HAL open science

Fonctions PN sur une infinité d'extensions de F_p, p impair

Elodie Leducq

▶ To cite this version:

Elodie Leducq. Fonctions PN sur une infinité d'extensions de F_p, p impair. 2010. hal-00488098

HAL Id: hal-00488098
https://hal.science/hal-00488098v1

Preprint submitted on 1 Jun 2010

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Fonctions PN sur une infinité d'extensions de $\mathbb{F}_p$, p impair

Elodie Leducq*

1 Introduction

Dans les articles [5] et [4], les auteurs s'intéressent aux m tels que x^m soit presque parfaitement non linéaire (APN) dans une infinité d'extensions de $\mathbb{F}_2$. En utilisant des méthodes analogues aux leurs, nous étudions ici le cas des fonctions parfaitement non linéaires (PN) sur des corps finis de caractéristique impaire.
On rappelle la définition suivante :

Définition 1 *Soit p un nombre premier, on dit qu'une fonction ϕ est APN sur $\mathbb{F}_{p^n}$ si*

$$\forall a, b \in \mathbb{F}_{p^n}, a \neq 0, |\{x \in \mathbb{F}_{p^n}, \phi(x+a) - \phi(x) = b\}| \leq 2.$$

et si, de plus, il existe un couple (a, b) tel que cette inégalité soit une égalité.

Jedlicka, Hernando et McGuire ont démontré qu'en caractéristique 2, les seuls exposants m tels que x^m soit APN sur une infinité d'extensions de $\mathbb{F}_2$ sont $m = 2^k + 1$ (Gold) et $m = 4^k - 2^k + 1$ (Kasami). Pour cela, ils utilisent le fait qu'une fonction est APN sur $\mathbb{F}_{2^n}$ si et seulement si les seuls points rationnels sur $\mathbb{F}_{2^n}$ de $f(x, y) = (x+1)^m + x^m + (y+1)^m + y^m$ sont les points tels que $x = y$ ou $x = y + 1$. Ils cherchent alors à déterminer les m tels que pour une infinité de n les seuls points rationnels de $f(x, y)$ soient ceux tels que $x = y$ ou $x = y + 1$. Ceci ne peut se produire que si la courbe $\frac{f(x,y)}{(x+y)(x+y+1)}$ n'a pas de facteur absolument irréductible sur $\mathbb{F}_2$.

En caractéristique 2, si $\phi(x+a) + \phi(x) = b$ alors
$\phi(x+a+a) + \phi(x+a) = b$. En particulier, il n'existe pas de fonction PN (voir définition ci-dessous) et il suffit que $|\{x \in \mathbb{F}_{p^n}, \phi(x+a) - \phi(x) = b\}| \leq 2$ pour que ϕ soit APN.

En caractéristique impaire, contrairement à la caractéristique 2, pour ϕ APN, on ne connait pas la relation entre les deux racines éventuelles (il peut n'y en avoir qu'une) de $\phi(x+a) - \phi(x) = b$, il ne semble donc pas possible d'adapter cette démonstration aux fonctions APN. Le bon cadre semble être les fonctions PN, dont nous rappelons ici la définition :

*IMJ, en thèse sous la direction de Jean-françois Mestre

Définition 2 *Soit p un nombre premier impair. Une fonction ϕ est dite PN sur $\mathbb{F}_{p^n}$ si pour tout $b \in \mathbb{F}_{p^n}$ et pour tout $a \in \mathbb{F}_{p^n}^*$*

$$|\{x \in \mathbb{F}_{p^n}, \phi(x+a) - \phi(x) = b\}| = 1$$

De manière équivalente, une fonction ϕ est PN sur $\mathbb{F}_{p^n}$ si et seulement si pour tout $\alpha \in \mathbb{F}_{p^n}$ les seuls points rationnels sur $\mathbb{F}_{p^n}$ de

$$f_\alpha(x,y) = \phi(x+\alpha) - \phi(x) - \phi(y+\alpha) + \phi(y)$$

sont les points tels que $x = y$.

On considère maintenant $\phi(x) = x^m$, $m \geq 3$. On peut alors se ramener au cas où $\alpha = 1$.

Remarque 3 *Si m est impair, 0 et -1 sont solutions de l'équation $(x+1)^m - x^m = 1$ donc x^m n'est pas PN sur $\mathbb{F}_{p^n}$ pour tout n.*

On pose $f(x,y) = (x+1)^m - x^m - (y+1)^m + y^m$; f étant divisible par $(x-y)$, on définit $h(x,y) = \frac{f(x,y)}{(x-y)}$.

On peut supposer $m \not\equiv 0 \mod p$. En effet, si x^m est PN et si $m \equiv 0 \mod p$ alors $x^{\frac{m}{p}}$ est aussi PN.
Dans toute la suite, on va s'intéresser au cas $m \equiv 1 \mod p$. On note l le plus grand entier tel que p^l divise $m-1$, et
$d = \text{pgcd}(m-1, p^l - 1) = \text{pgcd}\left(\frac{m-1}{p^l}, p^l - 1\right)$.

Proposition 4 *Si $m = p^l + 1$, avec $\frac{n}{\text{pgcd}(n,l)}$ impair, x^m est PN sur $\mathbb{F}_{p^n}$*

Preuve : Si $m = p^l + 1$, $(x+1)^m - x^m = b \Leftrightarrow x^{p^l} + x = b - 1$. Par le corollaire 3.3 de [1], on a le résultat.

□

Proposition 5 *Si h a un facteur absolument irréductible sur $\mathbb{F}_p$ alors $\phi(x) = x^m$ n'est pas PN sur $\mathbb{F}_{p^n}$ pour n assez grand.*

Preuve : Soit $m \not\equiv 0 \mod p$ tel que x^m soit PN. Supposons que h ait un facteur absolument irréductible que l'on note q.
Si $q = c(x-y)$, $c \in \mathbb{F}_{p^n}^*$ alors $f(x,y) = (y-x)^2 \widetilde{q}(x,y)$, $\widetilde{q} \in \mathbb{F}_{p^n}[x,y]$.
On dérive cette expression par rapport à y et on obtient :

$$-m(y+1)^{m-1} + my^{m-1} = 2(y-x)\widetilde{q}(x,y) + (y-x)^2 \frac{\partial \widetilde{q}}{\partial y}(x,y)$$

On obtient donc que pour tout $x \in \mathbb{F}_{p^n}$, $-m(x+1)^{m-1} + mx^{m-1} = 0$. C'est impossible car $m \not\equiv 0 \mod p$.
Soit d le degré de q. Comme $q \neq c(x-y)$, $g(x,x)$ n'est pas le polynôme nul. Il y a donc au plus d points rationnels de q tels que $x = y$.
D'autre part, si on note P le nombre total de points rationnels de q sur $\mathbb{F}_{p^n}$, par le théorème de Weil on a :

$$|P - (p^n + 1)| \leq 2g\sqrt{p^n},$$

où g est le genre de q.
Donc pour n assez grand, q a un point rationnel tel que $x \neq y$, ce qui est absurde car x^m est PN. Par contraposée, on a démontré la proposition.

