Des. Codes Cryptogr. (2015) 75:281–299
DOI 10.1007/s10623-013-9912-6

Functions which are PN on infinitely many extensions of $\mathbb{F}_p$, p odd

Elodie Leducq

Received: 25 January 2013 / Revised: 16 December 2013 / Accepted: 17 December 2013 /
Published online: 3 January 2014

Abstract Jedlicka, Hernando and McGuire proved that Gold and Kasami functions are the only power mappings which are APN on infinitely many extensions of $\mathbb{F}_2$. For p an odd prime, we prove that the only power mappings $x \mapsto x^m$ such that $m \equiv 1 \mod p$ which are PN on infinitely many extensions of $\mathbb{F}_p$ are those such that $m = 1 + p^l$, l positive integer. As Jedlicka, Hernando and McGuire, we prove that $\frac{(x+1)^m - x^m - (y+1)^m + y^m}{x-y}$ has an absolutely irreducible factor by using Bézout's theorem.

Keywords Exceptional numbers · Perfectly nonlinear functions · Absolutely irreducible polynomial · Singularities

Mathematics Subject Classification 11T71 · 14H20

1 Introduction

In the following, p is a prime number, n a positive integer, $q = p^n$ and $\mathbb{F}_q$ is a finite field with q elements.

Communicated by G. McGuire.

This paper is available on arxiv.org (http://arxiv.org/abs/1006.2610) since June 2010 but publication has been delayed due to unforeseen events.

E. Leducq
Institut de Mathématiques de Jussieu - Paris Rive Gauche, UMR7586, Batiment Sophie Germain, Case 7012, 75205 Paris Cedex 13, France

Present Address:
E. Leducq (✉)
Département de Mathématiques, Batiment 425, Faculté des Sciences d'Orsay, Université Paris-Sud 11, 91405 Orsay Cedex, France
e-mail: elodie.leducq@u-psud.fr

To resist differential cryptanalysis, a function ϕ from $\mathbb{F}_q$ to $\mathbb{F}_q$ used in a bloc cypher like DES has to have a low uniformity, that is to say for all $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$, the equation $\phi(x+a) - \phi(x) = b$ must have few solutions.

In characteristic 2, if $\phi(x+a) + \phi(x) = b$ then $\phi(x+a+a) + \phi(x+a) = b$. So, the functions which resist differential cryptanalysis the most are the following

Definition 1 We say that the function $\phi : \mathbb{F}_q \to \mathbb{F}_q$ is almost perfectly nonlinear (APN) over $\mathbb{F}_q$ if:

$$\forall a, b \in \mathbb{F}_q, a \neq 0, |\{x \in \mathbb{F}_q, \phi(x+a) - \phi(x) = b\}| \leq 2$$

and if, furthermore, there exists a pair (a, b) such that we have equality.

On the contrary, in odd characteristic, $x \mapsto \phi(x+a) - \phi(x)$ can be one to one. So, the functions which resist differential cryptanalysis the most are the following:

Definition 2 If q is odd, a function $\phi : \mathbb{F}_q \to \mathbb{F}_q$ is perfectly nonlinear (PN) over $\mathbb{F}_q$ if for all $b \in \mathbb{F}_q$ and all $a \in \mathbb{F}_q^*$

$$|\{x \in \mathbb{F}_q, \phi(x+a) - \phi(x) = b\}| = 1.$$

In [5,8], Jedlicka, Hernando and McGuire are interested in integers m such that the function $x \mapsto x^m$ is APN on infinitely many extensions of $\mathbb{F}_2$. They prove that the only integers m such that $x \mapsto x^m$ is APN on infinitely many extensions of $\mathbb{F}_2$ are $m = 2^k + 1$ (Gold) and $m = 4^k - 2^k + 1$ (Kasami). They use the fact that a function $x \mapsto x^m$ is APN over $\mathbb{F}_{2^n}$ if and only if the rational points in $\mathbb{F}_{2^n}$ of $(x+1)^m + x^m + (y+1)^m + y^m = 0$ are points such that $x = y$ or $x = y + 1$. This can happen on infinitely many extensions of $\mathbb{F}_p$ only if $\frac{(x+1)^m + x^m + (y+1)^m + y^m}{(x+y)(x+y+1)}$ has no absolutely irreducible factor over $\mathbb{F}_2$.

