exceptionnels sur $\mathbb{F}_{2^n}$ sont ceux qui sont CCZ-équivalents aux monômes de degré $2^\ell + 1$ ou $4^\ell - 2^\ell + 1$ avec* $\mathrm{pgcd}(\ell, n) = 1$.

L'étude de cette conjecture a suscité l'intérêt de nombreux auteurs. Dans le cas des polynômes de degré impair, plusieurs résultats ont été démontrés par Hernando

et McGuire dans [14], par Aubry, McGuire et Rodier dans [4] et par Delgado dans [10]. Dans le cas des polynômes de degré pair, des résultats sont obtenus par Janwa et Wilson dans [18], par Aubry McGuire et Rodier dans [4], par Bartoli et Schmidt dans [5], par Rodier dans [22] et par Caullery dans [8]. Nous détaillerons ces résultats dans la section 2.2. Nous verrons que jusqu'à maintenant nous n'avons pas d'informations sur l'uniformité différentielle des polynômes de degré $m \equiv 0 \pmod 8$ ou $m = 4(2^\ell + 1)$ avec $\ell \in \mathbb{N}$. Ainsi on dégage les deux questions ouvertes suivantes :

**Question ouverte 1.** *Pour un entier naturel $\ell$, parmi les polynômes de degré $m = 4(2^\ell + 1)$, lesquels sont APN exceptionnels ?*

**Question ouverte 2.** *Parmi les polynômes de degré $m \equiv 0 \pmod 8$, lesquels sont APN exceptionnels ?*

**Principaux résultats obtenus dans le cadre de la thèse :**

L'objectif de la thèse était d'étudier l'uniformité différentielle des polynômes de degré pair dans le but de trouver une réponse aux deux questions ouvertes posées ci-dessus. Le principal résultat obtenu, qui a été soumis pour publication ([3]), est le suivant :

**Théorème** (Théorème 5.3.1 dans ce manuscrit et Théorème 4.1 dans [3])**.** *Soit $m = 2^\ell(2^r + 1)$, où $\ell$ et $r$ sont deux entiers tels que $\gcd(\ell, r) \leq 2, \ell \geq 2$ et $r \geq 1$. Pour un entier $n$ suffisamment grand et pour tout polynôme*

$$f(x) = \sum_{k=0}^{m} a_{m-k} x^k \in \mathbb{F}_{2^n}[x]$$

*de degré $m$ tel que $a_1 \neq 0$ on a $\delta(f) = m - 2$.*

Ce théorème apporte bien une contribution aux deux questions ouvertes mentionnées ci-dessus. En effet, en choisissant $\ell = 2$, on montre qu'aucun polynôme $f(x) = \sum_{k=0}^{m} a_{m-k} x^k \in \mathbb{F}_{2^n}[x]$ de degré $m = 4(2^r + 1)$ avec $r \geq 2$ et $a_1 \neq 0$ n'est APN exceptionnel, ce qui répond presque entièrement à la question ouverte 1 (presque car il reste une condition sur $a_1$).

De plus, en choisissant $\ell > 2$, on montre qu'aucun polynôme $f(x) = \sum_{k=0}^{m} a_{m-k} x^k \in \mathbb{F}_{2^n}[x]$ de degré $m \equiv 0 \pmod 8$ avec $m = 2^\ell(2^r + 1)$, $r \geq 2$ et $a_1 \neq 0$ n'est APN exceptionnel. Nous contribuons ainsi à la question ouverte 2 en exhibant une famille infinie de polynômes de grande uniformité différentielle.

Le théorème suivant obtenu dans la thèse permet de dégager des familles infinies de trinômes pour lesquels l'uniformité différentielle est maximale. Nous obtenons un résultat sur les trinômes de degré $m$, où $m - 1$ appartient à un ensemble infini $\mathcal{M}$ introduit dans [2].

**Théorème** (Théorème 6.0.6 dans le manuscrit)**.** *Soit $\mathcal{M}$ l'ensemble des entiers impairs $m$ qui vérifient la condition suivante : Pour tout $\zeta_1, \zeta_2 \in \overline{\mathbb{F}_2}$,*

$$\zeta_1^{m-1} = \zeta_2^{m-1} = \left(\frac{1+\zeta_1}{1+\zeta_2}\right)^{m-1} = 1 \implies \zeta_1 = \zeta_2 \text{ ou } \zeta_1 = \zeta_2^{-1}.$$

*Soit $m$ un entier tel que $m \equiv 0 \pmod 4$ et $m-1 \in \mathcal{M}$. Pour $n$ suffisamment grand et pour tout trinôme*

$$f(x) = a_0 x^m + a_1 x^{m-1} + a_2 x^{m-2} \in \mathbb{F}_{2^n}[x]$$

*de degré $m$ tel que $a_1 \neq 0$, on a $\delta(f) = m-2$.*

Ce résultat fera l'objet d'un article qui est encore en cours de préparation ([15]).

Enfin, des calculs explicites obtenus à l'aide du logiciel de calcul formel Maple permettent d'obtenir des résultats pour des petits degrés. A titre d'exemple citons le résultat obtenu pour les polynômes de degré 15 ou 16.

**Théorème** (Théorème 4.3.2 dans le manuscrit)**.** *Pour $n$ suffisamment grand et pour tout polynôme*

$$f(x) = \sum_{k=0}^{16} a_{16-k} x^k \in \mathbb{F}_{2^n}[x]$$

*de degré 15 ou 16 tel que $a_1 \neq 0$ et*

$$a_1^6 a_2^6 a_3^6 + a_1^8 a_2^4 a_3^4 a_4^2 + a_1^{10} a_2^2 a_3^2 a_4^4 + a_1^{12} a_4^6 \neq 0,$$

*on a $\delta(f) = 14$.*

Un intérêt de ce résultat réside dans le fait que 16 est le premier entier $m \equiv 0 \pmod 8$ plus grand strictement que 8, qui n'appartient pas à la famille $2^\ell(2^r+1)$, avec $\ell \geq 2$ et $r \geq 2$.

### Méthode de la preuve

On va donner ici les grandes lignes de la preuve qui sera détaillée dans la section 3.3. Nous suivons ici la méthode introduite par Voloch dans [26] pour obtenir un résultat de densité et exploitée par Aubry, Herbaut et Voloch dans [2] pour obtenir cette fois un résultat valable pour tout polynôme d'un certain degré $m$. L'ingrédient principal est le théorème de densité de Chebotarev.

On va voir dans la section 3.3, que pour tout $\alpha \in \mathbb{F}_{2^n}^*$ si les groupes de monodromie géométriques et arithmétiques du polynôme $f(x)+f(x+\alpha)$ coïncident, alors pour $n$ suffisamment grand il existe $\beta \in \mathbb{F}_{2^n}^*$ pour lequel le nombre de solutions de l'équation $f(x)+f(x+\alpha) = \beta$ est égal au degré du polynôme $f(x)+f(x+\alpha)$ et donc l'uniformité différentielle est égale au degré de $f(x) + f(x + \alpha)$.

Notons $\Omega$ le corps de décomposition du polynôme $f(x) + f(x + \alpha) + t$ sur $\mathbb{F}_{2^n}(t)$ où $t$ est un élément transcendant sur $\mathbb{F}_{2^n}$. Pour pouvoir comparer ces deux groupes on construit un corps intermédiaire $F$ entre $\Omega$ et $\mathbb{F}_{2^n}(t)$ où $F$ est le corps de décomposition du polynôme $L_\alpha f(x) - t$ avec $L_\alpha f$ l'unique polynôme pour lequel $L_\alpha f(x(x + \alpha)) = f(x) + f(x + \alpha)$ (pour plus de détails voir Proposition 2.3 dans [2]). Autrement dit, on a le diagramme suivant :

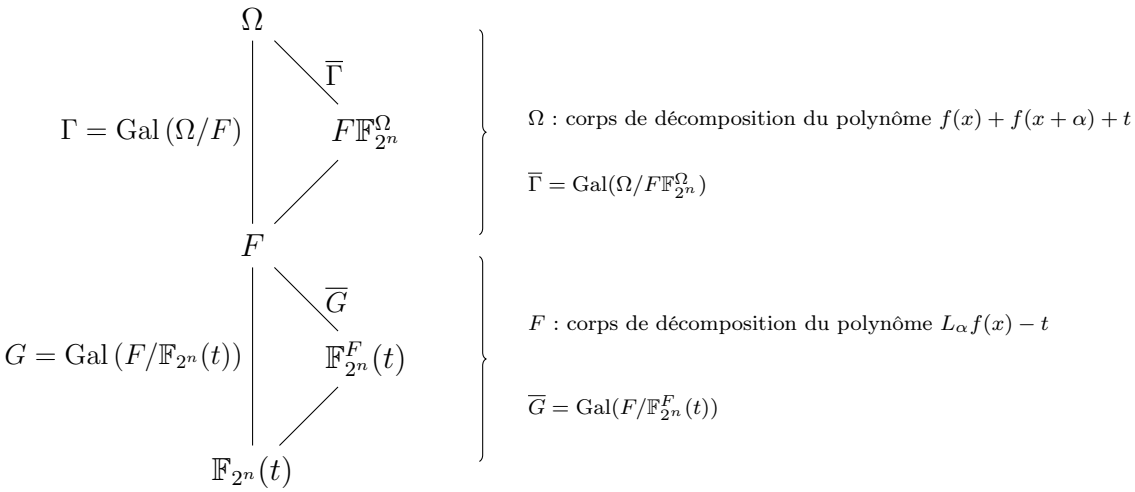


FIGURE 1.1 –

Le point clé de la démonstration réside dans le fait que pour presque tout $\alpha$, le polynôme $L_\alpha f$ est Morse. L'importance des polynômes Morse dans notre contexte, est que leur groupe de monodromie géométrique est le groupe symétrique tout entier d'après un résultat classique d'Hilbert et de Serre, ce qui implique l'égalité entre les groupes de monodromie arithmétique et géométrique du polynôme $L_\alpha f$.

Une grande partie du travail consiste à utiliser une caractérisation de Geyer des polynômes Morse en caractéristique 2 (appendice dans [16]). Il s'agit de vérifier si le degré de $L_\alpha f$ est impair, si ses points critiques sont non dégénérés (ce qui se traduira par une condition algébrique déduite de l'utilisation de Résultant) et si ses valeurs critiques sont distinctes.

Cette dernière condition est la plus difficile à démontrer. On utilisera à nouveau une caractérisation algébrique de Geyer des polynômes à valeurs critiques distinctes. Dans le cas des degrés $m = 2^r(2^l+1)$ les calculs font apparaître les polynômes Trace dont les propriétés permettent de conclure.

### Organisation du manuscrit

L'objectif principal de la thèse est de réussir à appliquer le théorème de Chebotarev pour calculer l'uniformité différentielle de certains polynômes $f \in \mathbb{F}_{2^n}[x]$ de degré $m \equiv 0 \pmod 4$. Expliquons l'organisation de cette thèse.

Dans le Chapitre 2, on va commencer par définir l'uniformité différentielle et présenter les notions de polynômes APN et APN exceptionnels. Nous énoncerons ensuite la conjecture d'Aubry, McGuire et Rodier avant de faire l'état de l'art des résultats démontrés par de nombreux auteurs autour de cette conjecture. On termine ce chapitre, par un rappel des résultats d'uniformité différentielle maximale obtenus par Voloch dans [26] et par Aubry, Herbaut et Voloch dans [2].

Le Chapitre 3 nous donne les outils principaux (résultant, factorisation du polynôme $f(x)+f(x+\alpha)$ sous la forme $g(x(x+\alpha))$, polynômes Morse) et les préliminaires nécessaires avant de détailler dans la dernière section la méthode de la preuve dont l'ingrédient principal est le théorème de densité de Chebotarev.

Après avoir donné tous ces préliminaires nécessaires, on présente dans le Chapitre 4 des résultats sur les polynômes de petit degré. On commence d'abord par le cas des polynômes de degré 12, 20 et 24, ce qui constituera une initiation aux cas des polynômes de degré $m = 2^l(2^r+1)$. Enfin, on démontre un résultat sur les polynômes de degré 16, qui est le premier entier plus grand que 8, multiple de 4 et n'appartenant pas à la famille $2^r(2^l+1)$.

Plus tard, on présente et on démontre dans le Chapitre 5 le résultat principal de la thèse en utilisant des propriétés du polynôme Trace. L'étape la plus compliquée dans la démonstration est de majorer le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels les valeurs

critiques de $L_\alpha f$ sont distinctes. Nous réussirons à mener à bien la démonstration grâce à l'intervention naturelle des polynômes Trace qui disposent de nombreuses propriétés

Finalement, on étudie dans le dernier chapitre l'uniformité différentielle des trinômes de certains degrés et on démontre notre dernier résultat, qui est une extension partielle des résultats du théorème 5.3 de [2].

# Chapitre 2

# Polynômes APN exceptionnels

## 2.1
## Uniformité différentielle.

L'uniformité différentielle d'un polynôme a été introduite en 1994 par Nyberg dans [20] pour obtenir certaines propriétés cryptographiques souhaitables. En effet, Nyberg explique dans cet article que les polynômes qui ont une uniformité différentielle minimale offrent une meilleure résistance en cryptanalyse contre les attaques différentielles. Rappelons d'abord dans un contexte assez général la définition de l'uniformité différentielle.

**Définition 2.1.1.** Soit $G_1$ et $G_2$ deux groupes abéliens finis et soit $F : G_1 \to G_2$ une application. On définit l'uniformité différentielle de $F$ sur $(G_1, G_2)$ par :

$$\delta_{G_1,G_2}(F) = \max_{(\alpha,\beta)\in G_1^*\times G_2} \mathrm{Card}\{x \in G_1 | F(x) - F(x+\alpha) = \beta\}.$$

Dans ce manuscrit on va se limiter au cas des polynômes définis sur des corps finis de caractéristique 2.

**Définition 2.1.2.** Pour un polynôme $f \in \mathbb{F}_{2^n}[x]$, on définit l'uniformité différentielle de $f$ sur $\mathbb{F}_{2^n}$ par :

$$\delta_{\mathbb{F}_{2^n}}(f) = \max_{(\alpha,\beta)\in \mathbb{F}_{2^n}^*\times \mathbb{F}_{2^n}} \mathrm{Card}\{x \in \mathbb{F}_{2^n} | f(x) + f(x+\alpha) = \beta\}.$$

L'uniformité différentielle d'un polynôme $f$ est parfois notée $\delta(f)$ s'il n'y a pas de confusion.

**Premières propriétés de l'uniformité différentielle**

Dans ce paragraphe nous présentons quelques propriétés simples liées à l'uniformité différentielle. En particulier, nous insistons sur les valeurs minimales et maximales que peut prendre l'uniformité différentielle. La remarque suivante permet, en calculant l'uniformité différentielle d'un polynôme, de négliger dans l'expression de ce dernier les monômes de la forme $x^{2^s}$ avec $s \geq 0$.

**Remarque 2.1.3.** Soit $f \in \mathbb{F}_{2^n}[x]$. Pour tout $s \geq 0$, on a

$$\delta(f + x^{2^s}) = \delta(f).$$

*Démonstration.* On a

$$\delta(f) = \max_{(\alpha,\beta)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}} \mathrm{Card}\left(\{x \in \mathbb{F}_{2^n} |\ f(x) + f(x+\alpha) = \beta\}\right).$$

Soit $g(x) = f(x) + x^{2^s}$, on a

$$g(x) + g(x+\alpha) = f(x) + f(x+\alpha) + \alpha^{2^s}.$$

Mais

$$\delta(g) = \max_{(\alpha,\beta)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}} \mathrm{Card}\left(\{x \in \mathbb{F}_{2^n} |\ g(x) + g(x+\alpha) = \beta\}\right).$$

Donc

$$\delta(g) = \max_{(\alpha,\beta)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}} \mathrm{Card}\left(\{x \in \mathbb{F}_{2^n} |\ f(x) + f(x+\alpha) + \alpha^{2^s} = \beta\}\right).$$

Alors

$$\delta(f) = \max_{(\alpha,\beta)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}} \mathrm{Card}\left(A_{\alpha,\beta}\right)$$

et

$$\delta(g) = \max_{(\alpha,\beta)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}} \mathrm{Card}\left(B_{\alpha,\beta}\right)$$

tel que

$$A_{\alpha,\beta} = \{x \in \mathbb{F}_{2^n} |\ f(x) + f(x+\alpha) = \beta\}$$

et

$$B_{\alpha,\beta} = \{x \in \mathbb{F}_{2^n} |\ f(x) + f(x+\alpha) + \alpha^{2^s} = \beta\}.$$

Soit $(\alpha_0, \beta_0) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$ avec $\mathrm{Card}\left(A_{\alpha_0,\beta_0}\right) = \delta(f)$. Pour $\alpha_1 = \alpha_0$ et $\beta_1 = \beta_0 + \alpha_0^{2^s}$, on a

$$A_{\alpha_0,\beta_0} = B_{\alpha_1,\beta_1}.$$

Donc

$$\mathrm{Card}\left(A_{\alpha_0,\beta_0}\right) \leq \max_{(\alpha,\beta)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}} \mathrm{Card}\left(B_{\alpha,\beta}\right)$$

alors, $\mathrm{Card}\left(A_{\alpha_0,\beta_0}\right) \leq \delta(g)$. Ce qui implique que $\delta(f) \leq \delta(g)$. De la même manière on peut démontrer que $\delta(f) \geq \delta(g)$. □

**Borne inférieure de $\delta(f)$**

Cherchons pour tout polynôme $f \in \mathbb{F}_{2^n}[x]$ une borne inférieure de $\delta(f)$.

On remarque d'abord que $\delta(f)$ est un nombre pair. En effet, pour tout polynôme $f \in \mathbb{F}_{2^n}[x]$, pour tout $(\alpha, \beta) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$ et pour tout $u \in \overline{\mathbb{F}_2}$ :

$u$ est une racine de $f(x)+f(x+\alpha)+\beta \iff u+\alpha$ est une racine de $f(x)+f(x+\alpha)+\beta$.

De plus, $\delta(f) \geq 1$. En effet, pour tout polynôme $f \in \mathbb{F}_{2^n}[x]$, en considérant un couple $(\alpha, \beta) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$ avec $\beta = f(1) + f(1+\alpha)$, l'équation

$$f(x) + f(x+\alpha) = \beta$$

admet 1 et $1+\alpha$ comme solutions dans $\mathbb{F}_{2^n}$.

On conclut que, pour tout polynôme $f \in \mathbb{F}_{2^n}[x]$, on a $\delta(f) \geq 2$.

**Borne supérieure de $\delta(f)$**

On va maintenant montrer que dans certains cas l'uniformité différentielle peut être très grande, ou au contraire bornée en fonction du degré du polynôme.

Considérons dans un premiers temps le cas des polynômes $f(x) \in \mathbb{F}_{2^n}[x]$ qui sont $\mathbb{F}_{2^n}$-linéaires. Autrement dit, ce sont les polynômes de la forme

$$f(x) = \sum_{k=0}^{s} a_{s-k} x^{2^k} \in \mathbb{F}_{2^n}[x]$$

avec $s \geq 0$. Dans ce cas, pour tout $u \in \mathbb{F}_{2^n}$, on a $f(u) + f(u+\alpha) = f(\alpha)$. Donc en choisissant $\beta = f(\alpha)$, tout élément de $\mathbb{F}_{2^n}$ est une solution de l'équation $f(x) + f(x+\alpha) = \beta$, ce qui implique que $\delta(f) = 2^n$.

Étudions maintenant le cas des polynômes $f(x) \in \mathbb{F}_{2^n}[x]$ qui ne sont pas $\mathbb{F}_{2^n}$-linéaires. Pour trouver une borne supérieure de $\delta(f)$, on va traiter pour tout $\alpha \in \mathbb{F}_{2^n}^*$, la dérivée du polynôme $f$ par rapport à $\alpha$. Rappelons d'abord la définition de cette dernière.

**Définition 2.1.4.** Soient $n \in \mathbb{N}$ et $f(x) \in \mathbb{F}_{2^n}[x]$ un polynôme de degré $m \in \mathbb{N}$. Pour tout $\alpha \in \mathbb{F}_{2^n}^*$, on définit le polynôme dérivé de $f$ par rapport à $\alpha$ par l'égalité : $D_\alpha f(x) = f(x) + f(x+\alpha)$.

Le lemme suivant nous donne des informations utiles sur les coefficients du polynôme dérivé $D_\alpha f$.

**Lemme 2.1.5.** *Soit $f(x) = \sum_{k=0}^{m} a_{m-k} x^k \in \mathbb{F}_{2^n}[x]$ un polynôme de degré $m$, avec $n \in \mathbb{N}^*$. Pour tout $\alpha \in \mathbb{F}_{2^n}^*$, le polynôme $D_\alpha f$ est de la forme $D_\alpha f(x) = \sum_{i=0}^{m-1} c_{m-i} x^i \in \mathbb{F}_{2^n}[x]$, avec $c_i = \sum_{k=m-i+1}^{m} a_{m-k} \binom{k}{m-i} \alpha^{k-m+i}$ pour tout $1 \leq i \leq m$.*

*Démonstration.* Soit $\alpha \in \mathbb{F}_{2^n}^*$. On a

$$\begin{aligned}
D_\alpha f(x) &= f(x) + f(x+\alpha) \\
&= \sum_{k=0}^{m} a_{m-k}x^k + \sum_{k=0}^{m} a_{m-k}(x+\alpha)^k \\
&= \sum_{k=0}^{m} a_{m-k}(x^k + (x+\alpha)^k) \\
&= \sum_{k=0}^{m} a_{m-k}\left(x^k + \sum_{i=0}^{k}\binom{k}{i}\alpha^{k-i}x^i\right) \\
&= a_m(1+1) + \sum_{k=1}^{m} a_{m-k}\left(x^k + \sum_{i=0}^{k}\binom{k}{i}\alpha^{k-i}x^i\right) \\
&= \sum_{k=1}^{m} a_{m-k}\left(x^k + \sum_{i=0}^{k}\binom{k}{i}\alpha^{k-i}x^i\right) \\
&= \sum_{k=1}^{m} a_{m-k}\left(\sum_{i=0}^{k-1}\binom{k}{i}\alpha^{k-i}x^i\right) \\
&= \sum_{k=1}^{m} a_{m-k}\left(\sum_{i=1}^{k}\binom{k}{i-1}\alpha^{k-i+1}x^{i-1}\right) \\
&= \sum_{i=1}^{m}\left(\sum_{k=i}^{m} a_{m-k}\binom{k}{i-1}\alpha^{k-i+1}x^{i-1}\right) \\
&= \sum_{i=1}^{m}\left(\sum_{k=i}^{m} a_{m-k}\binom{k}{i-1}\alpha^{k-i+1}\right)x^{i-1} \\
&= \sum_{i=0}^{m-1}\left(\sum_{k=i+1}^{m} a_{m-k}\binom{k}{i}\alpha^{k-i}\right)x^{i} \\
&= \sum_{i=0}^{m-1} c_{m-i}x^i,
\end{aligned}$$

où $c_i = \sum_{k=m-i+1}^{m} a_{m-k}\binom{k}{m-i}\alpha^{k-m+i}$, pour tout $i$ tel que $1 \leq i \leq m$. Ce qui permet de conclure. □

Le corollaire suivant nous donne une borne supérieure de l'uniformité différentielle des polynômes qui ne sont pas $\mathbb{F}_{2^n}$ linéaires.

**Corollaire 2.1.6.** *Soient $n \in \mathbb{N}^*$ et $\alpha \in \mathbb{F}_{2^n}^*$. Considérons $f(x) = \sum_{k=0}^{m} a_{m-k}x^k \in \mathbb{F}_{2^n}[x]$ un polynôme de degré $m$.*

*(1) Si $m$ est impair alors $D_\alpha f$ est de degré $m-1$.*

*(2) Si $m \equiv 0 \pmod 4$ et $a_1 \neq 0$ alors $D_\alpha f$ est de degré $m-2$.*

.

*Démonstration.* (1) On remarque par le Lemme 2.1.5 que

$$c_1 = ma_0\alpha = a_0\alpha \neq 0.$$

Ce qui permet de conclure.

(2) On remarque par le Lemme 2.1.5 que

$$c_1 = ma_0\alpha = 0$$

et

$$c_2 = (m-1)a_1\alpha + \binom{m}{2}a_0\alpha^2 = a_1\alpha \neq 0.$$

Ce qui permet de conclure.

□

En utilisant le Corollaire 2.1.6, pour tout $\alpha \in \mathbb{F}_{2^n}^*$, le polynôme $f(x) + f(x+\alpha)$ est de degré $m-1$ si $m$ est impair et de degré plus petit ou égale $m-2$ sinon. Donc $\delta(f) \leq m-2$ si m est pair, et $\delta(f) \leq m-1$ si $m$ est impair.

## 2.2 Polynômes APN et APN exceptionnels.

Comme on a vu dans la section précédente, pour tout polynôme $f \in \mathbb{F}_{2^n}[x]$, on a $\delta(f) \geq 2$. Les polynômes qui ont une uniformité différentielle minimale sont appelés APN (Almost Perfect Non-Linear).

**Définition 2.2.1.** Soit $f \in \mathbb{F}_{2^n}[x]$ un polynôme non nul. On dit que $f$ est APN sur $\mathbb{F}_{2^n}$ si $\delta_{\mathbb{F}_{2^n}}(f) = 2$.

Parmi ces polynômes, on distingue les polynômes APN exceptionnels.

**Définition 2.2.2.** Soit $f \in \mathbb{F}_{2^n}[x]$ un polynôme non nul. On dit que $f$ est APN exceptionnel sur $\mathbb{F}_{2^n}$ s'il est APN sur une infinité d'extensions de $\mathbb{F}_{2^n}$.

La remarque suivante nous montre que tout polynôme APN exceptionnel sur $\mathbb{F}_{2^n}$ est APN sur $\mathbb{F}_{2^n}$.

**Remarque 2.2.3.** Considérons deux corps $K$ et $L$ tel que $K \subset L$ et un polynôme $f(x) \in K[x]$. Si $f$ est APN sur $L$ alors $f$ est APN sur $K$.

On voit par exemple que tous les polynômes

$$f(x) = a_0x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$$

tel que $a_1 \neq 0$ sont APN exceptionnels. En effet, pour tout $(\alpha, \beta) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$ et pour tout $n \in \mathbb{N}^*$ le polynôme $f(x) + f(x + \alpha) + \beta$ est de degré 2 (voir Corollaire 2.1.6 ), donc $\delta(f) \geq 2$. Comme $\delta(f) \leq 2$, on obtient que $\delta(f) = 2$ et donc $f$ est APN exceptionnel.