□

Théorème 6 *Soit m un entier non divisible par p, $m \geq 3$, $m \equiv 1 \mod p$ et $m \neq p^l+1$. Supposons de plus que $\frac{m-1}{p^l} \neq p^l-1$, alors h a un facteur absolument irréductible sur $\mathbb{F}_p$.*

Corollaire 7 *Les seuls $m \equiv 1 \mod p$, tel que x^m soit PN dans $\mathbb{F}_{p^n}$ pour une infinité de n sont les $m = 1 + p^l$.*

Preuve : Par le théorème 6 et la proposition 5, on a tous les cas sauf le cas où $d = \frac{m-1}{p^l} = p^l - 1$. Dans ce dernier cas, on a $m = p^l(p^l - 1) + 1$, il est donc impair. D'où $x^{p^l(p^l-1)+1}$ n'est pas PN dans $\mathbb{F}_{p^n}$ pour tout n.

□

Il reste donc à démontrer le théorème 6. La méthode utilisée dans les articles [4] et [5] consiste à utiliser le théorème de Bézout pour montrer que h n'a pas assez de points singuliers pour ne pas avoir de facteur absolument irréductible. Dans la partie 2, on étudie les points singuliers de h et leur multiplicité. Dans la partie 3, on majore le nombre d'intersection (*cf.* [3] pour une définition) $I_t(u, v)$ en un point singulier t de h et pour une factorisation de h sous la forme $h = uv$. Enfin, dans la partie 4, on démontre le théorème 6.

2 Classification des singularités de h

Proposition 8 *Si $m \equiv 1 \mod p$, les singularités de h sont décrites dans le tableau 1.*

La preuve de ce théorème découle des lemmes 9 à 23 et de leurs corollaires.

2.1 Singularités à l'infini

On note $\widehat{f}$ (resp. $\widehat{h}$) l'homogénéisée de f (resp. h). On note $\widetilde{f}$ (resp. $\widetilde{h}$) la forme deshomogénéisée de $\widehat{f}$ (resp. $\widehat{h}$) par rapport à y.

Soit $F(x, y, z) = (x + z)^m - x^m - (y + z)^m + y^m = z\widehat{f}$. On a

$$\begin{cases} F_x &= m(x+z)^{m-1} - mx^{m-1} \\ F_y &= -m(y+z)^{m-1} + my^{m-1} \\ F_z &= m(x+z)^{m-1} - m(y+z)^{m-1} \end{cases}$$

On cherche les points singuliers à l'infini.

On a $F_x = F_y = 0$ et $F_z = m(x^{m-1} - y^{m-1})$ donc $(x_0, y_0, 0)$ est un point singulier de F si et seulement si $x_0^{m-1} = y_0^{m-1}$.
Si $y_0 = 0$ alors $x_0 = 0$ donc $y_0 \neq 0$ et on est ramené à étudier les solutions de

$$x_0^{m-1} = 1 \tag{1}$$

L'équation (1) est équivalente à $x_0^{\frac{m-1}{p^l}} = 1$. Or $\operatorname{pgcd}\left(\frac{m-1}{p^l}, p\right) = 1$ donc il y a $\frac{m-1}{p^l}$ solutions à (1).

TABLE 1 – Singularités de h pour $m \equiv 1 \mod p$

Type	Description	$m_t(h)$	max de I_t	nombre de points max
Ia	Affine $x_0 = y_0$ $x_0,\, y_0 \in \mathbb{F}_{p^l}^*$	p^l	$\frac{p^{2l}-1}{4}$	$d-1$
Ib	Affine $x_0 = y_0$, $x_0,\, y_0 \notin \mathbb{F}_{p^l}^*$	$p^l - 1$	0	$\frac{m-1}{p^l} - d$
IIa	Affine $x_0 \neq y_0$, $x_0,\, y_0 \in \mathbb{F}_{p^l}^*$	$p^l + 1$	$\left(\frac{p^l+1}{2}\right)^2$	$(d-1)(d-2)$
IIb	Affine $x_0 \neq y_0$, x_0 ou $y_0 \notin \mathbb{F}_{p^l}^*$	p^l	0	N_1 [a]
IIc	Affine $x_0 \neq y_0$, x_0 et $y_0 \notin \mathbb{F}_{p^l}^*$	p^l	p^l [b]	N_2 [c]
IIIa	$(1:1:0)$	$p^l - 1$	$\left(\frac{p^l-1}{2}\right)^2$	1
IIIb	$(\omega : 1 : 0)$, $\omega^d = 1$ et $\omega \neq 1$	p^l	$\frac{p^{2l}-1}{4}$	$d-1$
IIIc	$(\omega : 1 : 0)$, $\omega^d \neq 1$	$p^l - 1$	0	$\frac{m-1}{p^l}$

a. $N_1 = \left(\frac{m-1}{p^l} - 1\right)\left(2\frac{m-1}{p^l} - (m_b+1)p^{i_b - l} - 1\right) - (d-1)(d-2)$

b. $I_t(u,v) = 0$ si $y_0(x_0+1)^{p^l}(y_0^{p^l-1}-1)^{p^l+1} \neq x_0(y_0+1)^{p^l}(x_0^{p^l-1}-1)^{p^l+1}$

c. $N_2 = \begin{cases} \left(\frac{m-1}{p^l} - 1\right)\left(2\frac{m-1}{p^l} - (m_b+1)p^{i_b - l} - 1\right) - (d-1)(d-2) \\ \text{ou } ((p^l-2)(p^l+1)-1)(\frac{m-1}{p^l} - 1) \\ \qquad \text{si } y_0(x_0+1)^{p^l}(y_0^{p^l-1}-1)^{p^l+1} = x_0(y_0+1)^{p^l}(x_0^{p^l-1}-1)^{p^l+1} \end{cases}$

De plus $x_0 = 1$ est la seule solution telle que $x_0 = y_0$.

On étudie maintenant la multiplicité de ces singularités.

$$\begin{aligned} \widetilde{F}(x+x_0,z) &= (x+x_0+z)^m - (x+x_0)^m - (z+1)^m + 1 \\ &= \sum_{k=2}^{m} \binom{m}{k}(x+z)^k x_0^{m-k} - \sum_{k=2}^{m}\binom{m}{k} x^k x_0^{m-k} - \sum_{k=2}^{m}\binom{m}{k} z^k \end{aligned}$$

$m-1 \equiv 0 \mod p^l$ alors pour tout $k < p^l$, $\binom{m}{k} = 0$.
Calculons le terme de degré $p^l - 1$ de $\widetilde{f}$:

$$\frac{1}{z}\binom{m}{p^l}(x_0^{m-p^l}(x+z)^{p^l} - x_0^{m-p^l}x^{p^l} - z^{p^l}) = \binom{m}{p^l}(x_0^{m-p^l} - 1)z^{p^l-1}$$

donc on a un point singulier de $\widehat{f}$ de multiplicité strictement plus grande que $p^l - 1$ si et seulement si

$$x_0^{m-p^l} = 1 \Leftrightarrow x_0^d = 1.$$

Regardons maintenant le terme de degré p^l de $\widetilde{f}$:

$$\frac{1}{z}\binom{m}{p^l+1}(x_0^{m-p^l-1}(x+z)^{p^l+1} - x_0^{m-p^l-1}x^{p^l+1} - z^{p^l+1})$$
$$= \binom{m}{p^l+1}(x_0^{m-p^l-1}x^{p^l} + x_0^{m-p^l-1}xz^{p^l-1} + (x_0^{m-p^l-1}-1)z^{p^l})$$

or $x_0^{m-p^l-1} \neq 0$ donc les points singuliers de $\widehat{f}$ de multiplicité strictement supérieure à $p^l - 1$ sont de multiplicité p^l.