In this paper, we investigate the case of monomial functions which are PN on infinitely many extensions of $\mathbb{F}_p$ in odd characteristic. From now, we assume that the prime number p is odd. The only known PN power mappings are the following:

Proposition 1 *Let $\phi : x \mapsto x^m$ a power mapping. Then ϕ is PN on $\mathbb{F}_{p^n}$ for*

1. $m = 2$,
2. $m = p^l + 1$ *where l is an integer such that $\frac{n}{\gcd(n,l)}$ is odd [1,2],*
3. $m = \frac{3^l+1}{2}$ *where $p = 3$ and l is an odd integer such that* $\gcd(l, n) = 1$ *[1].*

All these monomials are PN on infinitely many extensions of $\mathbb{F}_p$. In this paper, using the same methods as Jedlicka, Hernando and McGuire, we prove the following theorem:

Theorem 1 *The only $m \equiv 1 \mod p$ such that $x \mapsto x^m$ is PN on infinitely many extensions of $\mathbb{F}_p$ are $m = 1 + p^l$.*

In the case where $m \not\equiv 1 \mod p$, using similar methods, Hernando, McGuire and Monserrat give partial results in [6]. Zieve completes the proof in [11] using a completely different method. However this method does not seem to apply in this case.

In Part 2 of this article, we give some background on algebraic curves and explain how we will prove Theorem 1. In the following parts, we prove Theorem 1.

2 Preliminaries

The notations set in this section hold for the remainder of the article.

2.1 Some background on algebraic curves

A reference for the following results is [4].

Definition 3 A polynomial $f \in \mathbb{F}_q[x, y]$ is said absolutely irreducible if it is irreducible on an algebraic closure of $\mathbb{F}_q$.

If $f \in \mathbb{F}_q[x, y]$ is irreducible over $\mathbb{F}_q$, then its absolutely irreducible factors are conjugate (see [10]).

Definition 4 For $f \in \mathbb{F}_q[x, y]$, we denote by $\widehat{f}$ the homogenized form of f and $\widetilde{f}$ the dehomogenized form of $\widehat{f}$ relatively to y.

Definition 5 Let $t = (x_0, y_0)$ be a point. We write $f(x+x_0, y+y_0) = f_0 + f_1 + \cdots$ where if f_i is non zero then, it is an homogeneous polynomial of degree i. Then, the multiplicity of f in t, denoted by $m_t(f)$ is the smallest i such that $f_i \neq 0$. and the factors of $f_{m_t(f)}$ on an algebraic closure of $\mathbb{F}_q$ are called the tangent lines of f in t.

A singular point of $f \in \mathbb{F}_q[x, y]$ is a point t such that $m_t(f) \geq 2$. In this case, we have $f(t) = 0$ and $\frac{\partial f}{\partial x}(t) = 0 = \frac{\partial f}{\partial y}(t)$.

The intersection number of two plane curves $u = 0$ and $v = 0$ is a number indicating the multiplicity of intersection of these two curves. The intersection number of two plane curves over $\mathbb{F}_q$, $u = 0$ and $v = 0$ at a point t is $\dim_{\mathbb{F}_q}(O_t(\mathbb{A}^2)/(u, v))$ where $O_t(\mathbb{A}^2)$ is the ring of rational functions over the affine plane defined at t. The intersection number of two plane curves $u = 0$ and $v = 0$ at a point t is denoted by $I_t(u, v)$. However, we will not calculate this intersection number using the definition but rather using its properties:

- $I_t(u, v) = 0$ if and only if $m_t(u) = 0$ or $m_t(v) = 0$.
- $I_t(u, v) = m_t(u)m_t(v)$ if and only if u and v have no common tangent lines.
- If $m_t(u) = 1$, then $I_t(u, v) = ord_t^u(v)$ where ord_t^u is the order on the discrete valuation ring $O_t(\mathbb{A}^2)/(u)O_t(\mathbb{A}^2)$.