On va rappeler maintenant la notion de la CCZ équivalence qui est utilisée dans la conjecture 2.2.8. (Pour plus de détails voir [7])

**Définition 2.2.4.** Soit $n \in \mathbb{N}$ et soient $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ et $g : \mathbb{F}_2^n \to \mathbb{F}_2^n$ deux fonctions. On dit que $f$ et $g$ sont CCZ ( pour Carlet, Charpin et Zinoviev) équivalents s'il existe une permutation $h : \mathbb{F}_2^{2n} \to \mathbb{F}_2^{2n}$ tel que $h(G_f) = G_g$, où $G_f$ et $G_g$ désignent le graphe de $f$ et $g$ respectivement.

La Définition 2.2.4 est donnée pour les fonctions. Mais comme on travaille dans ce manuscrit sur les polynômes, on va donner une relation entre un polynôme et une fonction.

**Lemme 2.2.5.** *Tout polynôme $f \in \mathbb{F}_{2^n}[x]$ peut être vu comme une fonction*

$$f_B : \mathbb{F}_2^n \to \mathbb{F}_2^n,$$

*où $B$ est une base de $\mathbb{F}_{2^n}$ sur $\mathbb{F}_2$.*

*Démonstration.* Soit $f \in \mathbb{F}_{2^n}[x]$ un polynôme et soit

$$\begin{array}{rccc} \overline{f} & : & \mathbb{F}_{2^n} & \to & \mathbb{F}_{2^n} \\ & & u & \mapsto & \overline{f}(u) = f(u) \end{array}$$

la fonction polynômial associée. Comme $\mathbb{F}_{2^n}$ est un $\mathbb{F}_2$ espace vectoriel de dimension $n$, il existe une base $B = \{e_1, \ldots, e_n\}$ de $\mathbb{F}_{2^n}$ sur $\mathbb{F}_2$ et une isomorphisme

$$\begin{array}{rccc} L_B & : & \mathbb{F}_{2^n} & \longrightarrow & \mathbb{F}_2^n \\ & & x = a_1e_1 + \ldots + a_ne_n & \mapsto & L_B(x) = (a_1, \ldots, a_n) \end{array}$$

Il suffit de choisir $f_B = L_B \circ \overline{f} \circ L_B^{-1}$. □

Le corollaire suivant donne une liaison entre polynômes APN et fonctions APN.

**Corollaire 2.2.6.** *Soit $f \in \mathbb{F}_{2^n}[x]$ un polynôme. Pour toute base $B$ de $\mathbb{F}_{2^n}$ sur $\mathbb{F}_2$, on a $\delta_{\mathbb{F}_2^n}(f_B) = \delta_{\mathbb{F}_{2^n}}(f)$.*

*Démonstration.* Soient $B = \{e_1, \ldots, e_n\}$ une base de $\mathbb{F}_{2^n}$ sur $\mathbb{F}_2$ et $(\alpha_{\max}, \beta_{\max}) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$ tel que

$$\alpha_{\max} = \alpha_{\max,1}e_1 + \alpha_{\max,2}e_2 + \ldots + \alpha_{\max,n}e_n,$$

$$\beta_{\max} = \beta_{\max,1}e_1 + \beta_{\max,2}e_2 + \ldots + \beta_{\max,n}e_n$$

et

$$\delta(f) = \mathrm{Card}\{x \in \mathbb{F}_{2^n} | f(x) + f(x + \alpha_{\max}) = \beta_{\max}\}.$$

Prenons $x = x_1e_1 + x_2e_2 + \ldots + x_ne_n \in \mathbb{F}_{2^n}$ tel que :

$$f(x) + f(x + \alpha_{\max}) = \beta_{\max}.$$

On a :

$$\overline{f}(x) + \overline{f}(x + \alpha_{\max}) = \beta_{\max},$$

donc

$$\overline{f} \circ L_B^{-1}(x_1, \ldots, x_n) + \overline{f} \circ L_B^{-1}(x_1 + \alpha_{\max,1}, \ldots, x_n + \alpha_{\max,n}) = \beta_{\max}$$

et alors

$$f_B(x_1, \ldots, x_n) + f_B(x_1 + \alpha_{max,1}, \ldots, x_n + \alpha_{\max,n}) = (\beta_{\max,1}, \ldots, \beta_{\max,n}).$$

Donc $\delta(f) \leq \delta(f_B)$. De la même manière on démontre que $\delta(f) \geq \delta(f_B)$. Ce qui permet de conclure.

□

La question naturelle qu'ont peut se poser est : peut on caractériser les polynômes APN exceptionnels ?

Avant de faire l'état d'art des résultats trouvés dans ce contexte, on va rappeler la définition suivante :

**Définition 2.2.7.** Pour tout entier $s \in \mathbb{N}$ :

(1) On dit que $s$ est Gold s'il est de la forme $s = 2^l + 1$.

(2) On dit que $s$ est Kasami-Welch s'il est de la forme $s = 4^l - 2^l + 1$.

Considérons deux entiers $l$ et $n$ avec $\text{pgcd}(l,n)=1$. Les monômes de degré $2^l+1$ et à coefficients dans $\mathbb{F}_{2^n}$ sont APN exceptionnels sur $\mathbb{F}_{2^n}$ (voir [20]). De même les monômes de degré $4^l-2^l+1$ et à coefficients dans $\mathbb{F}_{2^n}$ sont APN exceptionnels sur $\mathbb{F}_{2^n}$ (voir [18]).

En 2010, Aubry, McGuire et Rodier ont présenté dans [4] la conjecture suivante :

**Conjecture 2.2.8.** *Les seuls polynômes APN exceptionnels sont ceux qui sont CCZ-équivalents aux monômes Gold ou Kasami-Welch.*

Dans le même article, Aubry McGuire et Rodier ont démontré le résultat suivant sur des polynômes de degré impair. :

**Théorème 2.2.9.** *Si $f$ est un polynôme de degré impair $m$ tel que $m$ n'est pas Gold ou Kasami Welch, alors $f$ n'est pas APN exceptionnel.*

Ils ont également démontré le résultat suivant sur des polynômes de degré pair.

**Théorème 2.2.10.** *Si $f$ est un polynôme de degré $m=2e$ tel que $e$ n'est pas Gold ou Kasami Welch et $e$ est impair, alors $f$ n'est pas APN exceptionnel.*

Leur méthode consiste à démontrer que la surface $X$ défini par le polynôme :

$$\Phi(x,y,z)=\frac{f(x)+f(y)+f(z)+f(x+y+z)}{(x+y)(x+z)(y+z)}$$

est absolument irréductible. En utilisant la borne de Lang-Weil (voir [23]), cela implique que le polynôme $f$ n'est pas APN exceptionnel.

La Conjecture 2.2.8 a attiré l'attention de nombreux auteurs. En 2011, Hernando et McGuire ont démontré dans [14] qu'elle est vraie pour les monômes. Plus précisément, ils ont démontré le théorème suivant :

**Théorème 2.2.11.** *Les seules monômes APN exceptionnels sont les monômes Gold et les monômes Kasami-Welch de degré $2^l+1$ et $4^l-2^l+1$ respectivement où* $\text{pgcd}(l,n)=1$.

En 2017, Delgado a traité dans [10] le cas des polynômes de degré $2^k+1$ avec $k\geq 2$. On cite par exemple le résultat suivant :

**Théorème 2.2.12.** *Soient $k\geq 2$ et $f(x)=x^{2^k+1}+h(x)$ où $h$ est un polynôme de degré $s\equiv 1 \pmod 4$ avec $s<2^k+1$. Le polynôme $f$ n'est pas APN exceptionnel.*

Concernant, les polynômes de degré pair, très peu de résultats sont trouvés. Bartoli et Schmidt ont déclaré dans la Proposition 1.4 dans [5] que si $f$ est APN exceptionnel alors $m\equiv 0 \pmod 4$. Plus précisément, ils ont démontré le théorème suivant :

**Théorème 2.2.13.** *Soit $f \in \mathbb{F}_{2^n}[x]$ un polynôme de degré $d \leq 2^{\frac{n}{4}}$. Si $f$ est APN sur $\mathbb{F}_{2^n}$ alors $d \equiv 0 \pmod 4$.*

Donc pour chercher des polynômes APN exceptionnels de degré pair il suffit de traiter les polynômes de degré multiple de 4.

Le cas des polynômes $f$ de degré $4e$ tel que $e \equiv 3 \pmod 4$ a été étudié par Rodier dans [22] avec une condition supplémentaire sur $f$. Le théorème suivant illustre le résultat de Rodier.

**Théorème 2.2.14.** *Soit $f(x) \in \mathbb{F}_q[x]$ un polynôme de degré $4e$ avec $e \equiv 3 \pmod 4$ et $q = 2^n$. Soit $\Phi_f(x, y, z)$ le polynôme défini par :*

$$\Phi_f(x, y, z) = \frac{f(x) + f(y) + f(z) + f(x, y, z)}{(x + y)(x + z)(y + z)}.$$

*Si les polynômes de la forme*

$$(x + y)(x + z)(y + z) + P$$

*avec*

$$P(x, y, z) = a(x^2 + y^2 + z^2) + b(xy + xz + yz) + c(x + y + z) + d$$

*où $a, b, c, d \in \mathbb{F}_{q^3}$ ne divisent pas $f$, alors $f$ n'est pas APN sur $\mathbb{F}_{q^n}$ pour $n$ suffisamment grand (et donc $f$ n'est pas APN exceptionnel).*

Caullery a traité dans [8] le cas des polynômes de degré $4e$ lorsque $e > 3$ et lorsque le polynôme $\Phi_e$ est absolument irréductible si l'on note

$$\Phi_e = \frac{x^e + y^e + z^e + (x + y + z)^e}{(x + y)(x + z)(y + z)}.$$

Autrement dit il a démontré le théorème suivant :

**Théorème 2.2.15.** *Si $f(x) \in \mathbb{F}_{2^n}[x]$ est un polynôme de degré $4e$ avec $e > 3$ tel que $\Phi_e$ est absolument irréductible, alors $f$ n'est pas APN exceptionnel.*

La remarque suivante nous donne une condition suffisante sur le degré du polynôme $f$ pour qu'il ne soit pas APN exceptionnel.

**Remarque 2.2.16.** Si $e \equiv 3 \pmod 4$ ou $e \equiv 5 \pmod 4$, alors $\Phi_e$ est absolument irréductible (voir [18] et[17]) .

Signalons maintenant des limites dans cette approche, des cas que l'on ne peut pas ainsi traiter. En utilisant la preuve du Lemme 2.2 dans [2] on voit que le polynôme $\Phi_e$ n'est pas absolument irréductible si $e$ est pair. Donc la question sur les polynômes de degré $m \equiv 0 \pmod 8$ est toujours ouverte. De plus, Janwa et Wilson ont démontré dans le Théorème 4 de l'article [18] que $\Phi_e$ n'est pas absolument irréductible si $e$ est Gold. Donc le cas des polynômes de degré $4e$ n'était toujours pas traitée.

Nous avons ainsi identifié deux questions qui restaient encore ouvertes :

**Question ouverte 1.** *Pour un entier naturel $\ell$, quels sont les polynômes APN exceptionnels de degré $m = 4(2^\ell + 1)$ ?*

**Question ouverte 2.** *Quels sont les polynômes APN exceptionnels de degré $m \equiv 0 \pmod 8$ ?*

Le résultat principal de la thèse illustré dans le théorème 5.3.1, répond presque complètement à la première question ouverte. Il s'agit également d'un premier pas vers la réponse à la deuxième question ouverte.

## 2.3 Uniformité différentielle maximale

On a vu dans la section précédente que les polynômes qui ont une uniformité différentielle minimale sur une infinité d'extension de $\mathbb{F}_{2^n}$ sont intéressants surtout dans le domaine de la cryptanalyse. Cependant, en 2008, Voloch a prouvé que presque tous les polynômes ont une uniformité différentielle maximale.

Pour comprendre ce terme, on rappelle que si $f$ est un polynôme linéaire, alors $\delta(f) = 2^n$. Par contre, si $f$ est un polynôme non linéaire de degré $m$, alors le degré de $D_\alpha f$ est plus petit ou égal à $m-1$ si $m$ est impair et plus petit ou égal à $m-2$ sinon.

**Définition 2.3.1.** Soit $f \in \mathbb{F}_{2^n}[x]$ un polynôme non nul de degré impair $m \geq 5$. On dit que l'uniformité différentielle de $f$ est maximal si

$$\delta(f) = m - 1.$$

On donne maintenant la définition de l'uniformité différentielle maximale pour les polynômes $f(x) = \sum_{k=0}^{m} a_{m-k}x^k \in \mathbb{F}_{2^n}[x]$ de degré pair $m \equiv 0 \pmod 4$ avec $a_1 \neq 0$.

**Définition 2.3.2.** Soit $f(x) = \sum_{k=0}^{m} a_{m-k}x^k \in \mathbb{F}_{2^n}[x]$ un polynôme non nul de degré pair $m \equiv 0 \pmod 4$ avec $a_1 \neq 0$. On dit que l'uniformité différentielle de $f$ est maximale si

$$\delta(f) = m - 2.$$

Énonçons le résultat de densité des polynômes d'uniformité différentielle maximale établi par Voloch dans [26] en 2008. Plus précisément. il a démontré le Théorème suivant :

**Théorème 2.3.3.** *Soit $m > 4$ un entier tel que $m \equiv 0$ ou $3 \pmod 4$ et soit $\delta_0$ l'entier définie par :*

$$\delta_0 = \begin{cases} m-1 & \text{si } m \text{ est impair.} \\ m-2 & \text{si } m \text{ est pair.} \end{cases}$$

*On a :*

$$\lim_{n\to\infty} \frac{\text{Card}\left(\{f \in \mathbb{F}_{2^n}[x] | \deg(f) = m, \delta(f) = \delta_0\}\right)}{\text{Card}\left(\{f \in \mathbb{F}_{2^n}[x] | \deg(f) = m\}\right)} = 1.$$

En 2018, ce résultat a été étendu dans [1] par Aubry et Herbaut, à l'uniformité différentielle d'ordre 2. Plus tard, en 2019, Aubry, Herbaut et Voloch, ont explicité dans [2] des familles infinies d'entiers impairs $m$ pour lesquels tous les polynômes $f$ de degré $m$ ont une uniformité différentielle maximale. Avant d'énoncer leur théorème, on va rappeler la définition suivante donnée par Aubry, Herbaut et Voloch dans [2].

**Définition 2.3.4.** On définit l'ensemble $\mathcal{M}$ par l'ensemble des entiers impairs $m$ qui vérifient la condition suivante : pour tout $\zeta_1, \zeta_2 \in \overline{\mathbb{F}_2}$,

$$\zeta_1^{m-1} = \zeta_2^{m-1} = \left(\frac{1+\zeta_1}{1+\zeta_2}\right)^{m-1} = 1 \implies \zeta_1 = \zeta_2 \text{ ou } \zeta_1 = \zeta_2^{-1}.$$

L'exemple suivant nous montre que l'ensemble $\mathcal{M}$ contient des familles infinies d'entiers.

**Exemple 2.3.5.** (1) $\{7, 23, 39, 47, 55, 79, 87, 95, \ldots.\} \subset \mathcal{M}$.

(2) Pour tout $k \geq 1$, on a $6.9^k + 1 \in \mathcal{M}$.

(3) Pour tout $k \geq 1$, on a $3.2^k + 1 \in \mathcal{M}$.

Après avoir définir l'ensemble $\mathcal{M}$, on est prêt maintenant à énoncer le théorème suivant qui condense les résultats de [2]

**Théorème 2.3.6.** *(1) Soit $m \in \mathcal{M}$, un entier tel que $m \equiv 7 \pmod 8$. Pour $n$ suffisamment grand, et pour tout polynôme $f \in \mathbb{F}_{2^n}[x]$, $\delta(f)$ est maximale. Autrement dit, $\delta(f) = m - 1$.*

*(2) Soit $m \in \mathcal{M}$, un entier tel que $m \equiv 3 \pmod 8$. Pour $n$ pair et suffisamment grand, et pour tout polynôme $f \in \mathbb{F}_{2^n}[x]$, $\delta(f)$ est maximale. Autrement dit, $\delta(f) = m - 1$.*

*(3) Soit $m \in \mathcal{M}$, un entier tel que $m \equiv 3 \pmod 8$. Pour $n$ suffisamment grand, et pour tout polynôme $f(x) = \sum_{k=0}^{m} a_{m-k}x^k \in \mathbb{F}_{2^n}[x]$, tel que $a_1^2 + a_0a_2 \neq 0$, $\delta(f)$ est maximale. Autrement dit, $\delta(f) = m - 1$.*

On remarque que dans le dernier théorème, les polynômes traités sont tous de degré impair. L'objectif de la thèse est de réussir à appliquer ces méthodes dans le cas des polynômes de degré pair pour apporter une contribution à l'identification des polynômes APN exceptionnels.

# Chapitre 3

# Préliminaires et méthode de la preuve

Dans ce chapitre, nous fournirons les préliminaires et les définitions dont nous aurons besoin pour démontrer les nouveaux résultats, sachant que tous les éléments présentés dans ce chapitre peuvent être retrouvés dans les deux premières sections de [2], avec plus ou moins de détails.

On présente également dans ce chapitre la méthode de la preuve qui s'appuie sur le théorème de densité de Chebotarev. La méthode va se résumer à démontrer 4 conditions que l'on appellera ((I.a), (I.b), (I.c) et (II)).

On va traiter dans ce chapitre les conditions ((I.a), (I.c) et (II)) pour tout polynôme de degré $m \equiv 0 \pmod 4$. La condition la plus difficile à traiter est la condition (I.b) qui nécessite un traitement particulier pour chacun des contextes qu'on étudiera plus tard. Le traitement de cette condition sera l'objet des Chapitres 4,5 et 6.

## 3.1 Le polynôme $L_\alpha f$

Dans cette section on va rappeler quelques propriétés algébriques du polynôme $L_\alpha f$ défini par Voloch dans [26], qui va jouer un rôle essentiel et important dans la démonstration des nouveaux résultats. Dans tout ce qui suit on associe pour tout entier $m$ l'entier $d(m)$ suivant :

**Définition 3.1.1.** Soit $m \in \mathbb{N}^*$. On définit l'entier $d(m)$ par :

$$d(m) = \begin{cases} \frac{m-1}{2} & \text{si } m \text{ est impair.} \\ \frac{m-2}{2} & \text{si } m \text{ est pair.} \end{cases}$$

On note parfois $d(m)$ par $d$ lorsqu'il n'y a pas de confusion.

**Remarque 3.1.2.** Soit $m \in \mathbb{N}^*$. On a :

$$d(m) \equiv 1 \pmod 2 \iff m \equiv 0 \text{ ou } 3 \pmod 4.$$

La proposition suivante donne l'existence et l'unicité pour tout $\alpha \in \mathbb{F}_{2^n}^*$ du polynôme $L_\alpha f$ qui va remplacer le polynôme $D_\alpha f$ dans l'étude de l'uniformité différentielle du polynôme $f$.

**Proposition 3.1.3.** *Soit $n \in \mathbb{N}$. Considérons un polynôme*

$$f(x) = \sum_{k=0}^{m} a_{m-k} x^k \in \mathbb{F}_{2^n}[x]$$

*de degré $m \in \mathbb{N}$. Pour tout $\alpha \in \mathbb{F}_{2^n}^*$, il existe un unique polynôme $g$ de degré plus petit ou égal à $d(m)$ tel que*

$$g(x^2 + \alpha x) = D_\alpha f(x).$$

*On note pour la suite le polynôme $g$ par $L_\alpha f$.*

*Démonstration.* Soit $f \in \mathbb{F}_{2^n}[x]$ un polynôme de degré $m$ et soit $\alpha \in \mathbb{F}_{2^n}^*$. Notons par $S_k$ l'ensemble des racines de $D_\alpha f$ de multiplicité $k$. On remarque que $u \in S_k$ si et seulement si $u + \alpha \in S_k$. Comme l'application $x \mapsto x + \alpha$ est un involution de $S_k$ pour tout $k$, il existe alors un ensemble

$$S'_k := \{u \in S_k; \forall v \in S_k, u \neq v + \alpha\}$$

tel que :

$$\begin{aligned} D_\alpha f(x) &= \prod_{k \geq 0} \prod_{u \in S'_k} (x+u)^k (x+u+\alpha)^k \\ &= \prod_{k \geq 0} \prod_{u \in S'_k} \left((x+u)(x+u+\alpha)\right)^k \\ &= \prod_{k \geq 0} \prod_{u \in S'_k} \left(x(x+\alpha) + u(u+\alpha)\right)^k \end{aligned}$$

Donc, en choisissant

$$g(x) = \prod_{k \geq 0} \prod_{u \in S'_k} \left(x + u(u+\alpha)\right)^k,$$

on obtient $g(x(x+\alpha)) = D_\alpha f(x)$. Il reste à démontrer l'unicité de $L_\alpha f$. Supposons qu'il existe deux polynômes $g_1$ et $g_2$ tels que

$$D_\alpha f(x) = g_1(x(x+\alpha)) = g_2(x(x+\alpha)).$$

Supposons par l'absurde que $g_1 \neq g_2$. Soit $h = g_1 - g_2$, on a $h \neq 0$ et $h \circ T_\alpha = 0$ avec

$$\begin{array}{rccc} T_\alpha & : & \mathbb{F}_{2^n}[x] & \to & \mathbb{F}_{2^n}[x] \\ & & x & \mapsto & T_\alpha(x) = x(x+\alpha). \end{array}$$

Soit $l = \deg(h)$. On a $\deg(h \circ T_\alpha) = 2l$ et donc $h \circ T_\alpha \neq 0$. Ce qui permet de conclure. □

On va s'intéresser dans le Chapitre 5 au coefficient $a_0$ et à son apparition dans l'expression des $b_i$. La Proposition suivante nous donne une expression implicite des $b_i$ en fonction des $a_i$.

**Proposition 3.1.4.** *Soit $n \in \mathbb{N}$. Considérons un polynôme*

$$f(x) = \sum_{k=0}^{m} a_{m-k} x^k \in \mathbb{F}_{2^n}[x]$$

*de degré $m \in \mathbb{N}$. Pour tout $\alpha \in \mathbb{F}_{2^n}^*$, le polynôme*

$$L_\alpha f = \sum_{k=0}^{d} b_{d-k} x^k \in \mathbb{F}_{2^n}[x]$$

*est de degré $d$ et pour tout $0 \leq k \leq d$ on a :*

$$\sum_{s=\max\{0,2k-d\}}^{k} \binom{d-s}{2k-2s} \alpha^{2k-2s} b_s = \sum_{i=2d-2k+1}^{m} \binom{i}{2d-2k} \alpha^{i-2d+2k} a_{m-i}. \tag{3.1}$$

*Démonstration.* Commençons d'abord par la démonstration de l'égalité (2.1). Pour avoir des informations sur les coefficients de $L_\alpha f$ on va comparer les coefficients des monômes $1, x^2, x^4, \ldots, x^{2d-2}, x^{2d}$ dans l'équation

$$L_\alpha f(x(x+\alpha)) = D_\alpha f(x).$$

On va commencer par l'exhibition des coefficients de $D_\alpha f$. On a par le Lemme 2.1.5 que

$$D_\alpha f(x) = \sum_{k=0}^{m-1} c_{m-k} x^k$$

avec $c_k = \sum_{i=m-k+1}^{m} a_{m-i}\binom{i}{m-k}\alpha^{i-m+k}$. Donc pour tout $0 \leq k \leq d$, le coefficient du monôme $x^{2d-2k}$ dans $D_\alpha f$ est

$$\begin{aligned} c_{m-2d+2k} &= \sum_{i=m-(m-2d+2k)+1}^{m} a_{m-i}\binom{i}{m-(m-2d+2k)}\alpha^{i-m+(m-2d+2k)} \\ &= \sum_{i=2d-2k+1}^{m} a_{m-i}\binom{i}{2d-2k}\alpha^{i-2d+2k}. \end{aligned}$$

Donc le coefficient multiplié par $x^{2d-2k}$ dans $D_\alpha f$ est bien le terme droit de l'égalité (2.1). Maintenant il nous reste à traiter le coefficient du monôme $x^{2d-2k}$ dans $L_\alpha f(x(x+\alpha))$. On a

$$L_\alpha f(x(x+\alpha)) = \sum_{k=0}^{d} b_{d-k}(x(x+\alpha))^k \tag{3.2}$$

$$= \sum_{k=0}^{d} b_{d-k}x^k(x+\alpha)^k \tag{3.3}$$

$$= b_0x^d(x+\alpha)^d + b_1x^{d-1}(x+\alpha)^{d-1} + \ldots + b_{d-1}x(x+\alpha) + b_d \tag{3.4}$$

$$= b_0x^d\left[\sum_{k=0}^{d}\binom{d}{k}\alpha^{d-k}x^k\right] + b_1x^{d-1}\left[\sum_{k=0}^{d-1}\binom{d-1}{k}\alpha^{d-1-k}x^k\right] \tag{3.5}$$

$$+ \ldots + b_sx^{d-s}\left[\sum_{k=0}^{d-s}\binom{d-s}{k}\alpha^{d-s-k}x^k\right] + \ldots + b_{d-1}x(x+\alpha) + b_d \tag{3.6}$$

$$= \sum_{s=0}^{d} b_s \sum_{k=0}^{d-s}\binom{d-s}{k}\alpha^{d-s-k}x^{d-s+k}. \tag{3.7}$$

D'après l'égalité 3.7, on voit que dans l'expression de $L_\alpha f(x(x+\alpha))$, pour tout $0 \leq s \leq d$, $b_s$ apparaît seulement dans les termes de la forme :

$$b_s\binom{d-s}{k}\alpha^{d-s-k}x^{d-s+k} \text{ avec } 0 \leq k \leq d-s.$$

Autrement dit, une condition nécessaire pour que le terme $b_sx^t$ apparaisse est que

$$d - t \leq s \leq d - \frac{t}{2}$$

et il apparaît avec le coefficient

$$\binom{d-s}{t-d+s}\alpha^{(2d-2s)-t}$$

On rappelle qu'on s'intéresse à calculer le coefficient multiplié par le monôme $x^{2d-2k}$ dans $L_\alpha f(x(x+\alpha))$ avec $k$ varie entre 0 et $d$. D'après la condition nécessaire qu'on a élaboré ci dessus, $b_s$ apparaît dans le coefficient multiplié par $x^{2d-2k}$ dans l'expression de $L_\alpha f(x(x+\alpha))$ si

$$d-(2d-2k) \leq s \leq d-\frac{2d-2k}{2},$$

c'est-à-dire si

$$2k-d \leq s \leq k.$$

Donc $b_s$ apparaît dans le coefficient multiplié par $x^{2d-2k}$ si

$$\max\{0, 2k-d\} \leq s \leq k.$$

Plus précisément, il apparaît avec le coefficient

$$\begin{aligned}\binom{d-s}{2d-2k-d+s}\alpha^{2k-2s} &= \binom{d-s}{d-2k+s}\alpha^{2k-2s} \\ &= \binom{d-s}{d-s-(d-2k+s)}\alpha^{2k-2s} \\ &= \binom{d-s}{2k-2s}\alpha^{2k-2s}.\end{aligned}$$

Par suite, le monôme $x^{2d-2k}$ du polynôme $L_\alpha f(x(x+\alpha)$ est multiplié par

$$\sum_{s=\max\{0,2k-d\}}^{k} b_s\binom{d-s}{2k-2s}\alpha^{2k-2s}.$$

Ce qui nous donne le terme gauche de l'égalité 3.1. Il nous reste à démontrer que

$$L_\alpha f(x(x+\alpha)) \in \mathbb{F}_{2^n}[x].$$

D'après l'égalité 3.1, on a pour tout $0 \leq k \leq d$ :

$$\sum_{s=\max\{0,2k-d\}}^{k}\binom{d-s}{2k-2s}\alpha^{2k-2s}b_s = \sum_{i=2d-2k+1}^{m}\binom{i}{2d-2k}\alpha^{i-2d+2k}a_{m-i}.$$

Donc

$$b_k + \sum_{s=\max\{0,2k-d\}}^{k-1} \binom{d-s}{2k-2s} \alpha^{2k-2s} b_s = \sum_{i=2d-2k+1}^{m} \binom{i}{2d-2k} \alpha^{i-2d+2k} a_{m-i}.$$

Ce qui implique que pour tout $0 \leq k \leq d$ on a :

$$b_k \in \mathbb{F}_{2^n}[b_0, b_1, \ldots, b_{k-1}].$$

Donc il suffit de démontrer que $b_0 \in \mathbb{F}_{2^n}$. Or si on choisit $k = 0$ dans l'égalité 3.1, on obtient :

$$b_0 = \sum_{i=2d+1}^{m} \binom{i}{2d} \alpha^{i-2d} a_{m-i} \in \mathbb{F}_{2^n},$$

ce qui permet de conclure.