On a donc démontré le lemme suivant :

Lemme 9 *Si $m \equiv 1 \mod p$, alors $\widehat{h}$ a $\frac{m-1}{p^l}$ points singuliers à l'infini.*
Soit ω tel que $\omega^{\frac{m-1}{p^l}} = 1$, alors le point $(\omega : 1 : 0)$ a pour multiplicité dans $\widehat{h}$:

$$\begin{cases} p^l & \text{si } \omega^d = 1,\ \omega \neq 1 \\ p^l - 1 & \text{sinon} \end{cases}$$

2.2 Singularités affines

On a

$$\begin{cases} f_x &= m(x+1)^{m-1} - mx^{m-1} \\ f_y &= -m(y+1)^{m-1} + my^{m-1} \end{cases}$$

$$(x_0, y_0) \text{ point singulier de } f \Leftrightarrow \begin{cases} f(x_0,y_0) = 0 \\ (x_0+1)^{m-1} = x_0^{m-1} \\ (y_0+1)^{m-1} = y_0^{m-1} \end{cases}$$
$$\Leftrightarrow \begin{cases} x_0^{m-1}(x_0+1) - x_0^m - y_0^{m-1}(y_0+1) + y_0^m = 0 \\ (x_0+1)^{m-1} = x_0^{m-1} \\ (y_0+1)^{m-1} = y_0^{m-1} \end{cases}$$
$$\Leftrightarrow \begin{cases} x_0^{m-1} = y_0^{m-1} \\ (x_0+1)^{m-1} = x_0^{m-1} \\ (y_0+1)^{m-1} = y_0^{m-1} \end{cases}$$

Lemme 10 *Les points singuliers affines de f sont les points vérifiant :*

$$(x_0+1)^{m-1} = x_0^{m-1} = y_0^{m-1} = (y_0+1)^{m-1}.$$

Du lemme 10, on déduit $x_0,\ y_0 \neq 0, -1$.

$$(x_0, y_0) \text{ point singulier de } f \Leftrightarrow \begin{cases} x_0^{\frac{m-1}{p^l}} = y_0^{\frac{m-1}{p^l}} & (1) \\ (x_0+1)^{\frac{m-1}{p^l}} = x_0^{\frac{m-1}{p^l}} & (2) \\ (y_0+1)^{\frac{m-1}{p^l}} = y_0^{\frac{m-1}{p^l}} & (3) \end{cases}$$

Il y a au plus $\frac{m-1}{p^l} - 1$ solutions à l'équation (2).
Soit x_0 une telle solution, on cherche à déterminer le nombre de y_0 tel que (x_0, y_0) soit un point singulier de f.

On écrit $m = 1 + \sum_{j=1}^{b} m_j p^{i_j}$ avec $1 \leq m_j \leq p-1$, $i_j > i_{j-1}$, $i_1 = l$. On a alors :

$$\begin{aligned}
(y_0+1)^{\frac{m-1}{p^l}} = y_0^{\frac{m-1}{p^l}} \quad &\Leftrightarrow \quad \prod_{j=1}^{b} (y_0+1)^{m_j p^{i_j - l}} = y_0^{\frac{m-1}{p^l}} \\
&\Leftrightarrow \quad \sum_{0 \leq k_j \leq m_j}^{*} \left(\prod_{j=1}^{b} \binom{m_j}{k_j} \right) y_0^{\sum_{j=1}^{b} k_j p^{i_j - l}} = 0
\end{aligned}$$

où la somme * est la somme privée de l'indice $(m_1, \ldots, m_b)$.

On multiplie par $y_0^{\frac{m-1}{p^l} - m_b p^{i_b - l}}$ et on pose $\alpha = y_0^{\frac{m-1}{p^l}}$:

$$\sum_{\substack{0 \leq k_j \leq m_j \\ j \neq b}}^{*} \left(\prod_{j=1}^{b-1} \binom{m_j}{k_j} \right) \alpha y_0^{\sum_{j=1}^{b-1} k_j p^{i_j - l}}$$

$$+ \sum_{k_b=0}^{m_b-1} \sum_{\substack{0 \leq k_j \leq m_j \\ j \neq b}} \left(\prod_{j=1}^{b} \binom{m_j}{k_j} \right) y_0^{\frac{m-1}{p^l} - (m_b - k_b) p^{i_b - l} + \sum_{j=1}^{b-1} k_j p^{i_j - l}} = 0$$

Le degré de ce polynôme en y_0 est
$\frac{m-1}{p^l} - p^{i_b - l} + \sum_{j=1}^{b-1} m_j p^{i_j - l} = 2\frac{m-1}{p^l} - (m_b+1)p^{i_b - l}$

Lemme 11 *Le nombre de singularités affines de h est au plus*

$$\left(\frac{m-1}{p^l} - 1 \right) \left(2\frac{m-1}{p^l} - (m_b+1)p^{i_b - l} \right)$$

où $m = 1 + \sum_{j=1}^{b} m_j p^{i_j}$ *avec* $1 \leq m_j \leq p-1$, $i_j > i_{j-1}$, $i_1 = l$.

On étudie la multiplicité de ces singularités :

$$\begin{aligned}
f(x+x_0, y+y_0) &= (x+x_0+1)^m - (x+x_0)^m - (y+y_0+1)^m + (y+y_0)^m \\
&= \sum_{k=2}^{m} \binom{m}{k} x^k (x_0+1)^{m-k} - \sum_{k=2}^{m} x^k x_0^{m-k} \\
&\qquad - \sum_{k=2}^{m} \binom{m}{k} y^k (y_0+1)^{m-k} + \sum_{k=2}^{m} y^k y_0^{m-k}
\end{aligned}$$

$m - 1 \equiv 0 \mod p^l$ donc, pour tout $2 \leq k < p^l$, $\binom{m}{k} = 0$ et (x_0, y_0) est une singularité de multiplicité au moins p^l.
Regardons maintenant le terme de degré $p^l + 1$:

$$\binom{m}{p^l+1} (((x_0+1)^{m-p^l-1} - x_0^{m-p^l-1}) x^{p^l+1} - ((y_0+1)^{m-p^l-1} - y_0^{m-p^l-1}) y^{p^l+1})$$

Or (x_0, y_0) est un point singulier de f donc $(x_0+1)^{m-1} = x_0^{m-1}$ et $x_0 \neq -1, 0$ donc

$$\begin{aligned}(x_0+1)^{m-p^l-1} - x_0^{m-p^l-1} = 0 \quad &\Leftrightarrow \quad (x_0+1)^{p^l}((x_0+1)^{m-p^l-1} - x_0^{m-p^l-1}) = 0 \\ &\Leftrightarrow \quad -x_0^{m-p^l-1} = 0\end{aligned}$$

donc les singularités sont de multiplicité au plus $p^l + 1$.