For more information on intersection numbers, we can read [4, pp. 74–81]

The following lemma is proved in [7]:

Lemma 1 *Let $J(x, y) = 0$ be an affine curve over $\mathbb{F}_q$ and $t = (x_0, y_0)$ be a point of J of multiplicity m_t. Then*

$$J(x + x_0, y + y_0) = J_{m_t} + J_{m_t+1} + \cdots$$

where if J_i is non zero then, it is an homogeneous polynomial of degree i. We write

$$J(x, y) = u(x, y) \cdot v(x, y);$$

if J_{m_t} and J_{m_t+1} are relatively prime then $I_t(u, v) = m_t(u) \cdot m_t(v)$. In this case, if J has only one tangent line at t, then $I_t(u, v) = 0$.

Theorem 2 (Bézout) *Let $u = 0$ and $v = 0$ be two projective plane curves of degree n and m respectively without any common component then*

$$\sum_t I_t(u, v) = n \cdot m.$$

For a proof of this theorem see [4, p. 112]. From this theorem, we deduce the two following lemmas. The second one is proved in [5] for $p=2$ but it is the exact same proof for $p \neq 2$.

Lemma 2 *If $f \in \mathbb{F}_p[x,y]$ has no absolutely irreducible factor over $\mathbb{F}_p$ then there exists a factorization $f = uv$ such that*

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

Equivalently, if I_{tot} is any upper bound on the global intersection number $\sum_t I_t(u,v)$ of u and v for all factorizations of $f = u \cdot v$ over an algebraic closure of $\mathbb{F}_p$, then

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

Proof Suppose that f has no absolutely irreducible factor then, we write $f = e_1 \ldots e_r$, where each e_i is irreducible over $\mathbb{F}_p$, but not absolutely irreducible. Then each e_i factors into $c_i \geq 2$ factors on an algebraic closure of $\mathbb{F}_p$ and its factors are all of degree $\frac{\deg(e_i)}{c_i}$. Now, we factor each e_i into two factors u_i and v_i such that $\deg(u_i) = \deg(v_i) + \frac{\deg(e_i)}{c_i}$ if c_i is odd (thus $c_i \geq 3$) or $\deg(u_i) = \deg(v_i)$ if c_i is even. We set $u = \prod_{i=1}^r u_i$ and $v = \prod_{i=1}^r v_i$. Then $\deg(u) - \deg(v) \leq \frac{\deg(f)}{3}$. Since $\deg(u) + \deg(v) = \deg(f)$,

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

Let I_{tot} be an upper bound on the global intersection number of u and v for all factorizations of f into two factors over the algebraic closure of $\mathbb{F}_p$. Then by Bézout's theorem,

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

□

Lemma 3 *Let $f \in \mathbb{F}_p[x,y]$, f_k, $1 \leq k \leq r$, the irreducible factors of f over $\mathbb{F}_p$ and for all $1 \leq k \leq r$, we write $f_k = f_{k,1} \ldots f_{k,c_k}$ the factorization of f_k into c_k absolutely irreducible factors. Then,*

1. $\deg(f_k)^2 \leq \sum_{t \in Sing(f)} m_t(f_k)^2$ *where $Sing(f)$ is the set of singular points of f.*
2. *If t is a singular point of f, $\sum_{1 \leq i < j \leq c_k} m_t(f_{k,i}) m_t(f_{k,j}) \leq m_t(f_k)^2 \frac{c_k - 1}{2c_k}$.*

2.2 Strategy of proof

An equivalent definition for a PN function is that a function ϕ is PN over $\mathbb{F}_q$ if for all $a \in \mathbb{F}_q^*$, the only rational points in $\mathbb{F}_q$ of

$$\phi(x+a) - \phi(x) - \phi(y+a) + \phi(y) = 0$$

are points such that $x = y$.

In this article, we are only interested in monomial functions, $\phi : x \mapsto x^m$, $m \geq 3$. We only have to consider the case where $a = 1$ in the definition of PN functions (see [3]).

Remark 1 If m is odd then, 0 and -1 are solutions of $(x+1)^m - x^m = 1$. So, in this case, $x \mapsto x^m$ is not PN over $\mathbb{F}_{p^n}$ for any n.

We set $f(x, y) = (x+1)^m - x^m - (y+1)^m + y^m$. Since $(x-y)$ divides $f(x, y)$, we define $h(x, y) = \frac{f(x,y)}{(x-y)}$.