□

Dans la proposition précédente on a donné une expression implicite des $b_i$. Maintenant on va donner une expression explicite de $\frac{b_1}{b_0}$ qui va nous servir à étudier la condition (II).

**Corollaire 3.1.5.** *Soit $n \in \mathbb{N}$. Considérons un polynôme*

$$f(x) = \sum_{k=0}^{m} a_{m-k} x^k \in \mathbb{F}_{2^n}[x]$$

*de degré $m \equiv 0$ ou $3 \pmod 4$. Soit $\alpha \in \mathbb{F}_{2^n}^*$ et notons*

$$L_\alpha f = \sum_{k=0}^{d} b_{d-k} x^k \in \mathbb{F}_{2^n}[x]$$

*le polynôme associé. Si $b_0 \neq 0$, on a :*

| $m \pmod 8$ | $b_1/b_0$ |
|---|---|
| $m \equiv 0 \pmod 8$ | $\frac{a_2\alpha + a_3}{a_1}$ |
| $m \equiv 4 \pmod 8$ | $\frac{a_0\alpha^3 + a_2\alpha + a_3}{a_1} + \alpha^2$ |
| $m \equiv 3 \pmod 8$ | $\frac{a_1\alpha + a_2}{a_0} + \alpha^2$ |
| $m \equiv 7 \pmod 8$ | $\frac{a_1\alpha + a_2}{a_0}$ |

*Démonstration.* On va d'abord calculer $b_0$. On a d'après la Proposition 3.1.4 que

$$b_0 = \sum_{i=2d+1}^{m} \binom{i}{2d} \alpha^{i-2d} a_{m-i}.$$

On distingue deux cas : Cas 1 : Si $m \equiv 0 \pmod 4$, alors $m = 2d+2$ et

$$\begin{aligned} b_0 &= \binom{2d+1}{2d} \alpha^{2d+1-2d} a_{2d+2-(2d+1)} + \binom{2d+2}{2d} \alpha^{2d+2-2d} a_{2d+2-(2d+2)} \\ &= (2d+1)\alpha a_1 + (d+1)(2d+1)\alpha^2 a_0 \\ &= \alpha a_1. \end{aligned}$$

Cas 2 : Si $m \equiv 3 \pmod 4$, alors $m = 2d+1$ et

$$\begin{aligned} b_0 &= \binom{2d+1}{2d} \alpha^{2d+1-2d} a_{2d+1-(2d+1)} \\ &= (2d+1)\alpha a_0 \\ &= \alpha a_0. \end{aligned}$$

Il nous reste maintenant à calculer $b_1$.

On va distinguer 4 cas :

Cas 1 : Si $m \equiv 3 \pmod 8$, alors il existe $l \in \mathbb{N}$ tel que $m = 2d+1 = 3+8l$ et donc $d = 1+4l$. On a

$$\begin{aligned} b_1 &= \binom{d}{2} b_0 \alpha^2 + \sum_{i=2d-2+1}^{m} \binom{i}{2d-2} \alpha^{i-2d+2} a_{m-i} \\ &= \binom{d}{2} b_0 \alpha^2 + \sum_{i=2d-1}^{2d+1} \binom{i}{2d-2} \alpha^{i-2d+2} a_{2d+1-i} \\ &= \binom{d}{2} \alpha^3 a_0 + \binom{2d-1}{2d-2} \alpha a_2 + \binom{2d}{2d-2} \alpha^2 a_1 + \binom{2d+1}{2d-2} \alpha^3 a_0 \\ &= (\frac{d(d-1)}{2} + \frac{(2d+1)(2d)(2d-1)}{6})\alpha^3 a_0 + \alpha a_2 + \frac{(2d)(2d-1)}{2}\alpha^2 a_1 \\ &= (\frac{(4l+1)(4l)}{2} + 1)\alpha^3 a_0 + \alpha a_2 + \alpha^2 a_1 \\ &= \alpha^3 a_0 + \alpha a_2 + \alpha^2 a_1. \end{aligned}$$

Cas 2 : Si $m \equiv 7 \pmod 8$, alors il existe $l \in \mathbb{N}$ tel que $m = 2d+1 = 7+8l$ et donc $d = 3+4l$. On a :

$$\begin{aligned}
b_1 &= \binom{d}{2} b_0 \alpha^2 + \sum_{i=2d-2+1}^{m} \binom{i}{2d-2} \alpha^{i-2d+2} a_{m-i} \\
&= \binom{d}{2} b_0 \alpha^2 + \sum_{i=2d-1}^{2d+1} \binom{i}{2d-2} \alpha^{i-2d+2} a_{2d+1-i} \\
&= \binom{d}{2} \alpha^3 a_0 + \binom{2d-1}{2d-2} \alpha a_2 + \binom{2d}{2d-2} \alpha^2 a_1 + \binom{2d+1}{2d-2} \alpha^3 a_0 \\
&= \left( \frac{d(d-1)}{2} + \frac{(2d+1)(2d)(2d-1)}{6} \right) \alpha^3 a_0 + \alpha a_2 + \frac{(2d)(2d-1)}{2} \alpha^2 a_1 \\
&= \left( \frac{(4l+2)(4l+3)}{2} + 1 \right) \alpha^3 a_0 + \alpha a_2 + \alpha^2 a_1 \\
&= \alpha a_2 + \alpha^2 a_1.
\end{aligned}$$

Cas 3 : Si $m \equiv 4 \pmod 8$, alors il existe $l \in \mathbb{N}$ tel que $m = 2d + 2 = 4 + 8l$ et donc $d + 1 = 2 + 4l$. On a :

$$
\begin{aligned}
b_1 &= \binom{d}{2} b_0 \alpha^2 + \sum_{i=2d-2+1}^{m} \binom{i}{2d-2} \alpha^{i-2d+2} a_{m-i} \\
&= \binom{d}{2} b_0 \alpha^2 + \sum_{i=2d-1}^{2d+2} \binom{i}{2d-2} \alpha^{i-2d+2} a_{2d+2-i} \\
&= \binom{d}{2} \alpha^3 a_1 + \binom{2d-1}{2d-2} \alpha a_3 + \binom{2d}{2d-2} \alpha^2 a_2 + \binom{2d+1}{2d-2} \alpha^3 a_1 + \binom{2d+2}{2d-2} \alpha^4 a_0 \\
&= \frac{d(d-1)}{2} \alpha^3 a_1 + \alpha a_3 + \frac{(2d)(2d-1)}{2} \alpha^2 a_2 + \frac{(2d+1)(2d)(2d-1)}{6} \alpha^3 a_1 \\
&+ \frac{(2d+2)(2d+1)(2d)(2d-1)}{24} \alpha^4 a_0 \\
&= \frac{d(d-1)}{2} \alpha^3 a_1 + \alpha a_3 + (d)(2d-1) \alpha^2 a_2 + \frac{(2d+1)(d)(2d-1)}{3} \alpha^3 a_1 \\
&+ \frac{(d+1)(2d+1)(d)(2d-1)}{6} \alpha^4 a_0 \\
&= (\frac{d(d-1)}{2} + 1) \alpha^3 a_1 + \alpha a_3 + \alpha^2 a_2 + \frac{(d+1)(2d+1)(d)(2d-1)}{6} \alpha^4 a_0 \\
&= (\frac{d(d-1)}{2} + 1) \alpha^3 a_1 + \alpha a_3 + \alpha^2 a_2 + \frac{(d+1)(2d+1)(d)(2d-1)}{6} \alpha^4 a_0 \\
&= (\frac{d(d-1)}{2} + 1) \alpha^3 a_1 + \alpha a_3 + \alpha^2 a_2 + \frac{(d+1)(2d+1)(d)(2d-1)}{6} \alpha^4 a_0 \\
&= (\frac{(4l+1)(4l)}{2} + 1) \alpha^3 a_1 + \alpha a_3 + \alpha^2 a_2 + \frac{(2l+1)(8l-1)(4l-1)(8l-3)}{3} \alpha^4 a_0 \\
&= \alpha^3 a_1 + \alpha a_3 + \alpha^2 a_2 + \alpha^4 a_0.
\end{aligned}
$$

Cas 4 : Si $m \equiv 0 \pmod 8$, alors il existe $l \in \mathbb{N}$ tel que $m = 2d+2 = 8l$ et donc $d+1 = 4l$. On a :

$$\begin{aligned}
b_1 &= \binom{d}{2} b_0 \alpha^2 + \sum_{i=2d-2+1}^{m} \binom{i}{2d-2} \alpha^{i-2d+2} a_{m-i} \\
&= \binom{d}{2} b_0 \alpha^2 + \sum_{i=2d-1}^{2d+2} \binom{i}{2d-2} \alpha^{i-2d+2} a_{2d+2-i} \\
&= \binom{d}{2} \alpha^3 a_1 + \binom{2d-1}{2d-2} \alpha a_3 + \binom{2d}{2d-2} \alpha^2 a_2 + \binom{2d+1}{2d-2} \alpha^3 a_1 + \binom{2d+2}{2d-2} \alpha^4 a_0 \\
&= \frac{d(d-1)}{2} \alpha^3 a_1 + \alpha a_3 + \frac{(2d)(2d-1)}{2} \alpha^2 a_2 + \frac{(2d+1)(2d)(2d-1)}{6} \alpha^3 a_1 \\
&+ \frac{(2d+2)(2d+1)(2d)(2d-1)}{24} \alpha^4 a_0 \\
&= \frac{d(d-1)}{2} \alpha^3 a_1 + \alpha a_3 + (d)(2d-1) \alpha^2 a_2 + \frac{(2d+1)(d)(2d-1)}{3} \alpha^3 a_1 \\
&+ \frac{(d+1)(2d+1)(d)(2d-1)}{6} \alpha^4 a_0 \\
&= (\frac{d(d-1)}{2} + 1) \alpha^3 a_1 + \alpha a_3 + \alpha^2 a_2 + \frac{(d+1)(2d+1)(d)(2d-1)}{6} \alpha^4 a_0 \\
&= (\frac{d(d-1)}{2} + 1) \alpha^3 a_1 + \alpha a_3 + \alpha^2 a_2 + \frac{(d+1)(2d+1)(d)(2d-1)}{6} \alpha^4 a_0 \\
&= (\frac{(4l-1)(4l-2)}{2} + 1) \alpha^3 a_1 + \alpha a_3 + \alpha^2 a_2 + \frac{(2l)(8l-1)(4l-1)(8l-3)}{3} \alpha^4 a_0 \\
&= \alpha a_3 + \alpha^2 a_2.
\end{aligned}$$

Ce qui permet de conclure. □

La remarque suivante est un outil essentiel dans la démonstration du Lemme 3.1.7. C'est un résultat d'homogénéité sur les coefficients $b_i$ en fonctions des indéterminées $a_i$ et $\alpha$, pour un poids particulier $w$.

**Remarque 3.1.6** (Lemme 2.4 dans [2])**.** Considérons un polynôme

$$f(x) = \sum_{k=0}^{m} a_{m-k} x^k \in \mathbb{F}_{2^n}[x]$$

de degré pair $m$ et notons $L_\alpha f = \sum_{k=0}^{d} b_{d-k} x^k$ le polynôme associé de degré $d$. Pour tout $i \in \{1, \ldots, d\}$, $b_i$ est un polynôme homogène de degré $2i+2$ si l'on considère le poids $w$ défini par $w(a_i) = i$ et $w(\alpha) = 1$.

On termine par le lemme suivant qui décrit l'homogénéité du polynôme

$$\Pi_d L_\alpha f := \prod_{i<j} \left(L_\alpha f(\tau_i) - L_\alpha f(\tau_j)\right).$$

Nous décrirons dans la section suivante le rôle important de $\Pi_d L_\alpha f$ dans l'étude des valeurs critiques distinctes.

**Lemme 3.1.7.** *Soient $m \equiv 0 \pmod 4$ un entier non nul et $f(x) = \sum_{k=0}^{m} a_{m-k}x^k \in \mathbb{F}_{2^n}[x]$ un polynôme de degré $m$ tel que $a_1 \neq 0$. Notons $L_\alpha f = \sum_{k=0}^{d} b_{d-k}x^k$ le polynôme associé de degré $d$. Considérons $e = \binom{(d-1)/2}{2}$ et $N = de$. Soient $w$ le poids définis par $w(a_i) = i$ et $w(\alpha) = 1$ et $\tilde{w}$ le poids définis par $\tilde{w}(a_i) = 1$ et $\tilde{w}(\alpha) = 0$. Le polynôme*

$$b_0^N \Pi_d(L_\alpha f) := b_0^N \prod_{i<j} \left(L_\alpha f(\tau_i) - L_\alpha f(\tau_j)\right)$$

*est homogène de degré $(6d+4)e$ par rapport à $w$ et de degré $(d+2)e$ par rapport à $\tilde{w}$.*

*Démonstration.* La preuve est similaire à celle de Lemme 3.8 dans [2]. Considérons, $\tau_1, \tau_2, \ldots, \tau_{(d-1)/2}$ les racines de $(L_\alpha f)'$. On a

$$\Pi_d(L_\alpha f) := \prod_{i<j} \left(L_\alpha f(\tau_i) - L_\alpha f(\tau_j)\right).$$

Donc

$$\Pi_d(L_\alpha f) := \prod_{i<j} \left(\sum_{k=0}^{d} b_{d-k}^2(\tau_i^{2k} + \tau_j^{2k})\right).$$

En utilisant le théorème fondamental des polynômes symétriques, on a

$$\Pi_d(L_\alpha f) \in \mathbb{F}_2[b_0, \ldots, b_d, \sigma_1, \ldots, \sigma_{(d-1)/2}],$$

où les $\sigma_i$ représentent les polynômes symétriques élémentaires en les $\tau_i$ ( c'est à dire $\sigma_1 = \sum \tau_i^2, \sigma_2 = \sum_{i<j} \tau_i\tau_j, \ldots$).

On remarque que

$$L_\alpha f(x)' = b_0 x^{d-1} + b_2 x^{d-3} + \ldots + b_{d-3}x^2 + b_{d-1}.$$

Donc $(L_\alpha f)' \in \mathbb{F}_2[b_0, b_2, b_4, \ldots, b_{d-1}]$, et par suite en utilisant les relations entre les coefficients et les racines du polynôme $(L_\alpha f)'$ on obtient que

$$\Pi_d(L_\alpha f) \in \mathbb{F}_2[b_0, \ldots, b_d, \frac{b_2}{b_0}, \frac{b_4}{b_0}, \ldots, \frac{b_{(d-1)/2}}{b_0}].$$

La plus grande puissance de $b_0$ qui apparaît dans le dénominateur de $\Pi_d(L_\alpha f)$ est $N$ (ce sera le cas si les $\tau_i$ sont les seuls termes qui contribuent au degré et s'ils font apparaître seulement le terme $\frac{b_2}{b_0}$). Donc $b_0^N \Pi_d(L_\alpha f)$ est un polynôme dans $\mathbb{F}_2[b_0, b_1, \ldots, b_d]$, dont chaque terme est un produit de $(d+2)e$ indéterminé $b_i$. De plus $b_0^N \Pi_d L_\alpha f$ est un polynôme homogène de degré $2de$ si l'on considère le poids $w$ défini par $w(b_i) = i$. En utilisant la Remarque 3.1.6. $b_0^N \Pi_d L_\alpha f$ est un polynôme homogène de degré $2 \times 2de + 2(d+2)e = (6d+4)e$. Cela nous permet de conclure. □

## 3.2 Polynôme Morse en caractéristique 2

Dans cette section, on procède à quelques rappels sur la notion de polynômes Morse donnée par Geyer dans l'annexe de [16]. Commençons d'abord par la définition d'un point critique et d'une valeur critique.

**Définition 3.2.1.** Soient $K$ un corps de caractéristique $p$ et $f \in K[x]$.

(1) On dit que $u$ est un point critique de $f$ si $f'(u) = 0$.

(2) On dit que $v$ est une valeur critique de $f$ si $v$ est l'image par $f$ d'un point critique.

**Exemple 3.2.2.** (1) Considérons un corps $K$ de caractéristique $p$. On voit par exemple que tout élément de $K$ est à la fois un point et une valeur critique de la fonction $x^p$.

(2) Considérons un corps $K$ de caractéristique $p$. 0 est le seul point critique et la seule valeur critique de la fonction $x^{p+1}$.

Pour pouvoir définir un polynôme Morse en caractéristique 2, on a besoin d'une extension de la dérivation donnée par Hasse et Schmidt en 1937.

**Définition 3.2.3.** Soit $K$ un corps de caractéristique 2 et $f$ un polynôme sur $K$. La dérivée seconde de Hasse–Schmidt de $f$ notée par $f^{[2]}$ est donnée par l'égalité suivante :

$$f(t+u) \equiv f(t) + f'(t)u + f^{[2]}(t)u^2 \pmod{u^3}$$

où $u$ et $t$ sont des variables indépendantes.

**Exemple 3.2.4.** (1) On a $x^{[2]} = 0$. En effet,

$$x + u = x + u + 0.u^2 \equiv x + u + 0.u^2 \pmod{u^3}.$$

(2) Pour tout $m \geq 2$, on a $(x^m)^{[2]} = \binom{m}{2} x^{m-2}$. En effet, pour tout $u$ on a :

$$\begin{aligned}(x+u)^m &= x^m + \binom{m}{1} x^{m-1}u + \binom{m}{2} x^{m-2}u^2 + \ldots + \binom{m}{m-2} x^2 u^{m-2} \\ &\quad + \binom{m}{m-1} x u^{m-1} + u^m \\ &= x^m + \binom{m}{1} x^{m-1}u + \binom{m}{2} x^{m-2}u^2 + \left( \binom{m}{3} x^{m-3} + \ldots + u^{m-3} \right) u^3 \\ &\equiv x^m + \binom{m}{1} x^{m-1}u + \binom{m}{2} x^{m-2}u^2 \pmod{u^3}.\end{aligned}$$

Cela nous permet de conclure.

On passe maintenant à la dernière étape avant de définir la notion de polynôme Morse en caractéristique 2.

**Définition 3.2.5.** Soient $K$ un corps de caractéristique 2 et $f$ un polynôme sur $K$. On dit que les points critiques de $f$ sont non dégénérés si $f'$ et $f^{[2]}$ n'ont pas de racines communes.

**Exemple 3.2.6.** (1) On remarque que pour $f(x) = x^3$, 0 est une racine commune de $f'$ et $f^{[2]}$ et donc les points critiques de $f$ sont non dégénérés.

(2) Si $f(x) = x^2$, on a $f'(x) = 0$ et $f^{[2]}(x) = 1 \neq 0$ et donc les points critiques de $f$ sont non dégénérés.

On est prêt maintenant à définir un polynôme Morse. On va se limiter aux cas des polynômes définis sur des corps de caractéristique 2. Pour une définition plus générale voir l'annexe de Geyer dans [16].

**Définition 3.2.7.** Soient $K$ un corps de caractéristique 2 et $f(x) \in K[x]$ . On dit que $f$ est Morse s'il vérifie les trois conditions suivantes :

$(M_1)$ Les points critiques de $f$ sont non dégénérés.

$(M_2)$ Les valeurs critiques de $f$ sont distinctes.

$(M_3)$ 2 ne divise pas le degré de $f$.

Pour faciliter la définition d'un polynôme Morse et pour l'adapter dans notre contexte on va introduire la définition de résultant.

**Définition 3.2.8.** Le résultant des deux polynômes $P$ et $Q$ est le déterminant de leur matrice de Sylvester.

La remarque suivante permet d'adapter la notion de résultant dans notre contexte.

**Remarque 3.2.9.** Soit $K$ un corps de caractéristiques $p$. Soient $f$ et $g$ deux polynômes sur $K$ de degré $n$ et $m$ respectivement tel que

$$f(x) = a_n \prod_{i=1}^{n} (x - \alpha_i)$$

et

$$g(x) = b_m \prod_{i=1}^{m} (x - \beta_i).$$

On définit le résultant de $f$ et $g$ par :

$$\mathrm{Res}(f, g) = a_n^m b_m^n \prod_{i,j} (\alpha_i - \beta_j).$$

**Remarque 3.2.10.** Considérons un corps $K$. Soient $f$ et $g$ deux polynômes sur $K$ de degré $n$ et $m$ respectivement. On a :

(1) $\mathrm{Res}(f, g) = (-1)^{nm} \mathrm{Res}(g, f)$

(2) $\mathrm{Res}(f, g) = 0$ si et seulement si $f$ et $g$ ont au moins une racine commune.

Dans notre travail les conditions $M_1, M_2$ et $M_3$ présentées dans la Définition 3.2.7 vont êtres caractérisées respectivement par les conditions $M_1', M_2'$ et $M_3'$ qui leur sont équivalentes.

**Proposition 3.2.11.** *Soient $K$ un corps de caractéristiques 2 et $f \in K[x]$ un polynôme de degré $s$. On dit que $f$ est Morse s'il vérifie les trois conditions suivantes.*

*($M_1'$) Le polynôme*

$$\mathrm{Res}(f', f^{[2]}) \neq 0.$$

*($M_2'$) Le polynôme*

$$\Pi_d(f) := \prod_{i<j} (f(\tau_i) - f(\tau_j)) \neq 0$$

*où les $\tau_i$ sont les racines de $f'$.*

*($M_3'$) Le degré $s$ est impair.*

*Démonstration.* En utilisant la Remarque 3.2.10 on obtient l'équivalence entre $M_1$ et $M_1'$. Ce qui permet de conclure. □

## 3.3 L'ingrédient principal de la démonstration

Dans cette section. on va donner la méthode de la preuve qui va nous permettre de démontrer les nouveaux théorèmes. L'ingrédient principal de la démonstration introduit par Voloch ([26]) dans ce contexte est le théorème de densité de Chebotarev. Pour pouvoir l'appliquer, l'idée d'Aubry, Herbaut et Voloch ([2]) est de trouver pour $n$ suffisamment grand un élément non nul $\alpha \in \mathbb{F}_{2^n}^*$ pour lequel l'extension $\Omega/\mathbb{F}_{2^n}(t)$ est régulière, où $\Omega$ est le corps de décomposition du polynôme $f(x) + f(x+\alpha) + t$ sur $\mathbb{F}_{2^n}(t)$.

### Vocabulaire des corps de fonctions

Avant d'énoncer ce théorème, on va rappeler quelques notions algébriques essentielles. Rappelons d'abord la définition d'une extension régulière.

**Définition 3.3.1.** Une extension $L/K$ est dite régulière si $L/K$ est séparable et $K$ est algébriquement fermé dans $L$ (c'est-à-dire $K$ n'admet pas d'extension algébrique propre dans $L$) .

Il est bien connu que toute extension d'un corps algébriquement clos est régulière et que la régularité est transitive. De plus, si $L/K$ est régulière et $K \subset M \subset L$, alors $M/K$ est régulière.

On donne maintenant la définition d'un corps de fonctions (tous les éléments de ce paragraphe sont tirés avec plus ou moins de détails du Chapitre 1 de [25]).

**Définition 3.3.2.** Considérons deux corps $K$ et $F$ avec $K \subseteq F$. On dit que $F$ est un corps de fonction sur $K$ s'il existe un élément transcendant $x$ sur $K$ pour lequel l'extension $F/K(x)$ est algébrique.

Pour simplifier, on dit que $F/K$ est un corps de fonctions algébrique. La somme, produit et division de deux éléments algébrique est également algébrique. Cela nous permet de définir le corps des constantes.

**Définition 3.3.3.** Soit $F/K$ une extension telle que $F$ est un corps de fonctions sur $K$. Le corps des constantes de l'extension $F/K$ est le corps $\tilde{K}$ défini par :

$$\tilde{K} := \{u \in F; u \text{ est algébrique sur } K\}.$$

Pour pouvoir définir une place $P$ d'un corps de fonction $F/K$, on introduit dans la définition suivante la notion d'anneau de valuation.

**Définition 3.3.4.** Soit $F/K$ un corps de fonction et considérons un anneau $\mathcal{O}$ tel que

$$K \subset \mathcal{O} \subset F.$$

On dit que $\mathcal{O}$ est un anneau de valuation de $F/K$ si pour tout élément $z \in F$ on a $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$.

Comme expliquée dans [25], la motivation de la Définition 3.3.4 apparaît dans l'exemple suivant.

**Exemple 3.3.5.** Considérons un corps $K$ et

$$K(x) = \{\frac{p(x)}{q(x)}; p(x), q(x) \in K[x]\}.$$

L'extension $K(x)/K$ est un corps de fonction appelé corps des fonctions rationnelles. Pour tout polynôme irréductible $p(x) \in K[x]$, l'anneau

$$O_p(x) = \{\frac{f(x)}{g(x)}; f(x), g(x) \in K[x], p(x) \text{ ne divise pas } g(x)\}$$

est un anneau de valuation de $F/K$.

**Remarque 3.3.6** (Proposition 1.1.5 de [25])**.** Si $\mathcal{O}$ est un anneau de valuation d'un corps de fonction $F/K$ alors il admet un unique idéal maximal $P$.