Considérons maintenant le terme de degré p^l :

$$\binom{m}{p^l}(((x_0+1)^{m-p^l} - x_0^{m-p^l})x^{p^l} - ((y_0+1)^{m-p^l} - y_0^{m-p^l})y^{p^l})$$

$$\begin{aligned}(x_0+1)^{m-p^l} - x_0^{m-p^l} = 0 \quad &\Leftrightarrow \quad (x_0+1)^{p^l}((x_0+1)^{m-p^l} - x_0^{m-p^l}) = 0 \\ &\Leftrightarrow \quad (x_0+1)^{m-1}(x_0+1) - x_0^m - x_0^{m-p^l} = 0 \\ &\Leftrightarrow \quad x_0^{m-p^l}(x_0^{p^l-1} - 1) = 0 \\ &\Leftrightarrow \quad x_0 \in \mathbb{F}_{p^l}^*\end{aligned}$$

On peut procéder de même pour y_0.

Lemme 12 *Si $m \equiv 1 \mod p$, il y a au plus :*

- $d-1$ *singularités affines de h telles que $x_0 = y_0 \in \mathbb{F}_{p^l}^*$. Elles sont de multiplicités p^l (p^l+1 pour f).*
- $\frac{m-1}{p^l} - d$ *singularités affines de h telles que $x_0 = y_0 \notin \mathbb{F}_{p^l}^*$. Elles sont de multiplicité $p^l - 1$ (p^l pour f).*
- $(d-1)(d-2)$ *singularités affines de h telles que $x_0 \neq y_0$ et x_0, $y_0 \in \mathbb{F}_{p^l}^*$. Elles sont de multiplicité $p^l + 1$ (pour h et pour f).*
- $\left(\frac{m-1}{p^l} - 1\right)\left(2\frac{m-1}{p^l} - (m_b+1)p^{i_b-l} - 1\right) - (d-1)(d-2)$ *singularités affines de h tel que $x_0 \neq y_0$ et x_0 ou $y_0 \notin \mathbb{F}_{p^l}^*$. Elles sont de multiplicité p^l (pour f et h)*

3 Majoration du nombre d'intersection

On écrit $h = uv$; on cherche à majorer le nombre d'intersection $I_t(u, v)$ où t est une singularité de h.

3.1 Point singulier à l'infini

Soit $t = (\omega : 1 : 0)$ un point singulier de h à l'infini, $\omega^{\frac{m-1}{p^l}} = 1$. On écrit $\widetilde{h}(x+\omega, z) = \widetilde{H}_{m_t} + \widetilde{H}_{m_t+1} + \ldots$ où m_t est la multiplicité de t et $\widetilde{H}_i$ est le polynôme homogène de degré i composé des termes de degré i de $\widetilde{h}(x+\omega, z)$.

$$\begin{aligned}\widetilde{f}(x+\omega, z) &= \widetilde{h}(x+\omega, z)(x+\omega-1) \\ &= (R + \widetilde{H}_{m_t+1} + \widetilde{H}_{m_t})(x+\omega-1) \\ &\qquad \text{où } R \text{ est un polynôme de degré supérieur à } m_t+2 \\ &= xR + (\omega-1)R + x\widetilde{H}_{m_t} + (\omega-1)\widetilde{H}_{m_t+1} + (\omega-1)\widetilde{H}_{m_t}\end{aligned}$$

donc

· Si $\omega \neq 1$, on a $\widetilde{F}_{m_t} = (\omega - 1)\widetilde{H}_{m_t}$ et $\widetilde{F}_{m_t+1} = x\widetilde{H}_{m_t} + (\omega - 1)\widetilde{H}_{m_t+1}$
· Si $\omega = 1$, $\widetilde{F}_{m_t+1} = x\widetilde{H}_{m_t}$

Lemme 13 *Pour $m \equiv 1 \mod p$, si $t = (\omega : 1 : 0)$, $\omega^{\frac{m-1}{p^l}} = 1$, est un point singulier à l'infini de h de multiplicité m_t alors*
· *Si $\omega \neq 1$, on a $\widetilde{F}_{m_t} = (\omega - 1)\widetilde{H}_{m_t}$ et $\widetilde{F}_{m_t+1} = x\widetilde{H}_{m_t} + (\omega - 1)\widetilde{H}_{m_t+1}$*
· *Si $\omega = 1$, $\widetilde{F}_{m_t+1} = x\widetilde{H}_{m_t}$*

Corollaire 14 *Si $t = (1 : 1 : 0)$ alors*

$$I_t(u, v) \leq \left(\frac{p^l - 1}{2}\right)^2$$

Preuve : Si $t = (1 : 1 : 0)$ alors il a pour multiplicité $p^l - 1$. Par le lemme 13, $\widetilde{H}_{m_t} = a(x^{p^l-1} + z^{p^l-1})$, tous ses facteurs sont différents donc $I_t(u, v) = m_t(u)m_t(v)$. De plus $m_t(u) + m_t(v) = p^l - 1$ d'où le résultat.

□

Corollaire 15 *Si $t = (\omega : 1 : 0)$ tel que $\omega^d = 1$, $\omega \neq 1$ alors*

$$I_t(u, v) \leq \frac{p^{2l} - 1}{4}$$

Preuve : t est de multiplicité p^l. Par le lemme 13, on a

$$(\omega - 1)\widetilde{H}_{p^l} = \widetilde{F}_{p^l} = x^{p^l}\omega^{m-p^l-1} + xz^{p^l-1}\omega^{m-p^l-1} + (\omega^{m-p^l-1} - 1)z^{p^l}.$$

Donc $\widetilde{H}_{p^l}$ n'a que des facteurs simples et $I_t(u, v) = m_t(u)m_t(v)$. Comme $m_t(u) + m_t(v) = p^l$, on a le résultat.

□

Corollaire 16 *Si $t = (\omega : 1 : 0)$ avec $\omega^{\frac{m-1}{p^l}}$, $\omega^d \neq 1$, on a*

$$I_t(u, v) = 0$$

Preuve : t est de multiplicité $p^l - 1$. Par le lemme 13, $(\omega - 1)\widetilde{H}_{p^l-1} = \widetilde{F}_{p^l-1} = \alpha z^{p^l-1}$. De plus, on a $\mathrm{pgcd}(\widetilde{H}_{p^l}, \widetilde{H}_{p^l-1}) = \mathrm{pgcd}(\widetilde{F}_{p^l}, \widetilde{F}_{p^l-1})$ et $\widetilde{F}_{p^l} = x^{p^l}\omega^{m-p^l-1} + xz^{p^l-1}\omega^{m-p^l-1} + z^{p^l}(\omega^{m-1-p^l} - 1)$, donc z ne divise pas $\widetilde{F}_{p^l}$ et par le lemme 1 de [5], $I_t(u, v) = 0$.

□

3.2 Point singulier affine

On écrit $h(x + x_0, y + y_0) = H_{m_t} + H_{m_t+1} + \ldots$ où m_t est la multiplicité de t et H_i est le polynôme homogène de degré i composé des termes de degré i de $h(x + x_0, y + y_0)$
On appelle ici tangentes à h en t les facteurs de H_{m_t}.

Soit $t = (x_0, y_0)$ un point singulier affine de h de multiplicité m_t tel que $x_0 = y_0$.

$$\begin{aligned} f(x+x_0, y+y_0) &= h(x+x_0, y+y_0)(x+x_0-y-y_0) \\ &= (R + H_{m_t+1} + H_{m_t})(x-y) \\ &\qquad \text{où } R \text{ est un polynôme de degré supérieur à } m_t+2 \\ &= (x-y)R + (x-y)H_{m_t+1} + (x-y)H_{m_t} \\ &= F_{m_t+1} + F_{m_t+2} + \dots \end{aligned}$$

On a donc $F_{m_t+2} = (x-y)H_{m_t+1}$ et $F_{m_t+1} = (x-y)H_{m_t}$ et F_{m_t+1} est de la forme $a(x^{m_t+1} - y^{m_t+1})$ (*cf.* preuve du lemme 12).

Lemme 17 *Pour $t = (x_0, y_0)$ point singulier affine de h de multiplicité m_t tel que $x_0 = y_0$ on a :*
$F_{m_t+2} = (x-y)H_{m_t+1}$ et $F_{m_t+1} = (x-y)H_{m_t}$.
De plus les tangentes à h en t sont les facteurs de $\frac{x^{m_t+1}-y^{m_t+1}}{x-y}$.

Corollaire 18 *Pour $m \equiv 1 \mod p$, les singularités affines de h, $t = (x_0, y_0)$ telles que $x_0 = y_0 \in \mathbb{F}_{p^l}^*$ vérifient*

$$I_t(u,v) \leq \frac{p^{2l}-1}{4}.$$

Preuve : La multiplicité de t pour h est p^l. Les facteurs de $\frac{x^{p^l+1}-y^{p^l+1}}{x-y}$ étant tous distincts, par le lemme 17, u, v n'ont pas de tangente commune donc $I_t(u,v) = m_t(u)m_t(v)$. On a de plus $m_t(u) + m_t(v) = p^l$ d'où $m_t(u)m_t(v) \leq \frac{p^{2l}-1}{4}$, ce qui donne le résultat.

□

Corollaire 19 *Pour $m \equiv 1 \mod p$, les singularités affines de h, $t = (x_0, y_0)$, $x_0 = y_0 \notin \mathbb{F}_{p^l}^*$ vérifient*

$$I_t(u,v) = 0.$$

Preuve : t est de multiplicité $p^l - 1$. Par le lemme 17, on a $H_{p^l-1} = a(x-y)^{p^l-1}$ et $\text{pgcd}(H_{p^l-1}, H_{p^l}) = \text{pgcd}\left(\frac{F_{p^l-1}}{x-y}, \frac{F_{p^l}}{x-y}\right)$. Or $F_{p^l+1} = b(x^{p^l+1} - y^{p^l+1})$, d'où $\text{pgcd}(H_{p^l-1}, H_{p^l}) = 1$. Par le lemme 1 de [5], on a donc $I_t(u,v) = 0$

□

Soit $t = (x_0, y_0)$ un point singulier affine de h tel que $x_0 \neq y_0$, de multiplicité m_t.

$$\begin{aligned} f(x+x_0, y+y_0) &= h(x+x_0, y+y_0)(x+x_0-y-y_0) \\ &= (R + H_{m_t+1} + H_{m_t})(x+x_0-y-y_0) \\ &\qquad \text{où } R \text{ est un polynôme de degré supérieur à } m_t+2 \\ &= (x_0-y_0)H_{m_t} + ((x-y)H_{m_t} + (x_0-y_0)H_{m_t+1}) \\ &\qquad\qquad +((x-y+x_0-y_0)R + (x-y)H_{m_t+1}) \\ &= F_{m_t} + F_{m_t+1} + R' \\ &\qquad \text{où } R' \text{ est un polynôme de degré supérieur à } m_t+2. \end{aligned}$$

On a donc $F_{m_t} = (x_0-y_0)H_{m_t}$ et $F_{m_t+1} = (x_0-y_0)H_{m_t+1} + (x-y)H_{m_t}$.

Lemme 20 *Si $t = (x_0, y_0)$ est un point singulier affine de h de multiplicité m_t tel que $x_0 \neq y_0$ alors*

$$\mathbb{F}_{m_t} = (x_0 - y_0)H_{m_t} \text{ et } F_{m_t+1} = (x-y)H_{m_t} + (x_0 - y_0)H_{m_t+1}.$$

Corollaire 21 *Pour $m \equiv 1 \mod p$, si $t = (x_0, y_0)$ est un point singulier affine de h tel que $x_0 \neq y_0$, x_0, $y_0 \in \mathbb{F}_{p^l}^*$ alors*

$$I_t(u,v) \leq \left(\frac{p^l+1}{2}\right)^2.$$

Preuve : t est de multiplicité $p^l + 1$. Par le lemme 20,
$(x_0 - y_0)H_{m_t} = F_{m_t} = c_1 x^{p^l+1} - c_2 y^{p^l+1}$, avec c_1, $c_2 \neq 0$. On en déduit que H_{m_t} n'a que des facteurs simples, puis que $I_t(u,v) = m_t(u)m_t(v)$. Comme $m_t(u) + m_t(v) = p^l + 1$, on a le résultat.

□

Corollaire 22 *Pour $m \equiv 1 \mod p$, si $t = (x_0, y_0)$ est un point singulier affine de h tel que $x_0 \neq y_0$ et $x_0 \in \mathbb{F}_{p^l}^*$ et $y_0 \notin \mathbb{F}_{p^l}^*$ ou $x_0 \notin \mathbb{F}_{p^l}^*$ et $y_0 \in \mathbb{F}_{p^l}^*$ alors*

$$I_t(u,v) = 0$$

Preuve : t est de multiplicité p^l.
$(x_0 - y_0)H_{p^l} = F_{p^l} = \begin{cases} c_1 x^{p^l} & \text{si } y_0 \in \mathbb{F}_{p^l}^*,\ c_1 \neq 0 \\ c_2 y^{p^l} & \text{si } x_0 \in \mathbb{F}_{p^l}^*,\ c_2 \neq 0 \end{cases}$
$F_{p^l+1} = c_1' x^{p^l+1} - c_2' y^{p^l+1}$, c_1', $c_2' \neq 0$, donc, par le lemme 20,
$1 = \text{pgcd}(F_{p^l}, F_{p^l+1}) = \text{pgcd}(H_{p^l}, H_{p^l+1})$. Par le lemme 1 de [5], $I_t(u,v) = 0$.

□

Si $m \equiv 1 \mod p$, soit $t = (x_0, y_0)$ un point singulier affine de h tel que $x_0 \neq y_0$ et x_0 et $y_0 \notin \mathbb{F}_{p^l}$, t est de multiplicité p^l.
De plus $F_{p^l} = c_1 x^{p^l} - c_2 y^{p^l} = (c_3 x - c_4 y)^{p^l}$, où $c_1 = (x_0+1)^{m-p^l} - x_0^{p^l} \neq 0$, $c_2 = (y_0+1)^{m-p^l} - y_0^{m-p^l} \neq 0$ car x_0, $y_0 \notin \mathbb{F}_{p^l}^*$.
Par le lemme 20, on a $F_{p^l} = (x_0 - y_0)H_{p^l}$ et $F_{p^l+1} = (x_0 - y_0)H_{p^l+1} + (x-y)H_{p^l}$ donc H_{p^l} n'a qu'un facteur et $\text{pgcd}(F_{p^l}, F_{p^l+1}) = \text{pgcd}(H_{p^l}, H_{p^l+1})$.
$F_{p^l+1} = d_1 x^{p^l+1} - d_2 y^{p^l+1}$ avec $d_1 = (x_0+1)^{m-p^l-1} - x_0^{m-p^l-1} \neq 0$ et $d_2 = (y_0+1)^{m-p^l-1} - y_0^{m-p^l-1} \neq 0$.
Les polynômes F_{p^l} et F_{p^l+1} ont un facteur commun si et seulement si $c_3 x - c_4 y$ divise F_{p^l+1} ; F_{p^l} et F_{p^l+1} ont donc un facteur commun si et seulement si

$$\left(\frac{c_1}{c_2}\right)^{p^l+1} = \left(\frac{d_1}{d_2}\right)^{p^l}.$$

Si (x_0, y_0) est un point singulier, on a :

$$\begin{cases} x_0^{m-1} = y_0^{m-1} \\ (x_0+1)^{m-1} = x_0^{m-1} \\ (y_0+1)^{m-1} = y_0^{m-1} \end{cases}$$