On est prêt maintenant à définir la notion de place d'un corps de fonction.

**Définition 3.3.7.** Soit $F/K$ un corps de fonction. Une place $P$ de $F/K$ est l'idéal maximal d'un certain anneau de valuation $\mathcal{O}$.

La remarque suivante nous permet d'introduire la notion d'élément premier.

**Remarque 3.3.8** (Théorème 1.1.6 et Définition 1.1.8 dans [25])**.** Si $P$ est une place d'un corps de fonctions $F/K$ alors $P$ est un idéal principal. De plus tout élément $t \in \mathcal{O}$ pour lequel $P = t\mathcal{O}$ est dit élément premier de $F/K$.

La remarque suivante nous donne un exemple de place dans le cas des corps des fonctions rationnelles.

**Remarque 3.3.9.** Soit $K(x)/K$ un corps de fonctions rationnelles et $p(x) \in K[x]$ un polynôme irréductible. L'anneau

$$O_{p(x)} := \{\frac{f(x)}{g(x)}; f(x), g(x) \in K[x], \quad p(x) \text{ ne divise pas } g(x)\}$$

est un anneau de valuation de $K(x)/K$. De plus l'idéal

$$P_{p(x)} = \{\frac{f(x)}{g(x)}; f(x), g(x) \in K[x], p(x) \text{ divise } f(x) \text{ et } p(x) \text{ ne divise pas } g(x)\}$$

est l'unique idéal maximal de $O_{p(x)}$. Dans ce cas, $p(x)$ est un élément premier de $K(x)/K$.

Rappelons maintenant la définition du degré d'un élément premier.

**Définition 3.3.10.** Soient $F/K$ un corps de fonction d'anneau de valuation $\mathcal{O}$ et $P$ une place de $F/K$. On définit le degré de $P$ par $\deg(P) := [\mathcal{O}/P : K]$, où $[\mathcal{O}/P : K]$ désigne le degré de l'extension $(\mathcal{O}/P)/K$

La proposition suivante nous permet de calculer le degré d'une place dans le cas des corps de fonctions rationnelles.

**Proposition 3.3.11** (Proposition 1.2.1 dans [25])**.** *Soit $K(x)/K$ un corps de fonctions rationnelles et $p(x) \in K[x]$ un polynôme irréductible. Le degré de la place $P_{p(x)}$ est égal au degré du polynôme $p$. De plus $K$ est le corps des constantes de $K(x)$.*

### Théorème de densité de Chebotarev

Dans ce paragraphe on va présenter l'ingrédient principal de la démonstration. C'est le théorème de densité de Chebotarev. Ce théorème est l'un des résultats fondamentaux de la théorie algébrique des nombres. Voloch explique dans [26] qu'*il fournit une mesure quantitative d'ensembles de diviseurs premiers avec des propriétés qualitatives liées à des extensions galoisiennes finies. Sa nature fondamentale le rend très pratique à appliquer.*

Rappelons une version du théorème de densité de Chebotarev donnée par Pollack dans [21].

**Théorème 3.3.12.** ***(Chebotarev)*** *Supposons que $\Omega/\mathbb{F}_q(t)$ est une extension Galoisienne de corps de constantes $\mathbb{F}_{q^D}$. Soit $\mathcal{C}$ une classe de conjugaison de $\mathrm{Gal}(\Omega/\mathbb{F}_q(t))$ dont la restriction de chaque élément à $\mathbb{F}_{q^D}$ est $x^q$. Soit $V(\mathcal{C})$ le nombre de premiers de degré 1 sur $\mathbb{F}_q(t)$ non ramifiés dans $\Omega$ pour lesquels le symbole d'Artin $\left(\frac{\Omega/\mathbb{F}_q(t)}{v}\right)$ est égale à $\mathcal{C}$.*

*On a*

$$\left|V(\mathcal{C}) - \frac{\sharp\mathcal{C}}{[\Omega : \mathbb{F}_{q^D}(t)]}q\right| \leq 2\frac{\sharp\mathcal{C}}{[\Omega : \mathbb{F}_{q^D}(t)]}\big(gq^{1/2} + g + [\Omega : \mathbb{F}_{q^D}(t)]\big),$$

*où $g$ est le genre de $\Omega/\mathbb{F}_{q^D}$.*

On considère le corps de décomposition $\Omega$ du polynôme $f(x)+f(x+\alpha)+t$. Pour pouvoir appliquer le théorème de densité de Chebotarev on a besoin de la régularité de l'extension $\Omega/\mathbb{F}_{2^n}(t)$. Pour cela, on introduit un corps intermédiaire $F$, qui est le corps de décomposition du polynôme $L_\alpha f(x)+t$. On démontre ensuite que les extensions $\Omega/F$ et $F/\mathbb{F}_{2^n}(t)$ sont régulières.

**Définition 3.3.13.** Soit $n \in \mathbb{N}$. Considérons un polynôme $f(x) \in \mathbb{F}_{2^n}[x]$ et notons $L_\alpha f$ le polynôme associé. On définit le corps $F$ par le corps de décomposition du polynôme $L_\alpha f(x) - t$ sur $\mathbb{F}_{2^n}(t)$ où $t$ est un élément transcendant sur $\mathbb{F}_{2^n}$.

Le lemme suivant nous donne une condition suffisante pour que l'extension $F/\mathbb{F}_{2^n}(t)$ soit régulière.

**Lemme 3.3.14** (Proposition 4.1 dans [2])**.** *Si $f \in \mathbb{F}_{2^n}[x]$ est un polynôme tel que $L_\alpha f$ est Morse et de degré impair alors l'extension $F/\mathbb{F}_{2^n}(t)$ est régulière.*

La démonstration du lemme s'appuie sur l'analogue du théorème de Hilbert donné par Serre dans le Théorème 4.4.5 de [24] et détaillé en caractéristique paire dans l'annexe de Geyer dans [16]. Il nous donne que le groupe de monodromie géométrique $\mathrm{Gal}(F/\mathbb{F}_{2^n}^F(t))$ est égal au groupe symétrique $S_d$. Mais comme il est inclus dans $\mathrm{Gal}(F/\mathbb{F}_{2^n}(t))$ qui est à son tour inclus dans $S_d$ alors $\mathrm{Gal}(F/\mathbb{F}_{2^n}(t) = \mathrm{Gal}(F/\mathbb{F}_{2^n}^F(t))$.

Donnons maintenant le lemme suivant qui nous fournit une condition suffisante pour que l'extension $\Omega/F$ soit régulière.

**Lemme 3.3.15** (Proposition 4.6 dans [2])**.** *Soit $n \in \mathbb{N}$. Considérons un polynôme $f(x) = \sum_{k=0}^{m} a_{m-k}x^k \in \mathbb{F}_{2^n}[x]$ de degré $m \in \mathbb{N}$ et notons $L_\alpha f(x) = \sum_{k=0}^{d} b_{d-k}x^k$ le polynôme associé de degré $d$. Pour tout $\alpha \in \mathbb{F}_{2^n}^*$, si $L_\alpha f$ est Morse et l'équation $x^2 + \alpha x = \frac{b_1}{b_0}$ admet une solution dans $\mathbb{F}_{2^n}$ alors l'extension $\Omega/F$ est régulière (et par suite l'extension $\Omega/\mathbb{F}_{2^n}(t)$ est régulière).*

La méthode consiste à démontrer l'égalité entre les deux groupes $\Gamma = \mathrm{Gal}(\Omega/F)$ et $\overline{\Gamma} = \mathrm{Gal}(\Omega/F\mathbb{F}_{2^n}^\Omega)$, en montrant qu'ils sont égales au groupe $(\mathbb{Z}/2\mathbb{Z})^{d-1}$.

La proposition suivante résume la contribution du Théorème 3.3.12 dans notre contexte.

**Proposition 3.3.16.** *Soit $f \in \mathbb{F}_{2^n}[x]$ un polynôme de degré $m \equiv 0 \pmod 4$. Il existe $N \in \mathbb{N}^*$, tel que pour tout $n \geq N$, pour tout polynôme $f(x) \in \mathbb{F}_{2^n}[x]$ de degré $m$, et pour tout $\alpha \in \mathbb{F}_{2^n}^*$, tel que $\Omega/\mathbb{F}_{2^n}(t)$ est régulière, il existe $\beta \in \mathbb{F}_{2^n}$ tel que $f(x) + f(x+\alpha) + \beta$ est scindé sans racines multiples, et donc $\delta(f)$ est maximal.*

*Démonstration.* Comme l'extension $\Omega/\mathbb{F}_{2^n}(t)$ est régulière et le degré du polynôme $L_\alpha f$ est impair alors $\Omega/\mathbb{F}_{2^n}(t)$ est séparable. De plus $\Omega$ est bien le corps de décomposition du polynôme $f(x) + f(x+\alpha) + t$ sur $\mathbb{F}_{2^n}(t)$, donc $\Omega/\mathbb{F}_{2^n}(t)$ est normale et

par suite Galoisienne. Considérons $V$ le nombre de places de degré 1 sur $\mathbb{F}_{2^n}(t)$ non ramifiées dans $\Omega$ pour lesquels le symbole d'Artin est égal à $C$. En appliquant le Théorème 3.3.12 sur l'extension $\Omega/\mathbb{F}_{2^n}(t)$ on obtient :

$$V > \frac{2^n}{d_\Omega} - 2\left((1+\frac{g_\Omega}{d_\Omega})2^{\frac{n}{2}} + 2^{\frac{n}{4}} + 1 + \frac{g_\Omega}{d_\Omega}\right)$$

où $d_\Omega = [\Omega : \mathbb{F}_{2^n}(t)]$ et $g_\Omega$ est le genre de $\Omega$. En utilisant la démonstration du Lemme 3.3.14 et la démonstration du Lemme 3.3.15, on obtient $\mathrm{Gal}(F/\mathbb{F}_{2^n}(t)) = S_d$ et $\mathrm{Gal}(\Omega/F) = (\mathbb{Z}/2\mathbb{Z})^{d-1}$ et par suite $d_\Omega = d!2^{d-1}$. De plus en utilisant le Lemme 14 dans [21], on obtient :

$$g_\Omega \leq d!2^{d-1}(d-3/2)+1.$$

Cela implique l'existence d'un entier $N \in N$ pour lequel $v \geq 1$ et par suite il existe $\beta \in \mathbb{F}_{2^n}$ pour lequel le polynôme $f(x)+f(x+\alpha)+\beta$ est scindé sans racines multiples. □

La remarque suivante fournit un entier $N$ pour lequel la Proposition 3.3.16 s'applique pour tout $n \geq \mathbb{N}$.

**Remarque 3.3.17.** Soit $n \in \mathbb{N}$. Si l'extension $\Omega/\mathbb{F}_{2^n}(t)$ est régulière et

$$\frac{q}{d_\Omega} - 2\Big((1+\frac{g_\Omega}{d_\Omega})q^{1/2} + q^{1/4} + 1 + \frac{g_\Omega}{d_\Omega}\Big) \geqslant 1. \tag{3.8}$$

avec $q = 2^n$, $d_\Omega = d!2^{d-1}$ et $g_\Omega \leqslant d!2^d(d-3/2)+1$, alors le polynôme $f(x) + f(x+\alpha) + \beta$ est scindé sans racines multiples et par suite $\delta(f)$ est maximale.

Le corollaire suivant permet de résumer les deux grandes étapes à vérifier pour démontrer les nouveaux résultats de la thèse.

**Corollaire 3.3.18.** *Soit $f(x) = \sum_{k=0}^{m} a_{m-k}x^k \in \mathbb{F}_{2^n}[x]$ un polynôme de degré $m \equiv 0 \pmod 4$ tel que $a_1 \neq 0$ et soit $L_\alpha f = \sum_{k=0}^{d} b_{d-k}x^k$ le polynôme associé de degré $d$. S'il existe un $\alpha \in \mathbb{F}_{2^n}^*$ tel que :*

*(1) Le polynôme $L_\alpha f$ est Morse.*

*(2) Il existe $x \in \mathbb{F}_{2^n}$ tel que $x^2 + \alpha x = \frac{b_1}{b_0}$,*

*alors pour $n$ suffisamment grand, $\delta_{\mathbb{F}_{2^n}}(f)$ est maximal, autrement dit on a $\delta_{\mathbb{F}_{2^n}}(f) = m-2$.*

*Démonstration.* En utilisant la Proposition 3.3.16, pour que l'uniformité différentielle de $f$ soit maximale, on est ramené à trouver un $\alpha \in \mathbb{F}_{2^n}^*$ pour lequel l'extension $\Omega/\mathbb{F}_{2^n}(t)$ est régulière. Pour montrer que l'extension $\Omega/\mathbb{F}_{2^n}(t)$ est régulière, on construit un corps intermédiaire $F$ qui est le corps de décomposition du polynôme $L_\alpha f(x) - t$ sur $\mathbb{F}_{2^n}(t)$ et on démontre que les deux extensions $F/\mathbb{F}_{2^n}(t)$ et $\Omega/F$ sont régulières. Soit $\alpha \in \mathbb{F}_{2^n}^*$, tel que :

(1) Le polynôme $L_\alpha f$ est Morse.

(2) Il existe $x \in \mathbb{F}_{2^n}$ tel que $x^2 + \alpha x = \frac{b_1}{b_0}$,

Comme $L_\alpha f$ est Morse et $d = \frac{m-2}{2}$ est impair, alors par le Lemme 3.3.14, l'extension $F/\mathbb{F}_{2^n}(t)$ est régulière. De plus, comme l'équation $x^2 + \alpha x$ a une solution dans $\mathbb{F}_{2^n}$, alors par le Lemme 3.3.15, l'extension $\Omega/F$ est régulière et donc l'extension $\Omega/\mathbb{F}_{2^n}(t)$ est régulière, ce qui nous permet de conclure. □

Résumons les conditions à vérifier dans le diagramme suivant. Nous ferons référence régulièrement à ces quatre conditions ((I.a), (I.b), (I.c) et (II)) à la suite de notre travail.

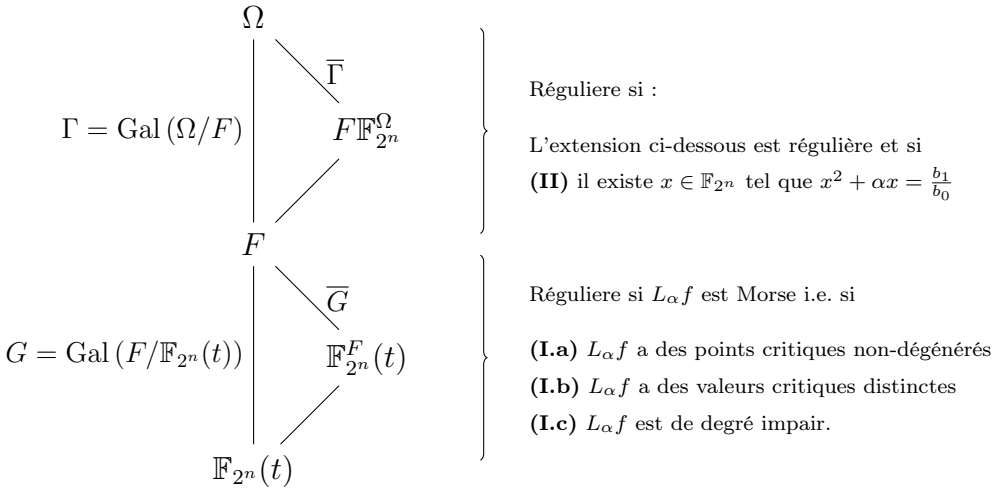


FIGURE 3.1 –

Dans ce manuscrit, on s'intéresse aux polynômes de degré $m \equiv 0 \pmod 4$ et donc la condition (I.c) est automatiquement vérifiée. En effet, si $m \equiv 0 \pmod 4$, alors $d(m) = \frac{m-2}{2}$ est impair. Donc pour un polynôme $f \in \mathbb{F}_{2^n}[x]$, de degré $m \equiv 0 \pmod 4$, pour démontrer que $\delta(f)$ est maximale il suffit de trouvez un $\alpha \in \mathbb{F}_{2^n}^*$ pour lequel les conditions (I.a), (I.b) et (II) sont vérifiées. On va utiliser la même procédure utilisée dans [2] : d'abord on majore le nombre de $\alpha \in \mathbb{F}_{2^n}^*$, pour lesquels une au moins des trois conditions (I.a), (I.b) et (II) n'est pas vérifiée. Ensuite, en choisissant $n$ suffisamment grand, on garantit l'existence d'un $\alpha \in \mathbb{F}_{2^n}^*$ pour lequel les trois conditions sont vérifiées simultanément. Finalement, comme $n$ est choisi suffisamment grand et l'extension $\Omega/\mathbb{F}_{2^n}(t)$ est régulière, on obtient que l'uniformité différentielle de $f$ est maximale.

## 3.4 Le théorème 90 de Hilbert.

On commence cette section par un rappel de quelques propriétés de la trace. On peut par exemple consulter [19] pour plus de détails. On termine par une version additive du théorème 90 de Hilbert qui va nous permettre de transformer la condition (II) en une équation algébrique. Commençons d'abord par la définition de la trace d'un élément sur un corps fini.

**Définition 3.4.1.** Soient $K$ un corps fini de caractéristiques $p$ et $L/K$ une extension

fini de degré $n$. Pour tout $a \in L$, on définit la trace de $a$ sur $L/K$ par :

$$\mathrm{Tr}_{L/K}(a) = a + a^p + \cdots + a^{p^{n-1}}.$$

On remarque que pour tout $a \in L$ on a :

$$(\mathrm{Tr}_{L/K}(a))^p = \mathrm{Tr}_{L/K}(a^p) = \mathrm{Tr}_{L/K}(a). \tag{3.9}$$

Le lemme suivant est un ingrédient essentiel dans la démonstration du Corollaire 5.1.4. Il nous dit que les éléments de $\mathbb{F}_{2^n}$ prend autant de fois la valeur 1 que la valeur 0.

**Lemme 3.4.2.** *Soit $n \in \mathbb{N}^*$. On a :*

$$\mathrm{Card}\left(\{b \in \mathbb{F}_{2^n}; \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(b) = 0\}\right) = \mathrm{Card}\left(\{b \in \mathbb{F}_{2^n}; \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(b) = 1\}\right) = 2^{n-1}.$$

*Démonstration.* Soit $S := \{b \in \mathbb{F}_{2^n}; \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(b) = 0\}$. Montrons que $\mathrm{Card}(S) = 2^{n-1}$. On a :

$$\begin{aligned} b \in S &\iff \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(b) = 0 \\ &\iff b \text{ est une racine de } T(x) = x + x^2 + x^4 + \cdots + x^{2^{n-1}}. \end{aligned}$$

Comme $T'(x) = 1 \neq 0$, les racines de $T$ sont distinctes. Comme $T(0) = 0$ et $\mathbb{F}_{2^n}/\mathbb{F}_2$ est normale, l'extension $\mathbb{F}_{2^n}$ contient tous les racines de $T$ et donc $\mathrm{Card}(S) = \deg(T) = 2^{n-1}$. Soit $S' := \{b \in \mathbb{F}_{2^n}; \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(b) = 1\}$. On a

$$\mathrm{Card}(S) + \mathrm{Card}(S') = 2^n,$$

cela nous permet de conclure. □

On rappelle maintenant la version additive du théorème 90 de Hilbert.

**Théorème 3.4.3.** *Soit $K$ un corps finis de caractéristique $p$ et $L/K$ une extension de degré $n$. On a pour tout $x \in L$ l'équivalence suivante :*

$$\mathrm{Tr}_{L/K}(x) = 0 \iff \textit{Il existe } \ \alpha \in L \textit{ tel que } x = \alpha - \alpha^p.$$

*Démonstration.* Soit $x \in L$ tel que $\mathrm{Tr}_{L/K}(x) = 0$. Montrons qu'il existe $\alpha \in L$ tel que $x = \alpha - \alpha^p$. Comme $\mathrm{Tr}_{L/K}$ est une application non nulle, il existe $\beta \in L$ tel que $\mathrm{Tr}_{L/K}(\beta) \neq 0$. Prenons

$$\alpha = \frac{1}{\mathrm{Tr}_{L/K}(\beta)} \left( x\beta + (x + x^p)\beta^p + \cdots + (x + x^p + \cdots + x^{p^{n-2}})\beta^{p^{n-2}} \right).$$

En utilisant l'équation 3.9, on a

$$\alpha^p = \frac{1}{\mathrm{Tr}_{L/K}(\beta)} \left( x^p\beta^p + (x^p + x^{p^2})\beta^{p^2} + \cdots + (x^p + \cdots + x^{p^{n-1}})\beta^{p^{n-1}} \right),$$

donc

$$\alpha - \alpha^p = \frac{1}{\mathrm{Tr}_{L/K}(\beta)} \left( x\beta + x\beta^p + \cdots + x\beta^{p^{n-2}} + (x^p + x^{p^2} + x^{p^3} + \cdots + x^{p^{n-1}})\beta^{p^{n-1}} \right).$$

Comme $\mathrm{Tr}_{L/K}(x) = 0$, on a

$$\alpha - \alpha^p = \frac{1}{\mathrm{Tr}_{L/K}(\beta)} \left( x\beta + x\beta^p + x\beta^{p^2} + \cdots + x\beta^{p^{n-2}} + x\beta^{p^{n-1}} \right),$$

donc

$$\alpha - \alpha^p = \frac{1}{\mathrm{Tr}_{L/K}(\beta)} (x \,\mathrm{Tr}_{L/K}(\beta)) = x.$$

Inversement, soit $\alpha \in L$ tel que $x = \alpha - \alpha^p$. En utilisant la linéarité de la Trace et l'équation 3.9 on a :

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}_{L/K}(\alpha - \alpha^p) = \mathrm{Tr}_{L/K}(\alpha) - \mathrm{Tr}_{L/K}(\alpha^p) = 0.$$

□

Le corollaire suivant nous permet d'exprimer la condition (I) en terme de la Trace. Autrement dit si $f(x) = \sum_{k=0}^{m} a_{m-k}x^k \in \mathbb{F}_{2^n}[x]$ un polynôme de degré $m$ tel que $a_1 \neq 0$ et $\alpha \in \mathbb{F}_{2^n}^*$ et si on note

$$L_\alpha f(x) = \sum_{k=0}^{d} b_{d-k}x^k \in \mathbb{F}_{2^n}[x]$$

le polynôme associé, pour trouver un $\alpha \in \mathbb{F}_{2^n}^*$ pour lequel il existe un $x \in \mathbb{F}_{2^n}$ vérifiant

$$x^2 + \alpha x = \frac{b_1}{b_0},$$

il faut et il suffit de trouver un $\alpha \in \mathbb{F}_{2^n}^*$ tel que

$$\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\frac{b_1}{b_0\alpha^2}) = 0.$$

**Corollaire 3.4.4.** *Soient $b_0, \alpha \in \mathbb{F}_{2^n}^*$ et $b_1 \in \mathbb{F}_{2^n}$. Les deux conditions suivantes sont équivalentes :*

*(1) Il existe $x$ dans $\mathbb{F}_{2^n}$ tel que $x^2 + \alpha x = \frac{b_1}{b_0}$.*

*(2)* $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\frac{b_1}{b_0\alpha^2}) = 0$.

*Démonstration.* Il existe $x$ dans $\mathbb{F}_{2^n}$ tel que

$$x^2 + \alpha x = \frac{b_1}{b_0},$$

soit tel que

$$(\frac{x}{\alpha})^2 + \frac{x}{\alpha} = \frac{b_1}{b_0\alpha^2},$$

si et seulement s'il existe $y$ dans $\mathbb{F}_{2^n}$ tel que

$$y^2 + y = \frac{b_1}{b_0\alpha^2},$$

ce qui est équivalent par le Théorème 3.4.3 à démontrer que

$$\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\frac{b_1}{b_0\alpha^2}) = 0.$$

□

## 3.5 La condition (II)

Dans cette section on va minorer le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels la condition (II) est vérifiée, puis on va majorer le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels la condition (I.a) n'est pas vérifiée. On commence par les deux lemmes suivants qui jouent un rôle important dans la démonstration du Corollaire 5.1.4.

**Lemme 3.5.1.** *Soient $a_1, a_2$ et $a_3$ dans $\mathbb{F}_{2^n}$ tel que $a_1 \neq 0$ et $n \in \mathbb{N}^*$. Si*

$$a_2^2 + a_3 a_1 \neq 0$$

*alors pour tout $\alpha \in \mathbb{F}_{2^n}^*$ l'application*

$$\alpha \mapsto \frac{a_2^2 + a_3 a_1}{a_1^2 \alpha^2}$$

*est une permutation de $\mathbb{F}_{2^n}^*$.*

*Démonstration.* Il suffit de démontrer que l'application

$$\begin{array}{rccc} T & : & \mathbb{F}_{2^n}^* & \to & \mathbb{F}_{2^n}^* \\ & & \alpha & \mapsto & \frac{1}{\alpha^2} \end{array}$$

est une permutation de $\mathbb{F}_{2^n}^*$. Soit

$$\begin{array}{rccc} T' & : & \mathbb{F}_{2^n}^* & \to & \mathbb{F}_{2^n}^* \\ & & \alpha & \mapsto & \frac{1}{\alpha^{2^{n-1}}}. \end{array}$$

On a

$$T \circ T'(\alpha) = T(\frac{1}{\alpha^{2^{n-1}}}) = (\alpha^{2^{n-1}})^2 = \alpha^{2^n}$$

De même

$$T' \circ T(\alpha) = T'(\frac{1}{\alpha^2}) = (\alpha^2)^{2^{n-1}} = \alpha^{2^n}$$

On conclut en utilisant que $\alpha^{2^n} = \alpha$.

□

**Lemme 3.5.2.** *Considérons $n \in \mathbb{N}^*$ et un entier $m \equiv 0 \pmod 8$. Soit $f = \sum_{i=0}^{m} a_{m-i} X^i \in \mathbb{F}_{2^n}[X]$ un polynôme de degré $m$, tel que $a_1 \neq 0$. On note $L_\alpha(f) = \sum_{i=0}^{d} b_{d-i} X^i$ le polynôme associé de degré $d$. On a*

$$\mathrm{Tr}(\frac{b_1}{b_0\alpha^2}) = \mathrm{Tr}(\frac{a_2^2 + a_3 a_1}{(a_1\alpha)^2})$$

*pour tout $\alpha \in \mathbb{F}_{2^n}^\star$.*

*Démonstration.* On a par le Corollaire 3.1.5 que

$$\frac{b_1}{b_0} = \frac{a_2\alpha + a_3}{a_1}.$$

Donc

$$\begin{aligned} \mathrm{Tr}(\frac{b_1}{b_0\alpha^2}) &= \mathrm{Tr}(\frac{a_2\alpha + a_3}{a_1\alpha^2}) && (3.10) \\ &= \mathrm{Tr}(\frac{a_2 a_1 \alpha + a_1 a_3}{(a_1)^2\alpha^2}) && (3.11) \\ &= \mathrm{Tr}(\frac{a_2}{a_1\alpha}) + \mathrm{Tr}(\frac{a_1 a_3}{(a_1)^2\alpha^2}) && (3.12) \\ &= \mathrm{Tr}(\frac{(a_2)^2}{(a_1)^2(\alpha)^2}) + \mathrm{Tr}(\frac{a_1 a_3}{(a_1)^2\alpha^2}) && (3.13) \\ &= \mathrm{Tr}(\frac{a_2^2 + a_3 a_1}{(a_1\alpha)^2}). && (3.14) \end{aligned}$$

□

Le corollaire suivant permet de minorer pour un polynôme $f \in \mathbb{F}_{2^n}[x]$ de degré $m \equiv 0 \pmod 8$, le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels la condition (II) est vérifiée.