On a :

$$\begin{aligned} d_1 = (x_0+1)^{m-p^l-1} - x_0^{m-p^l-1} &= \frac{(x_0+1)^{m-1} - x_0^{m-p^l-1}(x_0+1)^{p^l}}{(x_0+1)^{p^l}} \\ &= \frac{x_0^{m-1} - x_0^{m-1} - x_0^{m-p^l-1}}{(x_0+1)^{p^l}} \\ &= \frac{-x_0^{m-p^l-1}}{(x_0+1)^{p^l}} \end{aligned}$$

De même, $d_2 = \frac{-y_0^{m-p^l-1}}{(y_0+1)^{p^l}}$.
D'où $\frac{d_1}{d_2} = \frac{x_0^{m-p^l-1}(y_0+1)^{p^l}}{y_0^{m-p^l-1}(x_0+1)^{p^l}} = \frac{x_0^{m-1}y_0^{p^l}(y_0+1)^{p^l}}{y_0^{m-1}x_0^{p^l}(x_0+1)^{p^l}} = \frac{y_0^{p^l}(y_0+1)^{p^l}}{x_0^{p^l}(x_0+1)^{p^l}}$

On a d'autre part :

$$\begin{aligned} c_1 = (x_0+1)^{m-p^l} - x_0^{m-p^l} &= \frac{(x_0+1)(x_0+1)^{m-1} - x_0^{m-p^l}(x_0+1)^{p^l}}{(x_0+1)^{p^l}} \\ &= \frac{x_0^m + x_0^{m-1} - x_0^m - x_0^{m-p^l}}{(x_0+1)^{p^l}} \\ &= \frac{x_0^{m-p^l}(x_0^{p^l-1} - 1)}{(x_0+1)^{p^l}} \end{aligned}$$

De même, $c_2 = \frac{y_0^{m-p^l}(y_0^{p^l-1}-1)}{(y_0+1)^{p^l}}$.
D'où $\frac{c_1}{c_2} = \frac{x_0^{m-p^l}(x_0^{p^l-1}-1)(y_0+1)^{p^l}}{y_0^{m-p^l}(y_0^{p^l-1}-1)(x_0+1)^{p^l}} = \frac{y_0^{p^l}(y_0+1)^{p^l}(x_0^{p^l-1}-1)}{x_0^{p^l}(x_0+1)^{p^l}(y_0^{p^l-1}-1)}$
Après simplification, on obtient que F_{p^l} et F_{p^l+1} ont un facteur commun si et seulement si

$$y_0(x_0+1)^{p^l}(y_0^{p^l-1}-1)^{p^l+1} = x_0(y_0+1)^{p^l}(x_0^{p^l-1}-1)^{p^l+1} \qquad (*)$$

Si (x_0, y_0) n'est pas solution de $(*)$, alors $\mathrm{pgcd}(H_{p^l}, H_{p^l+1}) = 1$ et par le lemme 1 de [5], $I_t(u,v) = 0$.

Sinon on écrit $u(x+x_0, y+y_0) = U_r + U_{r+1} + \ldots$, avec $U_r \neq 0$
et $v(x+x_0, y+y_0) = V_s + V_{s+1} + \ldots$, avec $V_s \neq 0$.
Si r ou $s = 0$ alors u ou v ne contient pas t et $I_t(u,v) = 0$.
Supposons r, $s > 0$. Comme (x_0, y_0) vérifie $(*)$, F_{p^l} et F_{p^l+1}ont un facteur commun que l'on notera e. On a $H_{p^l} = U_r V_s = e^{p^l}$ et $H_{p^l+1} = U_r V_{s+1} + U_{r+1} V_s$. On a de plus $\mathrm{pgcd}(F_{p^l}, F_{p^l+1}) = e$ et donc $\mathrm{pgcd}(H_{p^l}, H_{p^l+1}) = e$. Comme $r \geq 1$ et $s \geq 1$, e divise U_r et V_s et donc $\mathrm{pgcd}(U_r, V_s)$. Si $\mathrm{pgcd}(U_r, V_s) = e^k$, e^k divise $\mathrm{pgcd}(H_{p^l}, H_{p^l+1})$ donc $\mathrm{pgcd}(U_r, V_s) = e$.
On peut supposer, sans perte de généralité, que $U_r = e^{p^l-1}$ et $V_s = e$; t est un point simple de v donc par [3], $I_t(u,v) = \mathrm{ord}_t^v(u)$; e^2 ne divisant pas H_{p^l+1}, e ne divise pas U_{p^l}, on peut donc écrire U_{p^l} comme produit de p^l facteurs linéaires différents de e. Chaque facteur linéaire n'est pas tangent à v, donc l'ordre de chaque facteur est 1, d'où l'ordre de U_{p^l} est p^l. On a donc $\mathrm{ord}_t^v(u) \leq p^l$.

Lemme 23 *Pour $m \equiv 1 \mod p$, si $t = (x_0, y_0)$ est un point singulier affine de h tel que $x_0 \neq y_0$ et x_0 et $y_0 \notin \mathbb{F}_{p^l}^*$ alors*

- *si $y_0(x_0+1)^{p^l}(y_0^{p^l-1}-1)^{p^l+1} \neq x_0(y_0+1)^{p^l}(x_0^{p^l-1}-1)^{p^l+1}$, $I_t(u,v) = 0$*
- *sinon $I_t(u,v) \leq p^l$ et il y a au plus $((p^l-2)(p^l+1)-1)(\frac{m-1}{p^l}-1)$ tels points singuliers.*

4 Preuve du théorème 6

Lemme 24 *Si h n'a pas de facteur absolument irréductible alors il existe une factorisation de $h = uv$ telle que*

$$\sum_t I_t(u,v) \geq 2\frac{\deg(h)^2}{9}.$$

Autrement dit , si I_{tot} est un majorant du nombre d'intersection global,

$$e = \frac{I_{tot}}{\frac{\deg(h)^2}{4}} \geq \frac{8}{9}.$$

Preuve : Supposons que h se factorise sur $\mathbb{F}_p$. Comme $h = e_i \dots e_r$, où chaque e_i est irréductible sur $\mathbb{F}_p$ mais pas absolument irréductible. Chaque e_i se factorise alors en $c_i \geq 2$ facteurs sur une clôture algébrique de $\mathbb{F}_p$ et chacun des ces facteurs est de degré $\frac{\deg(e_i)}{c_i}$.
On factorise maintenant chaque facteur e_i en 2 polynômes u_i, v_i tels que $\deg(u_i) = \deg(v_i)$ si c_i est pair et $\deg(u_i) = \deg(v_i) + \frac{\deg(e_i)}{c_i}$ si c_i est impair (donc $c_i \geq 3$).
On pose $u = \prod_{i=1}^{r} u_i$ et $v = \prod_{i=1}^{r} v_i$.
On a alors $\deg(u) - \deg(v) \leq \frac{\deg(h)}{3}$. Comme de plus $\deg(u) + \deg(v) = \deg(h)$, on a

$$\deg(u)\deg(v) \geq \frac{8}{9}\frac{\deg(h)^2}{4}$$

Soit I_{tot} un majorant du nombre d'intersection global pour tout u, v. Alors par le théorème de Bézout on a

$$I_{tot} \geq \sum_t I_t(u,v) \geq \deg(u)\deg(v) \geq \frac{8}{9}\frac{\deg(h)^2}{4} = 2\frac{\deg(h)^2}{9}$$

□

Les théorèmes suivants pemettent de démontrer le théorème 6, on suppose jusqu'à la fin que $m \neq 1 + p^l$.