**Corollaire 3.5.3.** *Soit $f = \sum_{i=0}^{m} a_{m-i}X^i \in \mathbb{F}_{2^n}[X]$ un polynôme de degré $m$ tel que $m \equiv 0 \pmod 8$, $a_1 \neq 0$ et $n \in \mathbb{N}^*$. Soit $L_\alpha(f) = \sum_{i=0}^{d} b_{d-i}X^i$ le polynôme associé de degré $d$. Le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ tel que $\mathrm{Tr}(\frac{b_1}{b_0\alpha^2}) = 0$ est $2^{n-1} - 1$ si $a_2^2 + a_3a_1 \neq 0$ et $2^n - 1$ sinon.*

*Démonstration.* Supposons que $a_2^2 + a_3a_1 \neq 0$ et soit

$$\sigma : \alpha \mapsto \frac{a_2^2 + a_3a_1}{(a_1\alpha)^2}$$

la permutation de $\mathbb{F}_{2^n}^*$ défini dans le Lemme 3.5.1. Soit $\alpha \in \mathbb{F}_{2^n}^*$, on a par le Lemme 5.1.4 que

$$\mathrm{Tr}(\frac{b_1}{b_0\alpha^2}) = \mathrm{Tr}(\frac{a_2^2 + a_3a_1}{(a_1\alpha)^2}).$$

Comme $\sigma$ est une permutation, le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ tel que $\mathrm{Tr}(\sigma(\alpha)) = 0$ est égale au nombre de $\beta \in \mathbb{F}_{2^n}^*$ tel que $\mathrm{Tr}(\beta) = 0$. On conclut en utilisant le Lemme 3.4.2. Si $a_2^2 + a_3a_1 = 0$ alors $\mathrm{Tr}(\frac{b_1}{b_0\alpha^2}) = 0$ pour tout $\alpha \in \mathbb{F}_{2^n}^*$, cela nous nous permet de conclure. □

On remercie José Felipe Voloch pour la démonstration du corollaire suivant qui nous aide à minorer pour un polynôme $f \in \mathbb{F}_{2^n}[x]$ de degré $m \equiv 4 \pmod 8$, le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels la condition (II) est vérifiée

**Corollaire 3.5.4.** *Soit $f = \sum_{i=0}^{m} a_{m-i}X^i \in \mathbb{F}_{2^n}[X]$ un polynôme de degré $m$ tel que $m \equiv 4 \pmod 8$, $a_1 \neq 0$ et $n \in \mathbb{N}^*$. Soit $L_\alpha(f) = \sum_{i=0}^{d} b_{d-i}X^i$ le polynôme associé de degré $d$. Le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ tel que $\mathrm{Tr}(\frac{b_1}{b_0\alpha^2}) = 0$ est égale $2^n - 1$ si $a_2^2 + a_1a_3 = 0$ et plus grand ou égale à $\frac{1}{2}(2^n + 2^{\frac{n}{2}+1} - 1)$ sinon.*

*Démonstration.* En utilisant le Corollaire 3.1.5, on a :

$$\mathrm{Tr}(\frac{b_1}{b_0\alpha^2}) = \mathrm{Tr}(1 + \frac{a_0\alpha}{a_1} + \frac{a_2^2 + a_1a_3}{a_1^2\alpha^2})$$

Donc $\mathrm{Tr}(\frac{b_1}{b_0\alpha^2}) = 0$ si et seulement si

$$\mathrm{Tr}(\frac{a_0\alpha}{a_1} + \frac{a_2^2 + a_1a_3}{a_1^2\alpha^2}) = n.$$

On distingue deux cas :

(1) Si $a_2^2 + a_1 a_3 = 0$, alors $\mathrm{Tr}(\frac{b_1}{b_0\alpha^2}) = 0$ si et seulement si

$$\mathrm{Tr}(\frac{a_0\alpha}{a_1}) = n.$$

Comme l'application

$$\alpha \mapsto \frac{a_0\alpha}{a_1}$$

est une permutation, le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ tel que $\mathrm{Tr}(\frac{a_0\alpha}{a_1}) = n$ est égale au nombre de $\beta \in \mathbb{F}_{2^n}^*$ tel que $\mathrm{Tr}(\beta) = n$. On conclut en utilisant le Lemme 3.4.2.

(2) Supposons maintenant que $a_2^2 + a_1 a_3 \neq 0$. En choisissant $C = \frac{a_0}{a_1}$ et $D^2 = \frac{a_2^2 + a_1 a_3}{a_1^2}$, le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ tel que $\mathrm{Tr}(\frac{b_1}{b_0\alpha^2}) = 0$ est égale au nombre de $\alpha \in \mathbb{F}_{2^n}^*$ tel que

$$\mathrm{Tr}(C\alpha) + \mathrm{Tr}(D/\alpha) = n.$$

En choisissant maintenant $K^2 = CD$ et $v = a_0\alpha/a_1K$, le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ tel que $\mathrm{Tr}(\frac{b_1}{b_0\alpha^2}) = 0$ est égale au nombre de $v \in \mathbb{F}_{2^n}^*$ tel que

$$\mathrm{Tr}(Kv) + \mathrm{Tr}(K/v) = n.$$

Prenons $S$ tel que $\mathrm{Tr}(S) = n$ on a

$$\mathrm{Tr}(Kv) + \mathrm{Tr}(K/v) = n$$

si et seulement si

$$\mathrm{Tr}(Kv + K/v + S) = 0.$$

Donc on est ramené à calculer le nombre de $v \in \mathbb{F}_{2^n}^*$ tel que

$$\mathrm{Tr}(Kv + K/v + S) = 0.$$

En utilisant le Théorème 3.4.3, pour tout $v \in \mathbb{F}_{2^n}^*$ tel que

$$\mathrm{Tr}(Kv + K/v + S) = 0$$

il existe deux couples $(v, w)$ et $(v, w+1)$ dans $\mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$ tel que

$$Kv + K/v + S = w + w^2.$$

En choisissant $y = vw$ et en multipliant par $v^2 \neq 0$, on peut déduire que le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ tel que

$$\mathrm{Tr}(\frac{b_1}{b_0\alpha^2}) = 0$$

en divisant par 2, le nombre de couples $(v, y) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$ tel que

$$K(v^3 + v) + Sv^2 = y^2 + vy,$$

qui est égale au nombre de couples $(v, y) \in (\mathbb{F}_{2^n} \times \mathbb{F}_{2^n})^*$ tel que

$$K(v^3 + v) + Sv^2 = y^2 + vy.$$

Cela définit une courbe elliptique (E) de clôture projective $(\overline{E})$ défini par :

$$P(x, y, z) := K(v^3 + vz^2) + Sv^2z + y^2z + vyz.$$

En remplaçant $z$ par 0 on voit que $(\overline{E})$ admet un seul point à l'infini. De plus on remarque que le gradient de $P$ n'admet pas de solutions et donc $(\overline{E})$ est lisse. En utilisant la borne de Hasse-Weil, le nombre des points rationnels de $\mathbb{F}_q$ sur $E$ est au moins $\frac{1}{2}(2^n - 2^{\frac{n}{2}+1} - 1)$. Cela nous permet de conclure.

□

On résume dans le corollaire suivant les résultats des deux corollaires précédents, autrement dit le corollaire suivant nous permet de minorer pour un polynôme $f \in \mathbb{F}_{2^n}[x]$ de degré $m \equiv 0 \pmod 4$, le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels la condition (II) est vérifiée.

**Corollaire 3.5.5.** *Soit $f = \sum_{i=0}^{m} a_{m-i}X^i \in \mathbb{F}_{2^n}[X]$ un polynôme de degré $m$ tel que $m \equiv 0 \pmod 4$, $a_1 \neq 0$ et $n \geq 2$. Soit $L_\alpha(f) = \sum_{i=0}^{d} b_{d-i}X^i$ le polynôme associé de degré $d$. Le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ tel que $\mathrm{Tr}(\frac{b_1}{b_0\alpha^2}) = 0$ est plus grand ou égal à $2^{n-1} - 2^{\frac{n}{2}} - 1$.*

*Démonstration.* En utilisant la Corollaire 3.5.4, et le Corollaire 3.5.5, le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ tel que $\mathrm{Tr}(\frac{b_1}{b_0\alpha^2}) = 0$, est plus grand ou égale à

$$\min\{2^{n-1} - 1, \frac{1}{2}(2^n + 2^{\frac{n}{2}+1} - 1)\} = \min\{2^{n-1} - 1, 2^{n-1} - 2^{\frac{n}{2}} - \frac{1}{2})\} = 2^{n-1} - 2^{\frac{n}{2}} - 1.$$

□

## 3.6 La condition (I.a)

On passe maintenant à la condition (I)(a). Le lemme suivant nous permet de faire le lien entre les polynômes de degré $m \equiv 0 \pmod 4$ et les polynômes de degré $m - 1$.

**Lemme 3.6.1.** *Soient* $m \equiv 0 \pmod 4$ *et* $f(x) = \sum_{k=0}^{m} a_{m-k}x^k \in \mathbb{F}_{2^n}[x]$ *un polynôme de degré* $m$. *Soit* $h(x) = a_0x^m + f(x)$, *un polynôme de degré* $m-1$. *On a*

$$\mathrm{Res}((D_\alpha f)', (D_\alpha f)^{[2]}) = \mathrm{Res}((D_\alpha h)', (D_\alpha h)^{[2]}).$$

*Démonstration.* Comme $m \equiv 0 \pmod 4$, on a

$$(D_\alpha h)'(x) = ma_0x^{m-1} + (D_\alpha f)'(x) = (D_\alpha f)'(x)$$

et

$$(D_\alpha h)^{[2]}(x) = \binom{m}{2} a_0x^{m-2} + (D_\alpha f)^{[2]}(x) = (D_\alpha f)^{[2]}(x).$$

Cela permet de conclure. □

Le Théorème suivant permet de majorer le nombre $\alpha$ dans $\mathbb{F}_{2^n}^*$ pour lesquels les points critiques de $L_\alpha f$ sont dégénérés, et donc il nous permet de traiter la condition (I)(a) pour tout polynôme de degré $m \equiv 0 \pmod 4$.

**Théorème 3.6.2.** *Soient* $m \equiv 0 \pmod 4$ *et* $f(x) = \sum_{k=0}^{m} a_{m-k}x^k \in \mathbb{F}_{2^n}[x]$ *un polynôme de degré* $m$. *Les points critiques de* $L_\alpha f$ *sont non dégénérés sauf pour au plus* $(m-1)(m-4)$ *valeurs de* $\alpha$ *dans* $\mathbb{F}_{2^n}^*$.

*Démonstration.* En utilisant le Lemme 3.3 de [2] et la Proposition 3.2.11, il suffit de démontrer que le polynôme $\mathrm{Res}((D_\alpha f)', (D_\alpha f)^{[2]})$ vu comme un polynôme dans $\mathbb{F}_2[a_0, a_1, \ldots, a_m][\alpha]$, est non nul de degré $(m-1)(m-4)$. Soit $h(x) = a_0x^m + f(x)$, un polynôme de degré $m-1$. En utilisant le Lemme 3.6.1, on a

$$\mathrm{Res}((D_\alpha f)', (D_\alpha f)^{[2]}) = \mathrm{Res}((D_\alpha h)', (D_\alpha h)^{[2]}).$$

En utilisant la Proposition 3.2 de [2], le polynôme $\mathrm{Res}((D_\alpha h)', (D_\alpha h)^{[2]})$ est un polynôme non nul dans $\mathbb{F}_2[a_1, a_2, \ldots, a_m][\alpha]$, de degré $(m-1)(m-1-3) = (m-1)(m-4)$. Nous avons terminé ainsi la démonstration. □

# Chapitre 4

# Les polynômes de petit degré.

Comme on l'a dit précédemment, la méthode appliquée consiste à majorer le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels une au moins des condition $(I.a)$, $(I.b)$ ou $(II)$ n'est pas vérifiée. Pour $m \equiv 0 \pmod 4$, on sait traiter les conditions $(I.a)$ et $(II)$ ( voir Théorème 3.6.2 et Corollaire 3.5.5). Le point le plus difficile dans la démonstration va être de majorer le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels la Condition (I.b) n'est pas vérifiée (c'est a dire pour lesquels le polynôme $L_\alpha f$ n'a pas des valeurs critiques distinctes). Nous y arriverons pour certains polynômes de certains degré $m$.

Dans ce chapitre nous traitons l'uniformité différentielle des polynômes de petit degré. Dans les deux premières sections on va étudier les polynômes de degré 12 et 20. Pour ces petits degrés, les calculs de $\Pi_d L_\alpha f$ restent raisonnables et peuvent être menés à la main. En observant $L_\alpha f$ dans ces deux cas, on remarque qu'il a une forme spéciale. Ça sera le point de départ pour généraliser dans le Chapitre 5 ces résultats sur la famille des polynômes de degré $2^r(2^\ell + 1)$.

Plus tard, dans la troisième section on va traiter le cas des polynômes de degré 16 (et par suite 15) à l'aide d'un logiciel de calcul formel. En fait 16 est le premier nouveau degré multiple de 4 que nous réussissons à traiter et qui n'appartient pas à cette famille. Dans ce cas, nous donnons des conditions algébriques qui garantissent que l'uniformité différentielle soit maximale.

Signalons que le cas des polynômes de petit degré a été étudié par Voloch dans [26]. En utilisant la Remarque 2.1.3, le cas des polynômes de degré 8 peut être déduit de celui des polynômes de degré 7 qui est également traité par Aubry, Herbaut et Voloch dans [2].

## 4.1

## Polynômes de degré 12

Dans cette section on va calculer pour tout entier $n$ suffisamment grand l'uniformité différentielle des polynômes $f(x) = \sum_{k=0}^{12} a_{m-k}x^k \in \mathbb{F}_{2^n}[x]$ de degré 12 avec $a_1 \neq 0$. On commence d'abord par le calcul des coefficients du polynôme associé $L_\alpha f = \sum_{k=0}^{d} b_{d-k}x^k \in \mathbb{F}_{2^n}[x]$.

#### 4.1.0.1 Calculs des $b_i$

En utilisant la Proposition 3.1.4 on a pour tout $k \in \{0\ldots,5\}$ :

$$\sum_{s=max\{0,2k-5\}}^{k} \binom{5-s}{2k-2s}\alpha^{2k-2s}b_s = \sum_{i=10-2k+1}^{12} \binom{i}{10-2k}\alpha^{i-10+2k}a_{12-i}.$$

— Pour $k=0$, on a :

$$\sum_{s=0}^{0} \binom{5-s}{-2s}\alpha^{-2s}b_s = \sum_{i=10+1}^{12} \binom{i}{10}\alpha^{i-10}a_{12-i}.$$

Cela implique que $\binom{5}{0}\alpha^0 b_0 = \binom{11}{10}\alpha^1 a_1 + \binom{12}{10}\alpha^2 a_0 = \alpha a_1$ et donc

$$\underline{b_0 = \alpha a_1}.$$

— Pour $k=1$, on a :

$$\sum_{s=0}^{1} \binom{5-s}{2-2s}\alpha^{2-2s}b_s = \sum_{i=10-2+1}^{12} \binom{i}{8}\alpha^{i-8}a_{12-i}.$$

Alors

$$\binom{5}{2}\alpha^2 b_0 + \binom{4}{0}\alpha^0 b_1 = \binom{9}{8}\alpha^1 a_3 + \binom{10}{8}\alpha^2 a_2 + \binom{11}{8}\alpha^3 a_1 + \binom{12}{8}\alpha^4 a_0.$$

Donc

$$\underline{b_1 = \alpha a_3 + \alpha^2 a_2 + \alpha^3 a_1 + \alpha^4 a_0}.$$

— Pour $k=2$, on a :

$$\sum_{s=0}^{2} \binom{5-s}{4-2s}\alpha^{4-2s}b_s = \sum_{i=7}^{12} \binom{i}{6}\alpha^{i-6}a_{12-i}.$$

Cela implique que

$$\binom{5}{4}\alpha^4 b_0 + \binom{4}{2}\alpha^2 b_1 + \binom{3}{0}\alpha^0 b_2 = \binom{7}{6}\alpha^1 a_5 + \binom{8}{6}\alpha^2 a_4 + \binom{9}{6}\alpha^3 a_3 + \binom{10}{6}\alpha^4 a_2 + \binom{11}{6}\alpha^5 a_1 + \binom{12}{6}\alpha^6 a_0.$$

Donc

$$\alpha^4 b_0 + b_2 = \alpha a_5.$$

Alors

$$\underline{b_2 = \alpha a_5 + \alpha^5 a_1}.$$

— Pour $k = 3$, on a :

$$\sum_{s=1}^{3} \binom{5-s}{6-2s}\alpha^{6-2s} b_s = \sum_{i=5}^{12} \binom{i}{4}\alpha^{i-4} a_{12-i}.$$

Alors $\binom{4}{4}\alpha^4 b_1 + \binom{3}{2}\alpha^2 b_2 + \binom{2}{0}\alpha^0 b_3 = \binom{5}{4}\alpha^1 a_7 + \binom{6}{4}\alpha^2 a_6 + \binom{7}{4}\alpha^3 a_5 + \binom{8}{4}\alpha^4 a_4 + \binom{9}{4}\alpha^5 a_3 + \binom{10}{4}\alpha^6 a_2 + \binom{11}{4}\alpha^7 a_1 + \binom{12}{4}\alpha^8 a_0$. Donc

$$\underline{b_3 = \alpha a_7 + \alpha^2 a_6 + \alpha^3 a_5 + \alpha^6 a_2}.$$

— Pour $k = 4$ on a

$$\underline{b_4 = \alpha a_9 + \alpha^3 a_7 + \alpha^5 a_5 + \alpha^7 a_3 + \alpha^9 a_1}$$

.

— Pour $k = 5$ on a :

$$\underline{b_5 = \alpha a_{11} + \alpha^2 a_{10} + \alpha^3 a_9 + \alpha^4 a_8 + \cdots + \alpha^{12} a_0}.$$

#### 4.1.0.2 Les valeurs critiques de $L_\alpha f$ sont distinctes

Soit

$$f(x) = \sum_{i=0}^{12} a_{12-i} x^i \in \mathbb{F}_{2^n}[x]$$

un polynôme de degré 12 avec $a_1 \neq 0$ et notons

$$L_\alpha f = \sum_{i=0}^{5} b_{d-i} x^i \in \mathbb{F}_{2^n}[x]$$

le polynôme associé de degré plus petit ou égale $d = \frac{12-2}{2} = 5$. Soient $\tau_1$ et $\tau_2$ les deux racines doubles de $(L_\alpha f)'$. Pour majorer le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels les valeurs critiques de $L_\alpha f$ ne sont pas distinctes il suffit de démontrer que $L_\alpha f(\tau_1) - L_\alpha f(\tau_2)$ vu comme un polynôme dans $\mathbb{F}_2[a_0, a_1, \ldots, a_{12}][\alpha]$ est non nul, où :

$$L_\alpha f(\tau_1) - L_\alpha f(\tau_2) = \sum_{k-0}^{5} (b_{5-k}^2)(\tau_1^{2k} + \tau_2^{2k}).$$

Considérons le polynôme symétrique $S_k(x, y) = x^{2k} + y^{2k}$. En utilisant le théorème fondamental des polynômes symétriques, pour tout $0 \leq k \leq d$ il existe un polynôme $Q_k(x, y) \in \mathbb{F}_2[x, y]$ tel que

$$S_k(\tau_1, \tau_2) = Q_k(\sigma_1, \sigma_2),$$

où $\sigma_1$ et $\sigma_2$ représentent les polynômes symétriques élémentaires (i.e $\sigma_1(\tau_1, \tau_2) = \tau_1 + \tau_2$ et $\sigma_2(\tau_1, \tau_2) = \tau_1\tau_2$). Exprimons pour tout $k$, tel que $0 \leq k \leq 5$, $S_k(\tau_1, \tau_2)$ en fonction de $\sigma_1$ et $\sigma_2$.

— Pour $k = 0$, on a : $S_0(\tau_1, \tau_2) = 0$.

— Pour $k = 1$, on a : $S_1(\tau_1, \tau_2) = \tau_1^2 + \tau_2^2 = \sigma_1^2$.

— Pour $k = 2$, on a : $S_2(\tau_1, \tau_2) = \tau_1^4 + \tau_2^4 = \sigma_1^4$.

— Pour $k = 3$, on a :

$$\begin{aligned} S_3(\tau_1, \tau_2) &= \tau_1^6 + \tau_2^6 \\ &= \sigma_1^6 + \tau_1^4\tau_2^2 + \tau_1^2\tau_2^4 \\ &= \sigma_1^6 + \sigma_1^2\sigma_2^2. \end{aligned}$$

— Pour $k = 4$, on a :

$$\begin{aligned} S_4(\tau_1, \tau_2) &= \tau_1^8 + \tau_2^8 \\ &= \sigma_1^8. \end{aligned}$$

— Pour $k = 5$, on a :

$$\begin{aligned} S_5(\tau_1, \tau_2) &= \tau_1^{10} + \tau_2^{10} \\ &= S_3(\tau_1, \tau_2)S_2(\tau_1, \tau_2) + \tau_1^4\tau_2^2 + \tau_2^4\tau_1^2 \\ &= (\sigma_1^6 + \sigma_1^2\sigma_2^2)\sigma_1^4 + \sigma_1^2\sigma_2^2 \\ &= \sigma_1^{10} + \sigma_1^6\sigma_2^2 + \sigma_1^2\sigma_2^2. \end{aligned}$$

Donc,

$$\begin{aligned} L_\alpha f(\tau_1) - L_\alpha f(\tau_2) &= \sum_{k=0}^{5} b_{5-k}^2 S_k(\tau_1, \tau_2) \\ &= b_4^2\sigma_1^2 + b_3^2\sigma_1^4 + b_2^2(\sigma_1^6 + \sigma_1^2\sigma_2^2) + b_1^2\sigma_1^8 \\ &\quad + b_0^2(\sigma_1^{10} + \sigma_1^6 + \sigma_2^2 + \sigma_1^2\sigma_2^2) \end{aligned}$$

Pour démontrer que les valeurs critiques de $L_\alpha f$ sont distinctes il faut et il suffit de démontrer que

$$L_\alpha f(\tau_1) - L_\alpha f(\tau_2) \neq 0.$$

Comme $\tau_1$ et $\tau_2$ sont les racines doubles de $(L_\alpha f)'$, on a :

$$(L_\alpha f)'(x) = b_0x^4 + b_2x^2 + b_4 = b_0(x-\tau_1)^2(x-\tau_2)^2.$$

En utilisant les relations entre les coefficients et les racines du polynôme $(L_\alpha f)'$, on obtient que $\sigma_1^2 = \frac{b_2}{b_0}$ et $\sigma_2^2 = \frac{b_4}{b_0}$. Cela implique que

$$L_\alpha f(\tau_1) - L_\alpha f(\tau_2) \in \mathbb{F}_2[b_0, b_1, b_2, b_3, b_4, \frac{b_2}{b_0}, \frac{b_4}{b_0}]$$

En remplaçant $\sigma_1$ et $\sigma_2$ par leurs valeurs on obtient :

$$L_\alpha f(\tau_1) - L_\alpha f(\tau_2) = \frac{b_4^2b_2}{b_0} + \frac{b_3^2b_2^2}{b_0^2} + b_2^2\left(\frac{b_2^3}{b_0^3} + \frac{b_2}{b_0}\frac{b_4}{b_0}\right) + b_1^2\frac{b_2^4}{b_0^4} + b_0^2\left(\frac{b_2^5}{b_0^5} + \frac{b_2^3}{b_0^3} + \frac{b_4}{b_0} + \frac{b_2b_4}{b_0^2}\right).$$

En remplaçant les $b_i$ par leur expression en fonction des $a_i$ et de $\alpha$, on obtient :

$$\begin{aligned} a_1^4\left(L_\alpha f(\tau_1) - L_\alpha f(\tau_2)\right) &= a_0^2a_1^4\alpha^{24} + a_1^6\alpha^{22} + a_1^4a_3^2\alpha^{18} + a_1^4a_5^2\alpha^{14} \\ &\quad + (a_1^2a_2^2a_5^2 + a_1^4a_6^2)\alpha^{12} + a_1^4a_7^2\alpha^{10} + a_0^2a_5^4\alpha^8 \\ &\quad + (a_2^2a_5^4 + a_1^2a_5^2a_6^2)\alpha^4 + (a_3^2a_5^4 + a_1^2a_5^2a_7^2)\alpha^2. \end{aligned}$$

Après avoir détaillé tous les préliminaires nécessaires, on est prêt maintenant à démontrer le théorème suivant qui majore le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels les valeurs critiques de $L_\alpha f$ ne sont pas distinctes. On donne dans ce théorème la plus petite valeur de $n$ pour laquelle notre méthode s'applique.

**Théorème 4.1.1.** *Soit*

$$f(x) = \sum_{i=0}^{12} a_{12-i}x^i \in \mathbb{F}_{2^n}[x]$$

*un polynôme de degré* 12 *avec* $a_1 \neq 0$ *et notons* $L_\alpha(f)(x) = \sum_{i=0}^{5} b_{5-i}x^i$ *le polynôme associé de degré* 5. *Les valeurs critiques de* $L_\alpha f$ *sont distinctes sauf pour au plus* 24 *valeurs de* $\alpha \in \overline{\mathbb{F}_2}$.

*Démonstration.* Le choix d'un polynôme $f(x) = \sum_{k=0}^{12} a_{m-k}x^k \in \mathbb{F}_{2^n}[x]$ de degré 12 avec $a_1 \neq 0$ revient à choisir des coefficients $a_0, a_1, \ldots, a_{12}$ dans $\mathbb{F}_{2^n}$ avec $a_0 \neq 0$ et $a_1 \neq 0$. cela nous nous permet de considérer $L_\alpha f(\tau_1) - L_\alpha f(\tau_2)$ comme un polynôme de $\mathbb{F}_2[a_0, a_1, \ldots, a_m][\alpha]$ de degré 24 qui admet donc au plus 24 racines dans $\overline{\mathbb{F}_2}$. Comme le coefficient dominant de $L_\alpha f(\tau_1) - L_\alpha f(\tau_2)$ est non nul, alors les valeurs critiques de $L_\alpha f$ sont distinctes sauf pour au plus 24 valeurs de $\alpha \in \overline{\mathbb{F}_2}$. □

#### 4.1.0.3 Résultat sur les polynômes de degré 12.

On est prêt maintenant à démontrer notre résultat sur les polynômes de degré 12.