Théorème 25 *Si $d = 1$, h a un facteur absolument irréductible sur $\mathbb{F}_p$.*

Preuve : Supposons que h n'ait pas de facteur absolument irréductible, alors par le lemme 24, on doit avoir $e = \frac{I_{tot}}{\frac{(m-2)^2}{4}} \geq \frac{8}{9}$, où I_{tot} est un majorant du nombre d'intersection global.

Comme $d = 1$, il n'existe que des singularités de type Ib, IIc, IIIa et IIIc (*cf.* tableau 1). On a donc

$$\sum_t I_t(u,v) \leq p^l \left(\frac{m-1}{p^l} - 1\right)\left(2\frac{m-1}{p^l} - (m_b+1)p^{i_b - l} - 1\right) + \left(\frac{p^l-1}{2}\right)^2 \tag{2}$$

Or $m = 1 + p^l k$ et $m \neq 1 + p^l$ donc $k \geq 2$, on a alors $\frac{m-3}{4} = \frac{p^k k - 2}{4} \geq \frac{p^l - 1}{2}$ d'où

$$\begin{aligned} e &\leq \frac{1}{\frac{(m-2)^2}{4}}\left(\frac{(m-3)^2}{16} + p^l(\frac{m-1}{p^l} - 1)^2\right) \\ &\leq \frac{1}{4} + \frac{4}{p^l} \end{aligned}$$

donc pour $p^l \neq 3$ ou 5, on a $e < \frac{8}{9}$ ce qui est absurde.

Regardons d'abord le cas où $p^l = 3$, $1 = d = \text{pgcd}(2,k)$ donc k est impair et non divisible par 3 par définition de l. D'où $k \geq 5$, on a alors

$$\begin{aligned} e &\leq \frac{p^l((p^l-2)(p^l+1)-1)(\frac{m-1}{p^l}-1) + \left(\frac{p^l-1}{2}\right)^2}{\frac{(m-2)^2}{4}} = \frac{9(k-1)+1}{\frac{(3k-1)^2}{4}} \\ &\leq \frac{4}{k-\frac{1}{3}} + \frac{4}{(3k-1)^2} \\ &\leq \frac{12}{14} + \frac{1}{49} < \frac{8}{9} \end{aligned}$$

ce qui est absurde.

Si $p^l = 5$, $1 = d = \text{pgcd}(4,k)$ et k est impair, d'où $k = 3$ ou $k \geq 7$.
Comme pour le cas $p^l = 3$, on a $e \leq \frac{68}{5}\frac{k-1}{(k-\frac{1}{5})^2} + \frac{16}{(5k-1)^2}$.
Or comme $\frac{68}{5}\frac{k-1}{(k-\frac{1}{5})^2} + \frac{16}{(5k-1)^2}$ est une fonction décroissante de k, pour $k \geq 17$ on a $e < \frac{8}{9}$ ce qui est absurde.
Il reste à traiter les cas où $k = 3$, 7, 9, 11, 13.
En reprenant l'équation (2), on a

k	3	7	9	11	13
m	16	36	46	56	66
I_{tot}	24	124	324	354	664
e	$\frac{24}{7^2}$	$\frac{124}{17^2}$	$\frac{324}{22^2}$	$\frac{354}{27^2}$	$\frac{664}{32^2}$

Dans tous les cas, on a $e < \frac{8}{9}$ ce qui est absurde.

□

Théorème 26 *Si $1 < d < \frac{m-1}{p^l}$, h a un facteur absolument irréductible sur $\mathbb{F}_p$*

Preuve : Supposons que h n'ait pas de facteur absolument irréductible, alors par le lemme 24, on doit avoir $e = \frac{I_{tot}}{\frac{(m-2)^2}{4}} \geq \frac{8}{9}$, où I_{tot} est un majorant du

nombre d'intersection global. On a alors

$$\begin{aligned}\sum_t I(u,v) \leq\ & \frac{p^{2l}-1}{4}(d-1)+\left(\frac{p^l-1}{2}\right)^2 \\ & +p^l\left((\frac{m-1}{p^l}-1)(2\frac{m-1}{p^l}-(m_b+1)p^{i_b-l}-1)-(d-1)(d-2)\right) \\ & +\left(\frac{p^l+1}{2}\right)^2(d-1)(d-2)+(d-1)\frac{p^{2l}-1}{4} \\ \leq\ & \frac{p^{2l}-1}{2}(d-1)+\left(\frac{p^l-1}{2}\right)^2(d-1)(d-2) \\ & +p^l\left(\frac{m-1}{p^l}-1\right)^2+\left(\frac{p^l-1}{2}\right)^2\end{aligned}$$

Or $m=1+kp^l$ avec $k\neq 1$ car $m\neq 1+p^l$ et $k\not\equiv 0 \mod p$ par définition de l. De plus, d divise $k=\frac{m-1}{p^l}$ et $d<k$ donc $d\leq\frac{m-1}{2p^l}$ d'où

$$\begin{aligned} e &\leq \frac{2(p^{2l}-1)(\frac{k}{2}-1)+(p^l-1)^2(\frac{k}{2}-1)(\frac{k}{2}-2)+4p^l(k-1)^2+(p^l-1)^2}{(p^lk-1)^2} \\ &\leq \frac{1}{\left(k-\frac{1}{p^l}\right)^2}\left((1-\frac{1}{p^{2l}})(k-2)+\frac{1}{4}(1-\frac{1}{p^l})^2(k-2)(k-4)\right. \\ &\qquad\qquad \left.+\frac{4}{p^l}(k-1)^2+(1-\frac{1}{p^l})^2\right) \\ e &\leq \frac{1}{k-\frac{1}{p^l}}+\frac{1}{4}+\frac{4}{p^l}+\frac{1}{\left(k-\frac{1}{p^l}\right)^2}\end{aligned}$$

Comme on doit avoir $e\geq\frac{8}{9}$, $1<d<k$ et $\mathrm{pgcd}(k,p)=1$, les seules possibilités restantes sont :

k	4	6	8	9	10	12	14	15	≥ 16
p^l	$3,7,11$	5	$3,5,7$	7	$3,7$	$5,7$	$3,5$	7	$3,5$

On a d'une part

$$\begin{aligned} e \leq\ & \frac{2(p^{2l}-1)(d-1)+(p^l+1)^2(d-1)(d-2)}{(p^lk-1)^2} \\ & +\frac{4p^l(k-1)\left((p^l-2)(p^l+1)-1\right)+(p^l-1)^2}{(p^lk-1)^2}\end{aligned} \tag{3}$$

et d'autre part

$$\begin{aligned} e \leq\ & \frac{2(p^{2l}-1)(d-1)+(p^l-1)^2(d-1)(d-2)}{(p^lk-1)^2} \\ & +\frac{4p^l(k-1)(2k-(m_b+1)p^{i_b-l}-1)+(p^l-1)^2}{(p^lk-1)^2}\end{aligned} \tag{4}$$

Considérons d'abord le cas $k\geq 16$. Dans l'inéquation (3), e est majoré par une fonction décroissante de k. On ne va donc considérer que le cas $k=16$. Si $p^l=3$

ou $p^l = 5$, on obtient alors $e < \frac{8}{9}$. Contradiction.
Ensuite, en utilisant soit l'inégalité (3), soit l'inégalité (4), on a dans tous les autres cas du tableau $e < \frac{8}{9}$, ce qui est absurde.

□

Théorème 27 *Si $d = \frac{m-1}{p^l} \neq p^l - 1$ alors h a un facteur absolument irréductible sur $\mathbb{F}_p$*

Preuve : On remarque d'abord que, comme $d = \frac{m-1}{p^l}$, il n'existe que des singularités de type Ia, IIa, IIa, IIIb (*cf.* tableau 1). Dans tous les cas, H_{m_t} n'a que des facteurs simples et donc quelque soit la factorisation $h = uv$, on a $I_t(u,v) = m_t(u)m_t(v)$. Comme $\frac{m-1}{p^l} \neq p^l - 1$, on a $\frac{m-1}{p^l} \leq \frac{p^l-1}{2}$.
Supposons maintenant que h n'ait pas de facteur absolument irréductible sur $\mathbb{F}_p$, alors on écrit $h = h_1 \dots h_r$ où chaque h_i se décompose en $c_i \geq 2$ facteurs de degré $\frac{\deg(h_i)}{c_i}$ sur une clôture algébrique de $\mathbb{F}_p$. On écrit $h_i = h_{i,1} \dots h_{i,c_i}$.

$$\begin{aligned} A &= \sum_{k=1}^{r} \sum_{1 \leq i < j \leq c_k} \sum_t I_t(h_{k,i}, h_{k,j}) + \sum_{1 \leq k < l \leq r} \sum_{\substack{1 \leq i \leq c_k \\ 1 \leq j \leq c_l}} \sum_t I_t(h_{k,i}, h_{l,j}) \\ &= \sum_{k=1}^{r} \sum_{1 \leq i < j \leq c_k} \sum_t m_t(h_{k,i}) m_t(h_{k,j}) + \sum_{1 \leq k < l \leq r} \sum_{\substack{1 \leq i \leq c_k \\ 1 \leq j \leq c_l}} \sum_t m_t(h_{k,i}) m_t(h_{l,j}) \end{aligned}$$

or

$$\begin{aligned} (m_t(h))^2 &= \left(\sum_{k=1}^{r} m_t(h_k) \right)^2 \\ &= \sum_{k=1}^{r} m_t(h_k)^2 + 2 \sum_{1 \leq k < l \leq r} m_t(h_k) m_t(h_l) \\ &= \sum_{k=1}^{r} m_t(h_k)^2 + 2 \sum_{1 \leq k < l \leq r} \sum_{\substack{1 \leq i \leq c_k \\ 1 \leq j \leq c_l}} m_t(h_{k,i}) m_t(h_{l,j}) \end{aligned}$$

d'où, en utilisant le lemme 17 de [4] (qui reste valable dans $\mathbb{F}_p$), on a :

$$A \leq \sum_t \left(\sum_{k=1}^{r} m_t(h_k)^2 \frac{c_k - 1}{2c_k} + \frac{1}{2}(m_t(h)^2 - \sum_{k=1}^{r} m_t(h_k)^2) \right)$$

et donc

$$A \leq \frac{1}{2} \sum_t \left(m_t(h)^2 - \sum_{k=1}^{r} \frac{m_t(h_k)^2}{c_k} \right)$$

D'autre part, par le théorème de Bézout, on a aussi

$$\begin{aligned}
A &= \sum_{k=1}^{r} \sum_{1\le i<j\le c_k} \deg(h_{k,i})\deg(h_{k,j}) + \sum_{1\le k<l\le r} \sum_{\substack{1\le i\le c_k\\ 1\le j\le c_l}} \deg(h_{k,i})\deg(h_{l,j}) \\
&= \sum_{k=1}^{r} \frac{\deg(h_k)^2}{c_k^2}\frac{c_k(c_k-1)}{2} + \sum_{1\le k<l\le r} \deg(h_k)\deg(h_l) \\
&= \sum_{k=1}^{r} \deg(h_k)^2 \frac{c_k-1}{2c_k} + \frac{1}{2}\left(\deg(h)^2 - \sum_{k=1}^{r}\deg(h_k)^2\right) \\
&= \frac{1}{2}\left(\deg(h)^2 - \sum_{k=1}^{r}\frac{\deg(h_k)^2}{c_k}\right)
\end{aligned}$$

On en déduit que

$$\deg(h)^2 - \sum_{k=1}^{r}\frac{\deg(h_k)^2}{c_k} \le \sum_t \left(m_t(h)^2 - \sum_{k=1}^{r}\frac{m_t(h_k)^2}{c_k}\right)$$

Puis en utilisant le lemme 17 de [4],

$$\deg(h)^2 - \sum_t m_t(h)^2 \le \sum_{k=1}^{r}\frac{1}{c_k}\left(\deg(h_k)^2 - \sum_t m_t(h_k)^2\right) \le 0$$

On note $k = \frac{m-1}{p^l}$, et on a

$$\begin{aligned}
\deg(h)^2 \le \sum_t m_t(h)^2 &\Leftrightarrow (m-2)^2 \le 2(k-1)p^{2l} \\
&\qquad +(k-1)(k-2)(1+p^l)^2 + (p^l-1)^2 \\
&\Leftrightarrow -(2p^l+1)k^2 + (p^{2l}+4p^l+3)k - (p^{2l}+2p^l+2) \le 0 \\
&\Leftrightarrow k \le 1 \text{ ou } k \ge \frac{p^{2l}+2p^l+2}{2p^l+1}
\end{aligned}$$

or par hypothèse on a $k \ge 2$ ($m \ne 1+p^l$) et $k \le \frac{p^l-1}{2} < \frac{p^{2l}+2p^l+2}{2p^l+1}$ ce qui est absurde.

□

Références

[1] H. Dobbertin, D. Mills, E.N. Müller, A. Pott, W. Willems, *APN functions in odd characteristic*, Discrete mathematics, vol. 267 (2003), p. 95-112.

[2] R.S. Coulter, R.W. Mathews, *Planar functions and plane of Lenz-Barlotti class II*, Design, Codes and Cryptography, vol.10 (1997), p. 167-184.

[3] W. Fulton, *Algebraic Curves*, Benjamin (1969).

[4] F. Hernando, G. McGuire, *Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions* (2009).

[5] D. Jedlicka, *APN monomials over $\mathbb{F}_{2^n}$ for finitely many n*, Finite Fields and their Applications, vol.13, n°4 (2007), p. 1006-1028.

[6] R. Lidl, H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press (2000).