**Théorème 4.1.2.** *Pour $n > 30$ et pour tout polynôme $f(x) = \sum_{k=0}^{12} a_{m-k}x^k \in \mathbb{F}_{2^n}[x]$ de degré 12 avec $a_1 \neq 0$, on a $\delta(f) = 10$.*

*Démonstration.* En utilisant le Corollaire 3.3.18 ça revient à démontrer qu'il existe un $\alpha \in \mathbb{F}_{2^n}^*$ pour lequel :

(1) $L_\alpha f$ est Morse.

(2) L'équation $x^2 + \alpha x = \frac{b_1}{b_0}$ admet une solution dans $\mathbb{F}_{2^n}$.

L'idée de la preuve est de majorer le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels une au moins des conditions (I.a), (I.b), ou (II) n'est pas vérifiée. En utilisant le Théorème 3.6.2, les points critiques de $L_\alpha f$ sont non dégénérés sauf pour au plus 88 valeurs de $\alpha$ dans $\mathbb{F}_{2^n}^*$. Concernant la condition (I.b), on a par le Théorème 4.1.1 que les valeurs critiques de $L_\alpha f$ sont distinctes sauf pour au plus 24 valeurs de $\alpha$ dans $\mathbb{F}_{2^n}^*$. Il nous reste maintenant de traiter la condition (II). En utilisant le Corollaire 3.5.5, il existe au moins $2^{n-1} - 2^{\frac{n}{2}} - 1$ valeurs de $\alpha$ dans $\mathbb{F}_{2^n}^*$ pour lesquels la condition (II) est vérifiée. En choisissant $n \in \mathbb{N}$ tel que

$$2^{n-1} - 2^{\frac{n}{2}} - 1 > 24 + 88 = 112,$$

et

$$\frac{q}{d_\Omega} - 2\Big((1 + \frac{g_\Omega}{d_\Omega})q^{1/2} + q^{1/4} + 1 + \frac{g_\Omega}{d_\Omega}\Big) \geqslant 1. \tag{4.1}$$

avec :

$q = 2^n$

$d_\Omega = d!2^{d-1} = (120)(16) = 1920$

$g_\Omega \leqslant d!2^{d-1}(d - 3/2) + 1 = d_\Omega(15/2) + 1 = 14401.$

$\frac{g_\Omega}{d_\Omega} \leqslant \frac{14401}{1920} \leq 8,$

on peut appliquer la Proposition 3.3.16 (et par suite le Corollaire 3.3.18) et on garantit ainsi l'existence d'un élément $\alpha$ dans $\mathbb{F}_{2^n}^*$ pour lequel le polynôme $L_\alpha f$ est Morse et l'équation $x^2+\alpha x=\frac{b_1}{b_0}$ admet une solution dans $\mathbb{F}_{2^n}$.

Pour conclure, il suffit de choisir $n\in\mathbb{N}$.tel que

$$2^{n-1}-2^{\frac{n}{2}}>113$$

et

$$\frac{2^n}{1920}-2\Big(9\times 2^{n/2}+2^{n/4}+9\Big)\geqslant 1$$

Cela revient à choisir $n\in\mathbb{N}$ tel que

$$n>9$$

et

$$2^{\frac{n}{2}}\Big(\frac{2^{\frac{n}{2}}}{1920}-\Big(18+\frac{1}{2^{\frac{n}{4}-1}}+\frac{9}{2^{\frac{n}{2}-1}}\Big)\Big)\geqslant 1.$$

Notons $C(n)=2^{\frac{n}{2}}\Big(\frac{2^{\frac{n}{2}}}{1920}-\Big(18+\frac{1}{2^{\frac{n}{4}-1}}+\frac{9}{2^{\frac{n}{2}-1}}\Big)\Big)$. On peut démontrer que $C(n)$ est une fonction croissante en $n$ et que $C(30)<1$ et $C(31)>1$. cela nous permet de conclure. □

## 4.2 Polynômes de degré 20

Dans cette section on va calculer l'uniformité différentielle de certains polynômes $f(x)\in\mathbb{F}_{2^n}[x]$ de degré 20. En utilisant le Corollaire 3.3.18, le Corollaire 3.5.5 et le Théorème 3.6.2 ça revient à majorer le nombre de $\alpha$ dans $\mathbb{F}_{2^n}^*$ pour lesquels les valeurs critiques de $L_\alpha f$ sont distinctes.

#### 4.2.0.1 Calcul des $b_i$

En utilisant la même méthode appliqué dans la sous section 4.1.0.1 on obtient les informations suivantes :

$b_0=a_1\alpha.$

$b_1=a_0\alpha^4+a_1\alpha^3+a_2\alpha^2+a_3\alpha.$

$b_2=a_5\alpha.$

$b_3=a_6\alpha^2+a_7\alpha.$

$b_4=a_1\alpha^9+a_7\alpha^3+a_9\alpha.$

$$b_5 = a_0\alpha^{12} + a_1\alpha^{11} + a_2\alpha^{10} + a_3\alpha^9 + a_8\alpha^4 + a_9\alpha^3 + a_{10}\alpha^2 + a_{11}\alpha.$$
$$b_6 = a_1\alpha^{13} + a_5\alpha^9 + a_9\alpha^5 + a_{13}\alpha.$$
$$b_7 = a_2\alpha^{14} + a_3\alpha^{13} + a_6\alpha^{10} + a_7\alpha^9 + a_{10}\alpha^6 + a_{11}\alpha^5 + a_{14}\alpha^2 + a_{15}\alpha.$$
$$b_8 = a_1\alpha^{17} + a_3\alpha^{15} + a_5\alpha^{13} + a_7\alpha^{11} + a_9\alpha^9 + a_{11}\alpha^7 + a_{13}\alpha^5 + a_{15}\alpha^3 + a_{17}\alpha.$$
$$b_9 = \sum_{k=0}^{19} a_{19-k}\alpha^{k+1}.$$

#### 4.2.0.2 Les valeurs critiques de $L_\alpha f$ sont distinctes.

Le théorème suivant nous permet de majorer le nombre de $\alpha$ pour lesquels les valeurs critiques de $L_\alpha f$ sont distinctes pour tout polynôme $f(x) = \sum_{k=0}^{20} a_{20-k}x^k \in \mathbb{F}_{2^n}[x]$ avec $a_1 \neq 0$.

**Théorème 4.2.1.** *Soit*

$$f(x) = \sum_{i=0}^{20} a_{20-i}x^i \in \mathbb{F}_{2^n}[x]$$

*un polynôme de degré* 20 *avec* $a_1 \neq 0$ *et notons* $L_\alpha(f)(x) = \sum_{i=0}^{5} b_{5-i}x^i$ *le polynôme associé de degré* 9. *Les valeurs critiques de* $L_\alpha f$ *sont distinctes sauf pour au plus* 102 *valeurs de* $\alpha \in \overline{\mathbb{F}_2}$.

*Démonstration.* Pour majorer le nombre de $\alpha$ dans $\mathbb{F}_{2^n}^*$ pour lesquels les valeurs critiques de $L_\alpha f$ sont distinctes, il suffit de démontrer que le polynôme

$$b_0^{12}\Pi_9 L_\alpha f := \prod_{i\neq j} (L_\alpha f(\tau_i) - L_\alpha f(\tau_j))$$

vu comme un polynôme dans $\mathbb{F}_2[a_0, a_1, \ldots, a_{20}][\alpha]$ est non nul, où les $\tau_i$ représentent les racines de $(L_\alpha f)'$. En utilisant les conditions d'homogénéité du Lemme 3.1.7, il suffit de démontrer que le terme $a_0^{12}a_1^{54}\alpha^{102}$ apparaît dans l'expression de $b_0^{54}\Pi_9 L_\alpha f$.Or

$$\begin{aligned}
b_0^{54}\Pi_9 L_\alpha f &= b_0^{54}\prod_{i<j}\sum_{k=0}^{9} b_{9-k}^2(\tau_i^{2k} + \tau_j^{2k}) \\
&= (a_1\alpha)^{54}\prod_{i<j}\left(b_1^2(\tau_i^8 + \tau_j^8) + b_5^2(\tau_i^4 + \tau_j^4) + \ldots\right) \\
&= a_0^{12}a_1^{54}\alpha^{102}\prod_{i<j}\left((\tau_i + \tau_j)^8\left((\tau_i + \tau_j)^8 + \alpha^{16}\right) + \ldots\right) \\
&= a_0^{12}a_1^{54}\alpha^{102}\prod_{i<j}\left((U(a_0, a_1, \ldots, a_m, \alpha) + \ldots\right)
\end{aligned}$$

où l'on note

$$U(a_0, a_1, \ldots, a_m, \alpha) := (\tau_i + \tau_j)^8 \left((\tau_i + \tau_j)^8 + \alpha^{16}\right)$$

Les seuls $b_i$ qui font apparaître $a_0$ dans l'expression de $b_0^{54}\Pi_9 L_\alpha f$ sont $b_1$ et $b_5$. De plus, en utilisant la relation entre les coefficients et les racines de $(L_\alpha f)'$, on a pour tout $i \in \{1,2,3,4\}$, $\tau_i \in \mathbb{F}_2(b_0, b_2, b_4, b_6, b_8)$ et donc $a_0$ n'intervient pas dans $\tau_i^{2k} + \tau_j^{2k}$ pour tout $k \in \{0, \ldots, 9\}$.

Alors pour démontrer que le terme $a_0^{12} a_1^{54} \alpha^{102}$ apparaît bien dans $b_0^{54}\Pi_9 L_\alpha f$, il suffit de démontrer que $U(0,1,0,\ldots,0,1) \neq 0$.

Soit $h(x) = x^{19}$. Pour démontrer que $U(0,1,0,\ldots,0,1) \neq 0$, il faut et il suffit de démontrer que pour tout $i, j \in \{1,2,3,4\}$ et pour tous racines $\tau_i, \tau_j$ de $(L_\alpha x^{19})'$, on a :

$$\tau_i \neq \tau_j$$

et

$$\tau_i \neq \tau_j + 1.$$

Supposons qu'il existe $i, j \in \{1,2,3,4\}$ tel que $\tau_i = \tau_j + 1$. Sans perdre de généralité on peut supposer que $\tau_1 + \tau_2 = 1$. Or

$$L_1(x^{19})' = (1 + x + x^2 + x^4)^2, \tag{4.2}$$

donc $\tau_1 + \tau_2 + \tau_3 + \tau_4 = 0$, cela implique que

$$\tau_3 + \tau_4 = \tau_1 + \tau_2 = 1 \tag{4.3}$$

Comme 1 est une racine de $L_1(x^{19})'$ alors en utilisant l'équation 4.3 , 0 l'est aussi, ce qui est impossible.

Pour déduire il suffit de démontrer que pour tout $i, j \in \{1,2,3,4\}$ tel que $i \neq j$, on a $\tau_i \neq \tau_j$. Supposons qu'il existe $i \neq j \in \{1,2,3,4\}$ tel que $\tau_i = \tau_j$. Sans perdre de généralité, on peut supposer que $\tau_1 = \tau_2$.

En utilisant l'équation 4.2, on obtient que

$$\tau_1 + \tau_2 + \tau_3 + \tau_4 = 0$$

et donc $\tau_3 = \tau_4$. Comme 1 est une racine de $(L_1 x^{19})'$ alors $\tau_1 = \tau_2 = 1$ ou $\tau_3 = \tau_4 = 1$.

En utilisant de nouveau l'équation 4.2, on obtient que

$$\tau_1\tau_2\tau_3\tau_4 = 1. \tag{4.4}$$

et que

$$\tau_1\tau_2 + \tau_1\tau_3 + \tau_1\tau_4 + \tau_2\tau_3 + \tau_2\tau_4 + \tau_3\tau_4 = 1. \tag{4.5}$$

L'équation 4.4 nous donne

$$\tau_1 = \tau_2 = \tau_3 = \tau_4 = 1.$$

En remplaçant les $\tau_i$ par leur valeurs dans l'équation 4.5, on obtient $1 = 0$ ce qui est impossible. Donc pour pour tous $i, j \in \{1, 2, 3, 4\}$ et pour tous racines $\tau_i, \tau_j$ de $(L_\alpha x^{19})'$, on a :

$$\tau_i \neq \tau_j$$

et

$$\tau_i \neq \tau_j + 1.$$

Par suite le terme $a_0^{12} a_1^{54} \alpha^{102}$ apparaît dans $b_0^{54} \Pi_9 L_\alpha f$. Cela nous permet de conclure. □

#### 4.2.0.3 Résultat sur les polynômes de degré 20.

On est prêt maintenant à démontrer notre résultat sur les polynômes de degré 20.

**Théorème 4.2.2.** *Pour $n$ suffisamment grand et pour tout polynôme*

$$f(x) = \sum_{k=0}^{20} a_{m-k} x^k \in \mathbb{F}_{2^n}[x]$$

*de degré 20 avec $a_1 \neq 0$, on a $\delta(f) = 18$.*

*Démonstration.* La démonstration est similaire à celle du Théorème 4.1.2. La seule différence est que la borne supérieure du nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels les valeurs critiques de $L_\alpha f$ ne sont pas distinctes est égale par le Théorème 4.2.1 à 120 dans le cas des polynômes de degré 20. □

## 4.3 Polynômes de degré 16

On termine ce chapitre par les polynômes de degré 16. Comme on a dit précédemment, pour calculer l'uniformité différentielle des polynômes de degré 16 il suffit de majorer le nombre de $\alpha \in \mathbb{F}_{2^N}^*$ pour lesquels la condition $(I.b)$ n'est pas vérifiée.

#### 4.3.0.1 Calcul des $b_i$

En utilisant la même méthode appliqué dans la sous section 4.1.0.1 on obtient les informations suivantes :

$b_0 = a_1\alpha.$

$b_1 = a_2\alpha^2 + a_3\alpha.$

$b_2 = a_3\alpha^3 + a_5\alpha.$

$b_3 = a_4\alpha^4 + a_5\alpha^3 + a_6\alpha^2 + a_7\alpha.$

$b_4 = a_1\alpha^9 + a_5\alpha^5 + a_9\alpha.$

$b_5 = a_2\alpha^{10} + a_3\alpha^9 + a_6\alpha^6 + a_7\alpha^5 + a_{10}\alpha^2 + a_{11}\alpha.$

$b_6 = a_1\alpha^{13} + a_3\alpha^{11} + a_5\alpha^9 + a_7\alpha^7 + a_9\alpha^5 + a_1 1\alpha^3 + a_{13}\alpha.$

$b_7 = \sum_{k=0}^{15} a_{15-k}\alpha^{k+1}.$

#### 4.3.0.2 Les valeurs critiques de $L_\alpha f$ sont distinctes.

Le théorème suivant nous permet pour tout polynôme

$$f(x) = \sum_{k=0}^{16} a_{16-k}x^k \in \mathbb{F}_{2^n}[x]$$

avec $a_1 \neq 0$,

$$a_1^6a_2^6a_3^6 + a_1^8a_2^4a_3^4a_4^2 + a_1^{10}a_2^2a_3^2a_4^4 + a_1^{12}a_4^6 \neq 0.$$

de majorer le nombre de $\alpha$ pour lesquels les valeurs critiques de $L_\alpha f$ ne sont pas distinctes.

**Théorème 4.3.1.** *Soit*

$$f(x) = \sum_{i=0}^{16} a_{16-i}x^i \in \mathbb{F}_{2^n}[x]$$

*un polynôme de degré* 16 *avec* $a_1 \neq 0$, *et*

$$a_1^6a_2^6a_3^6 + a_1^8a_2^4a_3^4a_4^2 + a_1^{10}a_2^2a_3^2a_4^4 + a_1^{12}a_4^6 \neq 0.$$

*Notons* $L_\alpha(f)(x) = \sum_{i=0}^{7} b_{7-i}x^i$ *le polynôme associé de degré* 7. *Les valeurs critiques de* $L_\alpha f$ *sont distinctes sauf pour au plus* 72 *valeurs de* $\alpha \in \overline{\mathbb{F}_2}$.

*Démonstration.* Pour majorer le nombre de $\alpha$ dans $\mathbb{F}_{2^n}^*$ pour lesquels les valeurs critiques de $L_\alpha f$ sont distinctes, il suffit de démontrer que le polynôme

$$b_0^{12}\Pi_7 L_\alpha f := \prod_{i\neq j}(L_\alpha f(\tau_i) - L_\alpha f(\tau_j))$$

vu comme un polynôme dans $\mathbb{F}_2[a_0, a_1, \ldots, a_{16}][\alpha]$ est non nul, où les $\tau_i$ représentent les racines de $(L_\alpha f)'$. On a

$$\Pi_7 L_\alpha f = \sum_{k-0}^{7}(b_{7-k}^2)(\tau_1^{2k} + \tau_2^{2k}).$$

Considérons pour tout $0 \leq k \leq 7$ le polynôme symétrique

$$S_k(x, y) = x^{2k} + y^{2k}.$$

En utilisant le théorème fondamental des polynômes symétriques, pour tout $0 \leq k \leq 7$ il existe un polynôme $Q_k(x, y, z) \in \mathbb{F}_2[x, y, z]$ tel que pour tout $i, j \in \{1, 2, 3\}$ :

$$S_k(\tau_i, \tau_j) = Q_k(\sigma_1, \sigma_2, \sigma_3),$$

où $\sigma_1$, $\sigma_2$ et $\sigma_3$ représentent les polynômes symétriques élémentaires (i.e $\sigma_1(\tau_1, \tau_2, \tau_3) = \tau_1 + \tau_2 + \tau_3$, $\sigma_2(\tau_1, \tau_2, \tau_3) = \tau_1\tau_2 + \tau_1\tau_3 + \tau_2\tau_3$ et $\sigma_3(\tau_1, \tau_2, \tau_3) = \tau_1\tau_2\tau_3$). En utilisant le logiciel du calcul formel **Maple**, on peut démontrer que $a_1^{12}\Pi_7 L_\alpha f$ est un polynôme dans $\mathbb{F}_2[a_0, a_1, \ldots, a_{16}][\alpha]$ de degré 72, de coefficient dominant :

$$a_1^6 a_2^6 a_3^6 + a_1^8 a_2^4 a_3^4 a_4^2 + a_1^{10} a_2^2 a_3^2 a_4^4 + a_1^{12} a_4^6.$$

Fixons un polynôme

$$f(x) = \sum_{i=0}^{16} a_{16-i}x^i \in \mathbb{F}_{2^n}[x]$$

de degré 16 avec $a_1 \neq 0$

$$a_1^6 a_2^6 a_3^6 + a_1^8 a_2^4 a_3^4 a_4^2 + a_1^{10} a_2^2 a_3^2 a_4^4 + a_1^{12} a_4^6 \neq 0.$$

Les valeurs critiques de $L_\alpha f$ sont distinctes sauf pour au plus 72 valeurs de $\alpha \in \mathbb{F}_{2^n}^*$. □

#### 4.3.0.3 Résultat sur les polynômes de degré 16.

On est prêt maintenant à démontrer notre résultat sur les polynômes de degré 16.

**Théorème 4.3.2.** *Pour $n$ suffisamment grand et pour tout polynôme*

$$f(x) = \sum_{k=0}^{16} a_{16-k} x^k \in \mathbb{F}_{2^n}[x]$$

*de degré* 16 *tel que* $a_1 \neq 0$ *et*

$$a_1^6 a_2^6 a_3^6 + a_1^8 a_2^4 a_3^4 a_4^2 + a_1^{10} a_2^2 a_3^2 a_4^4 + a_1^{12} a_4^6 \neq 0,$$

*on a* $\delta(f) = 14$.

*Démonstration.* La démonstration est similaire à celle du Théorème 4.1.2. La seule différence est que la borne supérieure du nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels les valeurs critiques de $L_\alpha f$ ne sont pas distinctes est égale par le Théorème 4.3.1 à 72 dans le cas des polynômes de degré 20. □

En utilisant la Remarque 2.1.3, on tire le résultat suivant sur les polynômes de degré 15.

**Corollaire 4.3.3.** *Pour $n$ suffisamment grand et pour tout polynôme*

$$f(x) = \sum_{k=0}^{15} a_{15-k} x^k \in \mathbb{F}_{2^n}[x]$$

*de degré* 15 *tel que* $a_0 \neq 0$ *et*

$$a_0^6 a_1^6 a_2^6 + a_0^8 a_1^4 a_2^4 a_3^2 + a_0^{10} a_1^2 a_2^2 a_3^4 + a_1^{12} a_4^6 \neq 0,$$

*on a* $\delta(f) = 14$.

# Chapitre 5

# Le théorème principal

Dans ce chapitre on va démontrer le résultat principal de la thèse. Comme on l'a vu dans les chapitres précédents, pour montrer que l'uniformité différentielle d'un polynôme est maximale, il suffit de trouver un élément $\alpha$ non nul, pour lequel les conditions (I.a), (I.b) et (II) sont vérifiées simultanément. Les conditions (I.a) et (II) sont déjà traitées dans le Chapitre 3.

On va étudier dans ce chapitre la condition (I.b) sur les polynômes de degré $2^r(2^\ell+1)$, cela va nous permettre de démontrer notre résultat. Pour cela, on introduit la définition des polynômes "Trace" $P_k$ et on étudie leurs propriétés algébriques.

On verra que la méthode utilisée pour étudier la condition (II) est en fait inspirée de celle utilisée pour les polynômes de degré 12 ou 20 dans le Chapitre 4.

On commence d'abord par l'étude de l'expression du polynôme $L_\alpha f$ et des propriétés élémentaires du polynôme $P_k$. Ensuite, on traite les racines du polynôme $(L_\alpha(x^{m-1}))'$ et on termine par la démonstration du Théorème 5.3.1 en distinguant trois cas en fonctions du pgcd de $\ell$ et de $r$. Dans le cas où ce pgcd est plus grand ou égal à 3, nous expliquons pourquoi notre méthode ne s'applique pas.

Enfin, expliquons pourquoi nous arrivons à conclure la preuve dans le cas des polynômes de degré $m = 2^r(2^\ell + 1)$. Le point clé est la forme spéciale du polynôme $L_\alpha f$. Plus précisément, si $f(x) = a_0x^m + \ldots$, nous arrivons à déterminer dans quelle coefficients $b_i$ de $L_\alpha f = b_0x^d + \ldots$ apparaît $a_0$. Ce sera l'objet du Lemme 5.1.1. Puis l'étude des valeurs critiques distinctes fera apparaître les polynômes "Trace" $P_k$, dont les propriétés spéciales nous permettront de conclure.

## 5.1

## Expression de $L_\alpha f$

Dans cette section on va donner pour tout $m = 2^r(2^\ell + 1)$ tel que $\ell \geq 1$, $r \geq 2$ et pour tout polynôme $f(x) = \sum_{k=0}^{m} a_{m-k}x^k$ de degré $m$, des informations sur l'expression de $L_\alpha f$. Le lemme suivant nous donne des informations indispensables sur le coefficient $a_0$.

**Lemme 5.1.1.** *Soit $m = 2^r(2^\ell + 1)$ tel que $\ell \geq 1$, $r \geq 2$. On a*

$$(L_1(x^m))(x) = 1 + \sum_{k=0}^{\ell-1} x^{2^{r+k}}.$$

*(En conséquence, si $f(x) = \sum_{k=0}^{m} a_{m-k}x^k \in \mathbb{F}_{2^n}[x]$ et $L_\alpha f(x) = \sum_{k=0}^{d} b_{d-k}x^k$, alors $a_0$ apparaît seulement dans les coefficients : $b_d, b_{d-2^r}, b_{d-2^{r+1}}, \ldots, b_{d-2^{r+\ell-1}}$.)*

*Démonstration.* Soit $g(x) = 1 + \sum_{k=0}^{\ell-1} x^{2^{r+k}}$. Il suffit de démontrer que

$$g(x^2 + x) = x^m + (x + 1)^m.$$

On a :

$$\begin{aligned} g(x^2 + x) &= 1 + \sum_{k=0}^{\ell-1} (x + x^2)^{2^{r+k}} \\ &= 1 + \sum_{k=0}^{\ell-1} (x^{2^{r+k}} + x^{2^{r+k+1}}) \\ &= 1 + x^{2^r} + x^{2^{r+l}}. \end{aligned}$$

Or $x^m + (x + 1)^m = x^{2^r+2^{r+\ell}} + (x + 1)^{2^r+2^{r+\ell}} = 1 + x^{2^r} + x^{2^{r+\ell}}$, cela nous permet de conclure. □

Dans ce qui suit on va utiliser la notation suivante :

**Notation 5.1.2.** Soit $k \geq 1$, on définit le polynôme $P_k(x)$ par

$$P_k(x) = x + x^2 + x^4 + x^8 + \ldots + x^{2^{k-1}}.$$

**Remarque 5.1.3.** Soit $k \geq 1$, pour tout $u \in \mathbb{F}_{2^k}$, on a :

$$P_k(u) = \mathrm{Tr}_{\mathbb{F}_{2^k}/\mathbb{F}_2}(u).$$

En utilisant les propriétés de la Trace et des calculs élémentaires, on dégage les informations suivantes :

**Remarque 5.1.4.** Pour tout $k \geq 1$, on a :

(1) $P_k$ est linéaire.

(2) Pour tout $s \geq 1$, $P_k(x^{2^s}) = P_k^{2^s}(x)$.

(3) $P_k(x) = P_{k-1}(x) + x^{2^{k-1}}$.

(4) $P_k(1) = 0$ si et seulement si $k \equiv 0 \pmod 2$.

Nous signalons aussi que l'application $k \mapsto P_k$ des propriétés algébriques remarquables par rapport à la somme et au produit. La condition (1) ci-dessous peut par exemple se retrouver dans l'article [6].

**Lemme 5.1.5.** *Soient $k$ et $s$ deux entiers non nuls. On a :*

*(1)* $P_{k+s}(x) = P_k(x) + P_s^{2^k}(x)$.

*(2)* $P_{ks}(x) = \sum_{i=0}^{s-1} P_k^{2^{ik}}(x)$,

*Démonstration.* (1) On va procéder par récurrence sur $s$. L'égalité est vérifiée si $s = 1$. Supposons que

$$P_{k+s}(x) = P_k(x) + P_s^{2^k}(x).$$

et montrons que :

$$P_{k+s+1}(x) = P_k(x) + P_{s+1}^{2^k}(x).$$

Or,

$$P_{k+s+1}(x) = P_{k+s}(x) + P_1(x)^{2^{k+s}}.$$

En utilisant l'hypothèse de récurrence on a :

$$\begin{aligned} P_{k+s+1}(x) &= P_k(x) + P_s^{2^k}(x) + P_1(x)^{2^{k+s}} \\ &= P_k(x) + (P_s(x) + P_1(x)^{2^s})^{2^k} \\ &= P_k(x) + P_{s+1}^{2^k}(x). \end{aligned}$$

(2) On va procéder par récurrence sur $s$. L'égalité est vérifiée si $s = 1$. Supposons que

$$P_{ks}(x) = \sum_{i=0}^{s-1} P_k^{2^{ik}}(x),$$

et montrons que

$$P_{k(s+1)}(x) = \sum_{i=0}^{s} P_k^{2^{ik}}(x).$$

Or en utilisant le Lemme 5.1.5

$$\begin{aligned} P_{k(s+1)}(x) &= P_{ks}(x) + P_k(x)^{2^{ks}} \\ &= \sum_{i=0}^{s-1} P_k^{2^{ik}}(x) + P_k(x)^{2^{ks}} \\ &= \sum_{i=0}^{s} P_k^{2^{ik}}(x). \end{aligned}$$

Cela nous permet de conclure.

□

Démontrons maintenant un résultat de divisibilité sur les polynômes $P_k$.

**Lemme 5.1.6.** *Si $k$ et $s$ sont deux entiers tel que $k$ divise $s$, alors $P_k$ divise $P_s$.*

*Démonstration.* Soit $k'$ un entier tel que $s = kk'$. On a par le lemme **??**

$$P_s(x) = P_{kk'}(x) = \sum_{i=0}^{k'-1} P_k^{2^{ik}}(x),$$

donc $P_k$ divise $P_s$. □

Le lemme suivant va nous servir à démontrer le Lemme 5.2.9, qui à son tour va nous aider à démontrer notre résultat dans le cas où $pgcd(\ell, r) = 2$.

**Lemme 5.1.7.** *Soit $u \in \mathbb{F}_4$ tel que $u \neq 0$ et $u \neq 1$ et soit $k$ un entier pair. On a*

$$P_k(u) = 0 \iff k \equiv 0 \pmod 4.$$

*Démonstration.* Comme $u \neq 0$ et $u \neq 1$ alors $u + u^2 = 1$. Or

$$\begin{aligned} P_k(u) &= u + u^2 + u^4 + u^8 + \cdots + u^{2^{k-1}} \\ &= u + u^2 + (u+u^2)^4 + (u+u^2)^{16} + \cdots + (u+u^2)^{2^{k-2}} \\ &= \sum_{i=0}^{\frac{k}{2}-1} (u+u^2)^{2^{2i}} \end{aligned}$$

Donc

$$P_k(u) = \sum_{i=0}^{\frac{k}{2}-1} 1 = \frac{k}{2}.$$

Cela nous permet de conclure. □

On donne maintenant une condition suffisante qui nous permet de majorer le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels les valeurs critiques de $L_\alpha f$ sont distinctes. Nous utilisons de façon importante le Lemme 3.1.7 qui à la fois donne un résultat d'homogénéité et permet de contrôler le degré du polynôme $b_0^N \Pi_d L_\alpha f$.

**Proposition 5.1.8.** *Soit $m = 2^r(2^\ell + 1)$ tel que $\ell \geq 1$, $r \geq 2$ et soit $f(x) = \sum_{k=0}^m a_{m-k}x^k \in \mathbb{F}_{2^n}[x]$ de degré $m$ tel que $a_1 \neq 0$. Soit $L_\alpha f(x) = \sum_{k=0}^d b_{d-k}x^k$ le polynôme associé de degré $d$. Si pour tous racines distinctes $\tau_i, \tau_j$ de $(L_1(x^{m-1}))'$, $P_\ell(\tau_i + \tau_j) \neq 0$ alors $L_\alpha f$ a des valeurs critiques distinctes sauf pour au plus $(5d+4)\binom{(d-1)/2}{2}$ valeurs de $\alpha \in \mathbb{F}_{2^n}^*$.*

*Démonstration.* En utilisant la Proposition 3.2.11, il suffit de démontrer que $b_0^N \Pi_d L_\alpha f$ vu comme un polynôme dans $\mathbb{F}_2[a_0, a_1, \ldots, a_m][\alpha]$ $\alpha$ est non nul de degré $(5d+4)\binom{(d-1)/2}{2}$. En utilisant les conditions d'homogénéité du Lemme 3.1.7, il suffit de démontrer que le terme $a_0^{2e}a_1^{de}\alpha^{(5d+4)e}$ apparaît dans l'expression de $b_0^N \Pi_d L_\alpha f$. Mais

$$\begin{aligned}
b_0^N \Pi_d(L_\alpha f) &= (a_1\alpha)^N \prod_{i<j} \left( \sum_{k=0}^{d} b_{d-k}^2 (\tau_i^{2k} + \tau_j^{2k}) \right) \\
&= (a_1\alpha)^N \prod_{i<j} \left( \sum_{k=0}^{\ell-1} b_{d-2^{r+k}}^2 (\tau_i + \tau_j)^{2^{r+k}} + \cdots \right) \\
&= (a_1\alpha)^N \prod_{i<j} \left( \sum_{k=0}^{\ell-1} b_{d-2^{r+k}}^2 (\tau_i + \tau_j)^{2^{r+k}} \right) + \cdots \\
&= a_0^{2e} a_1^N \alpha^N \prod_{i<j} \left( \sum_{k=0}^{\ell-1} (\alpha^{m-2^{r+k+1}})^2 (\tau_i + \tau_j)^{2^{r+k}} \right) + \cdots
\end{aligned}$$

où les $\tau_i$ sont les racines de $(L_\alpha f)'$. Comme

$$(L_\alpha f)'(x) = b_0 x^{d-1} + b_2 x^{d-3} + b_4 x^{d-5} + \ldots + b_{d-1}$$

et en utilisant les relations coefficients racines et le Lemme 5.1.1, le seul terme qui contient $a_0$ dans l'expression de $b_0^N \Pi_d L_\alpha f$ est

$$a_0^{2e} a_1^N \alpha^N \prod_{i<j} \left( \sum_{k=0}^{\ell-1} (\alpha^{m-2^{r+k+1}})^2 (\tau_i + \tau_j)^{2^{r+k}} \right).$$

Notons

$$S(a_1, a_2, \ldots, a_m, \alpha) = \sum_{k=0}^{\ell-1} (\alpha^{m-2^{r+k+1}})^2 (\tau_i + \tau_j)^{2^{r+k}}.$$

Pour démontrer que le terme $a_0^{2e} a_1^{de} \alpha^{(5d+4)e}$ apparaît dans l'expression de $b_0^N \Pi_d L_\alpha f$, il suffit de démontrer que

$$S(1, 0, \ldots, 1) = (\sum_{k=0}^{\ell-1} (\tau_i + \tau_j)^{2^k})^{2^r}$$

est non nul, ce qui est équivalent à étudier la nullité de $P_\ell(\tau_i + \tau_j)$ où les $\tau_i$ représentent les racines de $(L_1(x^{m-1}))'$.

□

## 5.2
## Les racines de $(L_1(x^{m-1}))'$

Dans cette section, on va étudier la nullité de $P_\ell(\tau_i + \tau_j)$ lorsque $\tau_i \neq \tau_j$, suivant les valeurs de $\ell$ et $r$, où les $\tau_k$ sont les racines de $L_1(x^{m-1})'$. Le lemme suivant nous permet de savoir pour tout polynôme $f(x) = \sum_{k=0}^{m} a_{m-k} x^k$ de degré $m = 2^r(2^\ell + 1)$ dans quels coefficients $b_k$ de $L_\alpha f = \sum_{k=0}^{d} b_{d-k} x^k$ l'indéterminée $a_1$ apparaît.

**Lemme 5.2.1.** *Considérons $m = 2^r(2^\ell + 1)$ avec $\ell \geq 1$, $r \geq 2$. On a*

$$(L_1(x^{m-1}))(x) = x^{2^r-1} + \left(1 + x^{2^r} + x^{2^{r+1}} + x^{2^{r+2}} + \ldots + x^{2^{r+\ell-1}}\right) \sum_{k=0}^{r-1} x^{2^k-1}.$$

*Démonstration.* Notons

$$g(x) = x^{2^r-1} + \left(1 + x^{2^r} + x^{2^{r+1}} + x^{2^{r+2}} + \ldots + x^{2^{r+\ell-1}}\right) \sum_{k=0}^{r-1} x^{2^k-1}.$$

Il suffit de montrer que

$$g(x^2 + x) = x^{m-1} + (x+1)^{m-1}.$$

On a

$$\begin{aligned}
g(x^2+x) &= (x+x^2)^{2^r-1} + \left(1+(x+x^2)^{2^r}+\ldots+(x+x^2)^{2^{r+\ell-1}}\right)\sum_{k=0}^{r-1}\frac{(x+x^2)^{2^k}}{x^2+x} \\
&= \frac{x^{2^r}+x^{2^{r+1}}}{x+x^2} + \left(1+x^{2^r}+x^{2^{r+\ell}}\right)\sum_{k=0}^{r-1}\frac{(x^{2^k}+x^{2^{k+1}})}{x^2+x} \\
&= \frac{1}{x+x^2}\left(x^{2^r}+x^{2^{r+1}}+(1+x^{2^r}+x^{2^{r+\ell}})(x+x^{2^r})\right) \\
&= \frac{1}{x+x^2}\left(x^{2^r}+x^{2^{r+1}}+x+x^{2^r}+x^{2^r+1}+x^{2^{r+1}}+x^{2^{r+\ell}+1}+x^{2^{r+\ell}+2^r}\right) \\
&= \frac{1}{x+x^2}\left(x+x^{2^r+1}+x^{2^{r+\ell}+1}+x^{2^{r+\ell}+2^r}\right)
\end{aligned}$$

Par ailleurs on a :

$$\begin{aligned}
x^{2^r+2^{r+\ell}-1}+(x+1)^{2^r+2^{r+\ell}-1} &= \frac{x^{2^r+2^{r+\ell}}}{x}+\frac{(x+1)^{2^r+2^{r+\ell}}}{x+1} \\
&= \frac{x^{2^r+2^{r+\ell}+1}+x^{2^r+2^{r+\ell}}+x(x+1)^{2^r+2^{r+\ell}}}{x(x+1)} \\
&= \frac{x^{2^r+2^{r+\ell}+1}+x^{2^r+2^{r+\ell}}+x(x^{2^r+2^{r+\ell}}+x^{2^r}+x^{2^{r+\ell}}+1)}{x(x+1)} \\
&= \frac{x+x^{2^r+1}+x^{2^{r+\ell}+1}+x^{2^r+2^{r+\ell}}}{x+x^2} \\
&= g(x^2+x).
\end{aligned}$$

□

Introduisons maintenant, le polynôme $h(x)$, qui va nous servir à faire pour l'étude des racines de $(L_1(x^{m-1})'$ à faire apparaître des polynômes "Trace" et à travailler dans l'anneau des polynômes ( et non dans le corps des fractions rationnelles) grâce à la multiplication par $x^2$.

**Proposition 5.2.2.** *Soit $m = 2^r(2^\ell+1)$ tel que $\ell \geq 1$, $r \geq 2$ et soit $h(x) = x^2(L_1(x^{m-1}))'$. On a*

$$h(x) = P_r^2(x) + P_\ell^{2^r}(x)P_{r-1}^2(x).$$

*Démonstration.* On a

$$\begin{aligned} h(x) &= x^2(L_1(x^{m-1}))' \\ &= x^2\left(x^{2^r-2} + (1 + x^{2^r} + x^{2^{r+1}} + x^{2^{r+2}} + \ldots + x^{2^{r+\ell-1}})\sum_{k=1}^{r-1} x^{2^k-2}\right) \\ &= x^{2^r} + (1 + P_\ell^{2^r}(x))P_{r-1}^2(x) \\ &= x^{2^r} + P_{r-1}^2(x) + P_\ell^{2^r}(x)P_{r-1}^2(x) \\ &= P_r^2(x) + P_{r-1}^2(x)P_\ell(x)^{2^r}. \end{aligned}$$

□

On donne maintenant l'expression explicite des racines de $L_1'(x^{m-1})$ en termes des racines $d-$ième de l'unité.

**Proposition 5.2.3.** *Considérons un entier $m = 2^r(2^\ell + 1)$ tel que $\ell \geq 1$ et $r \geq 2$. Les $\frac{d-1}{2}$ racines de $L_1'(x^{m-1})$ sont de la forme*

$$\tau_i = \frac{1}{1+\theta_i} + \frac{1}{1+\theta_i^2}$$

*où l'on considère un choix de $\frac{d-1}{2}$ racines $\theta_i$ telles que $\theta_i^d = 1$, $\theta_i \neq 1$ et $\theta i \theta j \neq 1$, pour tout $i \neq j$.*

*Démonstration.* On a :

$$D_1'(x^{m-1}) = L_1' \circ T_1$$

où l'on rappelle que $T_1(x) = x^2 + x$. Notons $u_i$ les racines de $D_1'(x^{m-1})$, on a

$$u_i^{m-2} + (u_i + 1)^{m-2} = 0,$$

donc

$$\left(\frac{u_i}{u_i+1}\right)^{m-2} = 1,$$

Alors

$$\left(\frac{u_i}{u_i+1}\right)^{d} = 1.$$

Prenons $\theta_i = \frac{u_i}{u_i+1}$. On a

$$u_i = \frac{\theta_i}{1+\theta_i}.$$

On conclut en utilisant que

$$T_1(u_i) = \tau_i$$

et que

$$T_1(u_i) = T_1(u_j) \iff \theta_i = \theta_j \text{ ou } \theta_i\theta_j = 1.$$

□

La proposition suivante est le point clé de la démonstration des Propositions 5.2.7 et 5.2.11.

**Proposition 5.2.4.** *Soit $m = 2^r(2^\ell + 1)$ tel que $\ell \geq 1$, $r \geq 2$ et soit $\tau_i$ une racine de $L_1'(x^{m-1})$. On a*

$$P_\ell(\tau_i + \tau_i^{2^\ell}) = \frac{1}{1+\theta_i} + \frac{1}{1+\theta_i^{2^{2\ell}}}.$$

*Démonstration.* On a

$$\begin{aligned}
P_\ell(\tau_i + \tau_i^{2^\ell}) &= P_\ell(\tau_i) + P_\ell(\tau_i)^{2^l} \\
&= \tau_i + \cdots + \tau_i^{2^{\ell-1}} + \tau_i^{2^\ell} + \cdots + \tau_i^{2^{2\ell-1}} \\
&= \frac{1}{1+\theta_i} + \frac{1}{1+\theta_i^2} + \frac{1}{1+\theta_i^2} + \frac{1}{1+\theta_i^4} + \cdots + \frac{1}{1+\theta_i^{2^{\ell-1}}} + \frac{1}{1+\theta_i^{2^\ell}} + \\
&+ \frac{1}{1+\theta_i^{2^\ell}} + \cdots + \frac{1}{1+\theta_i^{2^{2\ell-1}}} + \frac{1}{1+\theta_i^{2^{2\ell}}} \\
&= \frac{1}{1+\theta_i} + \frac{1}{1+\theta_i^{2^{2\ell}}}.
\end{aligned}$$

□

La proposition suivante joue un rôle important dans l'étude des racines de $L_1(x^{m-1})'$. On va se servir de l'équation 5.1 pour avoir des informations sur les $\tau_i$.

**Proposition 5.2.5.** *Considérons les deux entiers $\ell \geq 1$ et $r \geq 2$ et soit $m = 2^r(2^\ell + 1)$. Pour toutes racines distinctes $\tau_i$ et $\tau_j$ de $h$, si $P_\ell(\tau_i + \tau_j) = 0$, alors*

$$P_\ell(\tau_i)^{2^r} = \frac{P_r(\tau_i)^2}{P_{r-1}(\tau_i)^2} = \frac{P_r(\tau_i + \tau_j)^2}{P_{r-1}(\tau_i + \tau_j)^2} = \frac{P_r(\tau_j)^2}{P_{r-1}(\tau_j)^2} = P_\ell(\tau_j)^{2^r} \tag{5.1}$$

*Démonstration.* On a $h(\tau_i) = 0$, donc par la Proposition 5.2.2 on a $P_\ell(\tau_i)^{2^r} = \frac{P_r^2(\tau_i)}{P_{r-1}^2(\tau_i)}$ et donc on a la première égalité. De la même manière on obtient la dernière égalité. Or

$$0 = h(\tau_i) + h(\tau_j) = P_r^2(\tau_i) + P_\ell^{2^r}(\tau_i)P_{r-1}^2(\tau_i) + P_r^2(\tau_j) + P_\ell^{2^r}(\tau_j)P_{r-1}^2(\tau_j).$$

Comme $P_\ell(\tau_i) = P_\ell(\tau_j)$, alors

$$P_r^2(\tau_i) + P_\ell^{2^r}(\tau_i)P_{r-1}^2(\tau_i) + P_r^2(\tau_j) + P_\ell^{2^r}(\tau_i)P_{r-1}^2(\tau_j) = 0$$

et donc

$$P_r^2(\tau_i + \tau_j) + P_\ell^{2^r}(\tau_i)P_{r-1}^2(\tau_i + \tau_j) = 0.$$

Cela implique la deuxième égalité. □

### 5.2.1 Cas $\mathrm{pgcd}(\ell, r) = 1$ :

Dans cette section on va supposer que $\mathrm{pgcd}(\ell, r) = 1$. Le lemme suivant est fondamental dans la démonstration dans le cas $\mathrm{pgcd}(\ell, r) = 1$. Il va nous servir en particulier à démontrer la Proposition 5.2.7.

**Lemme 5.2.6.** *Soit $\ell$ et $r$ deux entiers premier entre eux. Si on note $d = 2^{r-1}(2^\ell + 1) - 1$ et $d' = 2^{2\ell} - 1$ alors on a $\mathrm{pgcd}(d, d') = 1$,*

*Démonstration.* On remarque que $d' = (2^\ell + 1)(2^\ell - 1)$. Soit $t$ un diviseur commun à $d$ et $d'$. Puisque $t$ divise $d'$, on peut écrire $t$ sous la forme : $t = ab$ avec $a$ un diviseur de $2^\ell + 1$ et $b$ un diviseur de $2^\ell - 1$. On a donc : $2^\ell \equiv -1 \pmod{a}$ et $2^\ell \equiv 1 \pmod{b}$. On en déduit que

(1) $d \equiv -1 \pmod{a}$ et

(2) $d \equiv 2^r - 1 \pmod{b}$.

Or $t = ab$ divise $d$ donc $d \equiv 0 \pmod{ab}$ cela entraîne que $d \equiv 0 \pmod{a}$ et $d \equiv 0 \pmod{b}$.

(i) $0 \equiv -1 \pmod{a}$ et donc $a = 1$ et

(ii) $2^r \equiv 1 \pmod{b}$.

Ainsi l'ordre de 2 dans $(\mathbb{Z}/b\mathbb{Z})^*$ divise $\ell$ et $r$. Donc $\mathrm{ordre}(2) = 1$ dans $(\mathbb{Z}/b\mathbb{Z})^*$. Cela implique que $2 \equiv 1 \pmod{b}$ et donc $b = 1$. □

Terminons maintenant avec la proposition suivante qui va nous servir à démontrer le Théorème 5.3.1.

**Proposition 5.2.7.** *Considérons les deux entiers $\ell \geq 1$ et $r \geq 2$ avec $\mathrm{pgcd}(\ell, r) = 1$ et soit $m = 2^r(2^\ell + 1)$. Soit $(i, j) \in \{1, \ldots, (d-1)/2\}^2$ tel que $i \neq j$. Pour toutes racines distinctes de $h$, $\tau_i$ et $\tau_j$, on a*

$$P_\ell(\tau_i + \tau_j) \neq 0.$$

*Démonstration.* Par l'absurde supposons que $P_\ell(\tau_i+\tau_j)=0$ et donc que $\tau_i+\tau_j \in \mathbb{F}_{2^\ell}$. Alors $\frac{P_r(\tau_i+\tau_j)}{P_{r-1}(\tau_i+\tau_j)} \in \mathbb{F}_{2^\ell}$. Cela implique par la Proposition 5.2.5 que $P_\ell(\tau_i)^{2^r} \in \mathbb{F}_{2^\ell}$, et donc $P_\ell(\tau_i) \in \mathbb{F}_{2^\ell}$. On a par la linéarité de $P_\ell$ que $P_\ell(\tau_i+\tau_i^{2^\ell})=0$. En utilisant la Proposition 5.2.4, on obtient que

$$\frac{1}{1+\theta_i} = \frac{1}{1+\theta_i^{2^{2\ell}}}$$

et donc $\theta_i = \theta_i^{2^{2\ell}}$. Donc $\theta_i^{2^{2\ell}-1}=1$, or $\theta_i^d=1$, alors $\theta_i^{\mathrm{pgcd}(2^{2\ell}-1,d)}=1$. Cela implique par le Lemme 5.2.6 que $\theta_i^1=1$ et donc $\theta_i=1$. Cela nous permet de conclure. □

### 5.2.2 Cas $\mathrm{pgcd}(\ell, r) = 2$ :

On passe maintenant au deuxième cas. On va supposer dans cette section que $\mathrm{pgcd}(\ell,r)=2$. On remarque d'abord que dans ce cas, contrairement au cas précèdent 1 est bien une racine de $h(x)$.

**Remarque 5.2.8.** Considérons les deux entiers $\ell \geq 1$ et $r \geq 2$ avec $\mathrm{pgcd}(\ell,r)=2$ et soit $m=2^r(2^\ell+1)$. Comme

$$h(1) = P_r^2(1) + P_\ell^{2^r}(1)P_{r-1}^2(1) = 0 + 0 \times 1 = 0,$$

les racines de $L_1'(x^{m-1})$ sont de la forme : $\tau_1, \tau_2, \ldots, \tau_{(d-1)/2}$ avec $\tau_1=1$.

Le lemme suivant montre que les racines de $L_1'(x^{m-1})$ n'appartient pas à $\mathbb{F}_{2^\ell}$.

**Lemme 5.2.9.** *Soit $i \in \{1, \ldots, \frac{d-1}{2}\}$. Si $\tau_i \neq 1$ alors $\tau_i \notin \mathbb{F}_{2^\ell}$.*

*Démonstration.* Supposons que $\tau_i \in \mathbb{F}_{2^\ell}$. On a $P_\ell(\tau_i)=0$, et donc par la Proposition 5.2.5, $P_r(\tau_i)=0$. Cela implique que $\tau_i \in \mathbb{F}_{2^\ell} \cap \mathbb{F}_{2^r} = \mathbb{F}_{2^2} = \mathbb{F}_4$. Comme $P_\ell(\tau_i) = P_r(\tau_i) = 0$, alors par le Lemme 5.1.7, 4 divise $\ell$ et $r$, Cela nous permet de conclure. □

On signale le résultat d'arithmétique élémentaire suivant, qui va nous servir à démontrer la Proposition 5.2.11.

**Lemme 5.2.10.** *Soit $l \in \mathbb{N}$. Considérons les deux entiers $d = 2^{r-1}(2^l+1)$ et $d' = 2^{2l}-1$. On a* $\mathrm{pgcd}(d,d')=3$,

*Démonstration.* On remarque que $d' = (2^\ell+1)(2^\ell-1)$. Soit $t$ un diviseur commun à $d$ et $d'$. Puisque $t$ divise $d'$, on peut écrire $t$ sous la forme : $t=ab$ avec $a$ un diviseur de $2^\ell+1$ et $b$ un diviseur de $2^\ell-1$. On a donc : $2^l \equiv -1 \pmod a$ et $2^\ell \equiv 1 \pmod b$. On en déduit que

(1) $d \equiv -1 \pmod{a}$ et

(2) $d \equiv 2^r - 1 \pmod{b}$.

Or $t = ab$ divise $d$ donc $d \equiv 0 \pmod{ab}$. Cela entraîne que $d \equiv 0 \pmod{a}$ et $d \equiv 0 \pmod{b}$.

(i) $0 \equiv -1 \pmod{a}$ et donc $a = 1$ et

(ii) $2^r \equiv 1 \pmod{b}$.

Ainsi l'ordre de 2 dans $(\mathbb{Z}/b\mathbb{Z})^*$ divise $\ell$ et $r$. Donc ordre$(2) = 1$ ou 2 dans $(\mathbb{Z}/b\mathbb{Z})^*$.

Si ord$(2) = 1$, alors $2 \equiv 1 \pmod{b}$, Cela implique que $b = 1$ et par suite $t = 1$.

Si ord$(2) = 2$, alors $b = 1$ ou 3 et par suite $t = 1$ ou $t = 3$.

Donc les seules diviseurs possibles de $pgcd(d, 2^{2\ell} - 1)$ sont 1 et 3. Or $2^{2\ell} - 1 \equiv 0 \pmod{3}$ et $2^{r-1}(2^\ell + 1) - 1 \equiv 0 \pmod{3}$, donc 3 divise $d$ et $d'$ et donc il divise leur plus grand diviseur commun, Cela nous permet de conclure. □

La proposition suivante nous montre que si pgcd$(\ell, r) = 2$, alors le terme $a_0^{2e} a_1^{de} \alpha^{(5d+4)e}$ apparaît dans l'expression de $b_0^N \Pi_d L_\alpha f$.

**Proposition 5.2.11.** *Considérons les deux entiers $\ell \geq 1$ et $r \geq 2$ avec* pgcd$(\ell, r) = 2$ *et soit $m = 2^r(2^\ell + 1)$. Soit $(i, j) \in \{1, \ldots, (d-1)/2\}^2$ tel que $i \neq j$ et soit $\tau_i$ et $\tau_j$ deux racines distinctes de $(L_1(x^{m-1})'$. On a :*

$$P_\ell(\tau_i + \tau_j) \neq 0.$$

*Démonstration.* Comme $\tau_i$ et $\tau_j$ sont différents, sans perdre de généralité on peut supposer que $\tau_i \neq 1$. Supposons que $P_\ell(\tau_i + \tau_j) = 0$, donc $\tau_i + \tau_j \in \mathbb{F}_{2^\ell}$. Alors $\frac{P_r(\tau_i+\tau_j)}{P_{r-1}(\tau_i+\tau_j)} \in \mathbb{F}_{2^l}$. Cela implique par la Proposition 5.2.5 que $P_\ell(\tau_i) \in \mathbb{F}_{2^\ell}$. On a par la linéarité de $P_\ell$ que $P_\ell(\tau_i + \tau_i^{2^\ell}) = 0$. En utilisant la Proposition 5.2.4, on obtient que

$$\frac{1}{1+\theta_i} = \frac{1}{1+\theta_i^{2^{2\ell}}}$$

et donc $\theta_i = \theta_i^{2^{2\ell}}$. Donc $\theta_i^{2^{2\ell}-1} = 1$, or $\theta_i^d = 1$, alors $\theta_i^{\text{pgcd}(2^{2\ell}-1,d)} = 1$. Cela implique par le Lemme 5.2.10 que $\theta_i^3 = 1$ et donc $\theta_i \in \mathbb{F}_4$. Cela implique que $\tau_i \in \mathbb{F}_4$. Mais comme $\mathbb{F}_4 \subset \mathbb{F}_{2^\ell}$, alors $\tau_i \in \mathbb{F}_{2^\ell}$. On conclut en utilisant le Lemme 5.2.9.

□

### 5.2.3 Cas $\text{pgcd}(\ell, r) \geq 3$ :

Il nous reste maintenant à traiter le troisième et dernier cas. On va démontrer dans ce cas que contrairement aux deux cas précédents on trouve deux racines distinctes $\tau_i$ et $\tau_j$ telle que que $P_\ell(\tau_i + \tau_j) = 0$. Par suite le terme $a_0^{2e} a_1^{de} \alpha^{(5d+4)e}$ n'apparaît pas dans l'expression de $b_0^N \Pi_d L_\alpha f$.

**Proposition 5.2.12.** *Considérons les deux entiers $\ell \geq 1$ et $r \geq 2$ avec $\text{pgcd}(\ell, r) \geq 3$ et soit $m = 2^r(2^\ell + 1)$. Il existe $\tau_i \neq \tau_j$ tel que $P_\ell(\tau_i + \tau_j) = 0$.*

*Démonstration.* D'après le Lemme 5.1.6 on a $P_a(x)$ divise $P_\ell(x)$ et $P_r(x)$. Comme $a \geq 3$, il existe deux racines distinctes non nuls $u$ et $v$ de $P_a$. Donc $u$ et $v$ sont deux racines distinctes non nulles de $P_\ell$ et $P_r$. En utilisant la Proposition 5.2.2, $u$ et $v$ sont des racines distinctes non nulles de $h$. Cela implique qu'il existe $(i, j) \in \{1, 2, \cdots, \frac{d-1}{2}\}$ tel que $u = \tau_i$ et $v = \tau_j$ et $\tau_i \neq \tau_j$. Alors,

$$P_\ell(\tau_i + \tau_j) = P_\ell(\tau_i) + P_\ell(\tau_j) = P_\ell(u) + P_\ell(v) = 0 + 0 = 0.$$

□

## 5.3 Démonstration du théorème principal.

Après avoir donné tous les préliminaires nécessaires on est prêt maintenant à démontrer le théorème principal de la thèse qui répond partiellement aux deux questions ouvertes mentionnées dans l'introduction.

**Théorème 5.3.1.** *Soit $m = 2^\ell(2^r+1)$, où $\ell$ et $r$ sont deux entiers tels que $\text{pgcd}(\ell, r) \leq 2, \ell \geq 2$ et $r \geq 1$. Pour un entier $n$ suffisamment grand et pour tout polynôme*

$$f(x) = \sum_{k=0}^{m} a_{m-k} x^k \in \mathbb{F}_{2^n}[x]$$

*de degré $m$ tel que $a_1 \neq 0$ on a $\delta(f) = m - 2$.*

*Démonstration.* En utilisant le Corollaire 3.3.18, pour démontrer que $\delta(f)$ est maximal, il suffit de démontrer que pour $n$ suffisamment grand il existe $\alpha \in \mathbb{F}_{2^n}^*$ pour lequel :

(1) $L_\alpha f$ est Morse.

(2) Il existe $x \in \mathbb{F}_{2^n}$ tel que $x^2 + \alpha x = \frac{b_1}{b_0}$ .

Cela est équivalent à démontrer qu'il existe $\alpha \in \mathbb{F}_{2^n}^*$ pour lequel :

(1) $L_\alpha f$ est Morse.

(2) $\mathrm{Tr}(\frac{b_1}{b_0\alpha^2}) = 0$.

Par le Proposition 5.1.8, la Proposition 5.2.7 et la Proposition 5.2.11, le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels $L_\alpha f$ n'a pas des valeurs critiques distinctes est au plus $(5d+4)\binom{(d-1)(2)}{2}$. En utilisant le Théorème 3.6.2, le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels $L_\alpha f$ n'a pas des points critiques non dégénérés est au plus $(m-1)(m-4)$. En plus, en utilisant le Corollaire 3.5.5, le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels il existe $x \in \mathbb{F}_{2^n}$ tel que $x^2 + \alpha x = \frac{b_1}{b_0}$ est au moins $2^{n-1} - 1$. Donc en choisissant $n$ tel que

$$2^{n-1} - 2^{\frac{n}{2}} > 1 + (5d+4)\binom{(d-1)(2)}{2} + (m-1)(m-4)$$

et

$$\frac{q}{d_\Omega} - 2\Big((1 + \frac{g_\Omega}{d_\Omega})q^{1/2} + q^{1/4} + 1 + \frac{g_\Omega}{d_\Omega}\Big) \geqslant 1. \tag{5.2}$$

avec : $q = 2^n$. $d_\Omega = d!2^{d-1}$ et $g_\Omega \leqslant d!2^d(d-3/2)+1$, on peut appliquer la Proposition 3.3.16 et on garantit l'existence d'un élément $\alpha$ dans $\mathbb{F}_{2^n}^*$ pour lequel le polynôme $L_\alpha f$ est Morse et l'équation $x^2 + \alpha x = \frac{b_1}{b_0}$ admet une solution dans $\mathbb{F}_{2^n}$. Cela nous nous permet de conclure. □

En choisissant $\ell = 2$ et $r = 1$, on retrouve le résultat sur les polynômes de degré 12. De même, en choisissant $\ell = 2$ et $r = 2$, on obtient le résultat sur les polynômes de degré 20.

Rappelons maintenant les deux questions ouvertes que l'on a posées dans l'introduction.

**Question ouverte 1.** *Pour un entier naturel $\ell$, parmi les polynômes de degré $m = 4(2^\ell + 1)$, lesquels sont APN exceptionnels ?*

**Question ouverte 2.** *Parmi les polynômes de degré $m \equiv 0 \pmod 8$, lesquels sont APN exceptionnels ?*

On remarque qu'en choisissant $\ell = 2$, on répond à la première question ouverte. De plus, si on choisit $\ell > 2$, on répond partiellement à la deuxième question ouverte.

# Chapitre 6

# Résultats obtenus dans le cas des trinômes

Dans ce Chapitre, nous nous consacrons au cas des trinômes. En effet, nous avons remarqué que dans le cas des trinômes, on peut plus facilement transférer des résultats de majoration du nombre de $\alpha$ tel que $L_\alpha f$ soit à valeurs critiques distinctes, à partir de l'article [2].

Nous traitons d'abord le cas des binômes et nous en déduisons celui des trinômes. Nous avons déjà défini dans la Définition 2.3.5, un ensemble $\mathcal{M}$ en termes des racines de l'unité. Rappelons maintenant une définition équivalente qui est donnée dans [2].

**Définition 6.0.1** (Définition 3.10 de [2])**.** On définit $\mathcal{M}$ par l'ensemble des entiers impairs $m$ pour lesquels $L_\alpha x^m$ a des valeurs critiques distinctes.

On passe maintenant au lemme suivant qui nous permet de traiter la condition (I.b) dans le cas des binômes.

**Lemme 6.0.2.** *Soit $m \equiv 0 \pmod 4$ un entier tel que $m-1 \in \mathcal{M}$. Pour tout binôme $f(x) = a_0x^m + a_1x^{m-1} \in \mathbb{F}_{2^n}[x]$ de degré $m$ tel que $a_1 \neq 0$, le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels les valeurs critiques de $L_\alpha f$ ne sont pas distinctes est au plus $(5d+2)\binom{(d-1)(2)}{2}$.*

*Démonstration.* On a par la Proposition 3.2.11 que $L_\alpha f$ a des valeurs critiques distinctes si et seulement si

$$\Pi_d(L_\alpha f) := \prod_{i<j} (L_\alpha f(\tau_i) - L_\alpha f(\tau_j)) \neq 0$$

où les $\tau_i$ sont les racines de $(L_\alpha f)'$. Pour majorer le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels le polynôme $L_\alpha f$ n'a pas des valeurs critiques distinctes, il suffit de démontrer que

le polynôme $b_0^N \Pi_d(L_\alpha f)$ vu comme un polynôme dans $\mathbb{F}_2[a_0, a_1][\alpha]$ est un polynôme non nul. Cela revient à démontrer qu'il existe un monôme non nul dans l'expression de $b_0^N \Pi_d(L_\alpha f)$. En utilisant le Lemme 3.1.7 on a :

$$b_0^N \Pi_d(L_\alpha f) = \sum \epsilon(i_0, i_1) a_0^{i_0} a_1^{i_1} \alpha^{r(i_0,i_1)}.$$

La somme est prise sur les couples d'entiers $(i_0, i_1)$ tel que :

(1) $\epsilon(i_0, i_1) = 0$ ou 1.

(2) $i_0 + i_1 = (d+2)\binom{(d-1)/2}{2}$.

(3) $r(i_0, i_1)$ est défini par $r(i_0, i_1) = (6d+4)\binom{(d-1)/2}{2} - i_1$.

Parmi les termes qui peuvent apparaître dans la somme, on va distinguer trois cas :
Premier cas : Si $i_0 = 0$, alors

$$\epsilon(i_0, i_1) a_0^{i_0} a_1^{i_1} \alpha^{r(i_0,i_1)} = \epsilon(0, i_1) a_1^{(d+2)\binom{(d-1)/2}{2}} \alpha^{(5d+2)\binom{(d-1)/2}{2}}.$$

Deuxième cas : Si $i_1 = 0$, alors

$$\epsilon(i_0, i_1) a_0^{i_0} a_1^{i_1} \alpha^{r(i_0,i_1)} = \epsilon(i_0, 0) a_0^{(d+2)\binom{(d-1)/2}{2}} \alpha^{(6d+4)\binom{(d-1)/2}{2}}.$$

Troisième cas : Si $i_0 \neq 0$ et $i_1 \neq 0$ alors

$$\begin{aligned}
\epsilon(i_0, i_1) a_0^{i_0} a_1^{i_1} \alpha^{r(i_0,i_1)} &= \epsilon(i_0, 0) a_0^{(d+2)\binom{(d-1)/2}{2}} \alpha^{(6d+4)\binom{(d-1)/2}{2} - i_1} \\
&= \epsilon(i_0, 0) a_0^{(d+2)\binom{(d-1)/2}{2}} \alpha^{(6d+4)\binom{(d-1)/2}{2} - (d+2)\binom{(d-1)/2}{2} + i_0} \\
&= \epsilon(i_0, 0) a_0^{(d+2)\binom{(d-1)/2}{2}} \alpha^{(5d+2)\binom{(d-1)/2}{2} + i_0}
\end{aligned}$$

Comme $m - 1 \in \mathcal{M}$, alors $L_\alpha(x^{m-1})$ a des valeurs critiques distinctes et donc

$$\Pi_d(L_\alpha(f)(a_0 = 0, a_1 = 1, a_2 = 0, \ldots, a_m = 0, \alpha = 1) \neq 0.$$

Cela implique que $\epsilon(0, i_1) \neq 0$ et par suite le terme

$$\epsilon(0, i_1) a_1^{(d+2)\binom{(d-1)/2}{2}} \alpha^{(5d+2)\binom{(d-1)/2}{2}} = a_1^{(d+2)\binom{(d-1)/2}{2}} \alpha^{(5d+2)\binom{(d-1)/2}{2}} \neq 0$$

apparaît dans l'expression de $b_0^N \Pi_d L_\alpha f$, cela nous permet de conclure. □

Dans la remarque suivante on rappelle un lemme de l'article [2] qui va nous servir dans la démonstration de la Proposition 6.0.4.

**Remarque 6.0.3** (Lemme 3.4 dans [2])**.** Soit $f \in \mathbb{F}_{2^n}[x]$. Pour tout $\alpha \in \mathbb{F}_{2^n}^*$, le polynôme $L_\alpha f$ a des valeurs critiques distinctes si et seulement si pour tout $(\tau, \eta) \in (\overline{\mathbb{F}_2})^2$, $(D_\alpha f)'(\tau) = (D_\alpha f)'(\eta) = 0$ et $D_\alpha f(\tau) = D_\alpha f(\eta)$ implique $\tau = \eta$ ou $\tau = \eta + \alpha$.

La proposition suivante permet de transférer un résultat sur les valeurs critiques des binômes aux trinômes.

**Proposition 6.0.4.** *Soit $m \in \mathbb{N}$ un entier tel que $m \equiv 0 \pmod 4$ et soit $f(x) = a_0x^m + a_1x^{m-1} \in \mathbb{F}_{2^n}[x]$ un binôme de degré $m$ tel que $a_1 \neq 0$. Pour tout polynôme $g(x) \in \mathbb{F}_{2^n}[x]$ de la forme*

$$g(x) = f(x) + a_2x^{m-2},$$

*les valeurs critiques de $L_\alpha f$ sont distinctes si et seulement si les valeurs critiques de $L_\alpha g$ sont distinctes.*

*Démonstration.* En utilisant la Remarque 6.0.3, $L_\alpha f$ a des valeurs critiques distinctes si et seulement si pour tout $(\tau, \eta) \in \overline{\mathbb{F}_2}$ :

$$D_\alpha f(\tau) = D_\alpha f(\eta) \text{ et } (D_\alpha f)'(\tau) = (D_\alpha f)'(\eta) = 0 \implies \tau = \eta \text{ ou } \tau = \eta + \alpha.$$

C'est le cas si et seulement si pour tout $(\tau, \eta) \in \overline{\mathbb{F}_2}$, les deux égalités suivantes

$$a_0(\tau+\alpha)^m+a_0\tau^m+a_1(\tau+\alpha)^{m-1}+a_1\tau^{m-1} = a_0(\eta+\alpha)^m+a_0\eta^m+a_1(\eta+\alpha)^{m-1}+a_1\eta^{m-1}$$

et

$$a_1(\tau+\alpha)^{m-2} + a_1\tau^{m-2} = a_1(\tau+\alpha)^{m-2} + a_1\tau^{m-2} = 0$$

impliquent que $\tau = \eta$ ou $\tau = \eta+\alpha$. C'est équivalent à dire que, pour tout $(\tau, \eta) \in \overline{\mathbb{F}_2}$, les deux égalités suivantes

- $a_0(\tau+\alpha)^m + a_0\tau^m + a_1(\tau+\alpha)^{m-1} + a_1\tau^{m-1} + a_2(\tau+\alpha)^{m-2} + a_2\tau^{m-2} = a_0(\eta+\alpha)^m + a_0\eta^m + a_1(\eta+\alpha)^{m-1} + a_1\eta^{m-1} + a_2(\eta+\alpha)^{m-2} + a_2\eta^{m-2}$.
- $a_1(\tau+\alpha)^{m-2} + a_1\tau^{m-2} = a_1(\tau+\alpha)^{m-2} + a_1\tau^{m-2} = 0$

impliquent que $\eta = \tau$ ou $\eta = \tau + \alpha$, c'est-à-dire que $L_\alpha g$ a des valeurs critiques distinctes. □

D'après le Corollaire 3.3.18, pour démontrer le Théorème 6.0.6, il suffit de trouver un $\alpha \in \mathbb{F}_{2^n}^*$ tel que :

(1) Le polynôme $L_\alpha f$ est Morse.

(2) Il existe $x \in \mathbb{F}_{2^n}$ tel que $x^2 + \alpha x = \frac{b_1}{b_0}$.

Dans le Théorème 3.6.2 on a réussi à majorer le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels la condition (I.a) n'est pas vérifiée, de même dans le Corollaire 3.5.5, on a réussi à majorer le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels la condition (II) n'est pas vérifiée. Comme $n$ est choisi suffisamment grand, il suffit alors de majorer le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels la condition (I.b) n'est pas vérifiée. C'est ce que l'on va faire dans le corollaire suivant :

**Corollaire 6.0.5.** *Soit $m \in \mathbb{N}$ un entier tel que $m \equiv 0 \pmod 4$ et $m-1 \in \mathcal{M}$. Pour tout trinôme $f(x) = a_0x^m + a_1x^{m-1} + a_2x^{m-2} \in \mathbb{F}_{2^n}[x]$ de degré $m$ tel que $a_1 \neq 0$, le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquelles les valeurs critiques de $L_\alpha f$ ne sont pas distinctes est au plus $(5d+2)\binom{(d-1)(2)}{2}$.*

*Démonstration.* Soit $W(x) = a_0x^m + a_1x^{m-1}$. En utilisant la Proposition 6.0.4, les valeurs critiques de $L_\alpha f$ sont distinctes si et seulement si les valeurs critiques de $L_\alpha W$ sont distinctes. Donc en utilisant le Lemme 6.0.2, le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquelles les valeurs critiques de $L_\alpha f$ ne sont pas distinctes est au plus $(5d+2)\binom{(d-1)(2)}{2}$. □

On est près maintenant à démontrer notre dernier résultat.

**Théorème 6.0.6.** *Soit $m \in \mathbb{N}$ un entier tel que $m \equiv 0 \pmod 4$ et $m-1 \in \mathcal{M}$. Pour $n$ suffisamment grand et pour tout trinôme $f(x) = a_0x^m + a_1x^{m-1} + a_2x^{m-2} \in \mathbb{F}_{2^n}[x]$ de degré $m$ tel que $a_1 \neq 0$, $\delta(f)$ est maximale, c'est-à-dire $\delta(f) = m-2$.*

*Démonstration.* En utilisant le Corollaire 3.3.18, pour démontrer que $\delta(f)$ est maximal, il suffit de démontrer que pour $n$ suffisamment grand il existe $\alpha \in \mathbb{F}_{2^n}^*$ pour lequel :

(1) $L_\alpha f$ est Morse.

(2) L'équation $x \in \mathbb{F}_{2^n}$ tel que $x^2 + \alpha x = \frac{b_1}{b_0}$ a une solution dans $\mathbb{F}_{2^n}$.

En utilisant le Corollaire 3.4.4, ça revient à démontrer qu'il existe $\alpha \in \mathbb{F}_{2^n}^*$ pour lequel :

(1) $L_\alpha f$ est Morse.

(2) $\mathrm{Tr}(\frac{b_1}{b_0\alpha^2}) = 0$.

Par le Corollaire 6.0.5, le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels $L_\alpha f$ n'a pas des valeurs critiques distinctes est au plus $(5d+2)\binom{(d-1)(2)}{2}$. En utilisant le Théorème 3.6.2, le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels $L_\alpha f$ n'a pas des points critiques non dégénérés est au plus $(m-1)(m-4)$. En plus, en utilisant le Corollaire 3.5.5, le nombre de $\alpha \in \mathbb{F}_{2^n}^*$ pour lesquels il existe $x \in \mathbb{F}_{2^n}$ tel que $x^2 + \alpha x = \frac{b_1}{b_0}$ est au moins $2^{n-1} - 2^{\frac{n}{2}} - 1$. Donc en choisissant $n$ suffisamment grand on garantit l'existence d'un $\alpha \in \mathbb{F}_{2^n}^*$ pour lequel les conditions (I.a), (I.b), (I.c) et (II) sont vérifiées, cela nous permet de conclure. □

En utilisant l'Exemple 2.3.5, et le Théorème 6.0.6, on obtient que pour $n$ suffisamment grand et pour tout trinôme $f(x) = a_0x^m + a_1x^{m-1} + a_2x^{m-2} \in \mathbb{F}_{2^n}[x]$ de degré $m = 6.9^k + 2$, avec $k \geq 1$, on a $\delta(f) = m - 2$ et donc $f$ n'est pas APN exceptionnel. On répond ainsi partiellement à la question ouverte 2 mentionnée dans la section 2.2.

# Bibliographie


[1] Yves Aubry and Fabien Herbaut. Differential uniformity and second order derivatives for generic polynomials, J. Pure Appl. Algebra 222, no. 5, 1095–1110, 2018.

[2] Yves Aubry, Fabien Herbaut and José Felipe Voloch. Maximal differential uniformity polynomials, Acta Arith. 188, no. 4, 345–366, 2019.

[3] Yves Aubry, Fabien Herbaut and Ali Issa. Polynomials with maximal differential uniformity and the APN conjecture. Article soumis pour publication, https://arxiv.org/abs/2207.13945, 2022.

[4] Yves Aubry, Gary McGuire and François Rodier. A few more functions that are not APN infinitely often, Finite fields : theory and applications, 23–31, Contemp. Math. 518, Amer. Math. Soc., Providence, RI, 2010.

[5] Daniele Bartoli and Kai-Uwe Schmidt. Low-degree planar polynomials over finite fields of characteristic two, J. Algebra 535, 541–555, 2019.

[6] Elwyn Ralph Berlekamp, H. Rumsey and G. Solomon. On the solution of algebraic equations over finite fields. Information and Control 10 , 553–564. 1967.

[7] Lilya Budaghyan, Claude Carlet and Alexander Pott. New classes of almost bent and almost perfect nonlinear polynomials. IEEE Trans. Inform. Theory 52, no. 3, 1141–1152, 2006.

[8] Florian Caullery. A new large class of functions not APN infinitely often, Des. Codes and Cryptogr., 73, no. 2, 601-614, 2014.

[9] Paul Moritz Cohn. Basic Algebra. Groups, Rings, and Fields. Springer-Verlag. ISBN 1-85233-587-4. Zbl 1003.00001, 2003.

[10] Moisés Delgado. The state of the art on the conjecture of exceptional APN functions, Note Mat. 37, no. 1, 41–51, 2017.

[11] Pierre-Alain Fouque and Mehdi Tibouchi. Estimating the size of the image of deterministic hash functions to elliptic curves. In Progress in Cryptology - Latincrypt Lecture Notes in Computer Science vol. 6212, 2010, pp. 81–91. Springer, 2010.

[12] Michael David Fried and Moshe Jarden. Field Arithmetic. In A Series of Modern Surveys in Mathematics vol. 1, Springer-Verlag, Berlin, 2007.

[13] Michael David Fried and Moshe Jarden. Field Arithmetic. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. Vol. 11 (3rd revised ed.). Springer-Verlag. pp. 38–41. ISBN 978-3-540-77269-9. Zbl 1145.12001, 2008

[14] Fernando Hernando and Gary McGuire. Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions, J. Algebra 343, 78–92, 2011.

[15] Ali Issa. Infinite famillies of not exceptional APN trinomials. Article en préparation.

[16] Moshe Jarden and Aharon Razon. Skolem density problems over large Galois extensions of global fields. In Hilbert's tenth problem : relations with arithmetic and algebraic geometry (Ghent, 1999), volume 270 of Contemp. Math., pages 213–235. Amer. Math. Soc., Providence, RI, 2000. With an appendix by Wulf-Dieter Geyer.

[17] Heeralal Janwa, Gary McGuire and Richard Michael Wilson. Double-error-correcting codes and absolutely irreducible polynomials over GF(2), Journal of Algebra vol. 178, 665-676, Academic Press, 1995.

[18] Heeralal Janwa and Richard Michael Wilson. Hyperplane sections of Fermat varieties in $\mathbb{P}^3$ in char. 2 and some applications to cyclic codes, Applied algebra, algebraic algorithms and error-correcting codes, 180–194, Lecture Notes in Comput. Sci., 673, Springer, Berlin, 1993.

[19] Serge Lang. Algebra, Graduate Texts in Mathematics 211, Springer Verlag, ISBN : 978-0-38795385-4, 2002.

[20] Kaisa Nyberg. Differentially uniform mappings for cryptography. In Advances in cryptology—Eurocrypt '93, 55–64, Lecture Notes in Comput. Sci., 765, Springer, Berlin, 1994.

[21] Paul Pollack. Simultaneous prime specializations of polynomials over finite fields. Proc. Lond. Math. Soc., (3) 97, no. 3, 545–567, 2008.

[22] François Rodier. Functions of degree 4e that are not APN infinitely often Cryptogr. Commun. 3, no.4, 227-240, 2011.

[23] François Rodier. Bornes sur le degré des polynômes presque parfaitement non-linéaires, in Arithmetic, Geometry, Cryptography and Coding Theory, G. Lachaud, C. Ritzenthaler and M.Tsfasman editors, Contemporary Math. no 487, AMS, Providence (RI), USA, pp. 169-181, 2009.

[24] Jean-Pierre Serre. Topics in Galois theory. Research Notes in Mathematics, 1, A K Peters, Ltd, Wellesley, MA, 2008.

[25] Henning Stichtenoth. Algebraic Function Fields and Codes. Volume 254 de Graduate Texts in Mathematics, Springer Science and Business Media, ISBN 3540768777, 9783540768777, 2008.

[26] José Felipe Voloch. Symmetric cryptography and algebraic curves. Algebraic geometry and its applications, 135–141, Ser. Number Theory Appl., 5, World Sci. Publ., Hackensack, NJ, 2008.

# Résumé

Nous étudions dans cette thèse l'uniformité différentielle des polynômes de degré pair définis sur des corps finis de caractéristique 2. Une caractérisation des polynômes Morse permet de comparer certains groupes de monodromie arithmétiques et géométriques et ainsi d'appliquer le théorème de densité de Chebotarev, central dans notre travail. On en déduit que si le pgcd de deux entiers $\ell \geq 1$ et $r \geq 2$ vaut 1 ou 2, les polynômes de degré $m = 2^r(2^\ell + 1)$ avec un second coefficient dominant non nul ont une uniformité différentielle maximale (c'est-à-dire égale à $m - 2$), sur une extension suffisamment grande du corps de base.

En particulier ces polynômes ne sont pas APN exceptionnels, ce qui apporte une contribution à la conjecture d'Aubry, McGuire et Rodier dans le sens où les cas des polynômes de degré multiple de 8 ou encore de degré $m = 4(2^\ell + 1)$ étaient encore complètement ouverts dans les travaux sur le sujet.

## Mots clés

Théorème de Chebotarev, groupes de monodromie et polynômes APN.

# Abstract

We study in this Ph.D. thesis the differential uniformity of polynomials of even degree defined over finite fields of characteristic 2. A characterization of Morse polynomials enables to compare some arithmetic and geometric monodromy groups and thus to apply the Chebotarev's density theorem which is central to our work. We deduce that if the gcd of two integers $\ell \geq 1$, $r \geq 2$ equals 1 or 2, then the polynomials of degree $m = 2^r(2^\ell + 1)$ with a non-zero second leading coefficient have a maximal differential uniformity (that is equals to m-2) on sufficently large extension of the base field.

In particular these polynomials are not exceptional APN. It contributes to the conjecture of Aubry, McGuire and Rodier in the sense that the cases of polynomials of degree multiple of 8 or $m = 4(2^\ell + 1)$ were open.

## Keywords

Chebotarev's theorem, monodromy groups and APN polynomials.