We can assume that $m \not\equiv 0 \mod p$. Indeed, if $x \mapsto x^m$ is PN over $\mathbb{F}_q$ and $m \equiv 0 \mod p$ then $x \mapsto x^{\frac{m}{p}}$ is also PN over $\mathbb{F}_q$.

Then, the proof of Theorem 1 follow from Proposition 2 and Theorem 3 below.

Proposition 2 *If h has an absolutely irreducible factor over* $\mathbb{F}_p$ *then, for n sufficiently large,* $x \mapsto x^m$ *is not PN on* $\mathbb{F}_{p^n}$.

Proof Assume that h has an absolutely irreducible factor over $\mathbb{F}_p$, denoted by Q. If $Q(x, y) = c(x-y)$ with $c \in \mathbb{F}_p^*$, then $f(x, y) = (y-x)^2 \widetilde{Q}(x, y),\ \widetilde{Q} \in \mathbb{F}_p[x, y]$. Hence,

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

So, we get that for all $x \in \mathbb{F}_{p^n}$, $-m(x+1)^{m-1} + mx^{m-1} = 0$ which is impossible since $m \not\equiv 0 \mod p$. Let s be the degree of Q. Since $Q \neq c(x-y)$, $Q(x, x)$ is not the null polynomial. So, there are at most s rational points of Q such that $x = y$.

On the other hand, if we denote by P the number of affine rational points of Q on $\mathbb{F}_{p^n}$, we have (see [9, p. 331]):

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

Hence, for n sufficiently large, Q has a rational point in $\mathbb{F}_{p^n}$ such that $x \neq y$ and $x \mapsto x^m$ is not PN over $\mathbb{F}_{p^n}$. □

Theorem 3 *Let m be an integer such that* $m \geq 3$, $m \equiv 1 \mod p$ *and* $m \neq 1 + p^l$. *Assume that* $\frac{m-1}{p^l} \neq p^l - 1$. *Then h has an absolutely irreducible factor over* $\mathbb{F}_p$.

From now, we are interested in the case where $m \equiv 1 \mod p$. We denote by l the greatest integer such that p^l divides $m-1$ and we set

$$d := \gcd(m-1, p^l - 1) = \gcd\left(\frac{m-1}{p^l}, p^l - 1\right).$$

Then, by Theorem 3 and Proposition 2, we only have to treat the case where $d = \frac{m-1}{p^l} = p^l - 1$ in Theorem 1. We have $m = p^l(p^l - 1) + 1$ which is odd; so $x \mapsto x^m$ is not PN on all extensions of $\mathbb{F}_p$.

Now, we only have to prove Theorem 3. The method of Jedlicka, Hernando and McGuire is, using Bézout's theorem, to prove that h has an absolutely irreducible factor over $\mathbb{F}_p$ because it has not enough singular points. In Part 3, we study singular points of h and their multiplicity. In Part 4, we bound the intersection number $I_t(u, v)$ where t is a singular point of h and $u,\ v$ are such that $h = uv$. In Part 5, we prove Theorem 3.

We set $F = (x+z)^m - x^m - (y+z)^m + y^m = z\widehat{f}$ and $\widetilde{F} = (x+z)^m - x^m - (z+1)^m + 1$ the dehomogenized form of F relatively to y.

3 Singularities of *h*

Proposition 3 *The singular points of h are described in Table 1.*

The proof of this theorem follows from Lemmas 4 to 11 and their corollaries (more precisions are given in the last column of the Table 1).

Table 1 Singularities of h for $m = 1 + \sum_{j=1}^{b} m_j p^{i_j}$ with $1 \le m_j \le p-1$, $i_j > i_{j-1}$, $i_1 = l$

Type	Description	$m_t(h)$	I_t bound	Max number of points	From
Ia	Affine $x_0 = y_0 x_0$, $y_0 \in \mathbb{F}^*_{p^l}$	p^l	$\frac{p^{2l}-1}{4}$	$d-1$	Lemma 7 Corollary 4
Ib	Affine $x_0 = y_0$, x_0, $y_0 \notin \mathbb{F}^*_{p^l}$	$p^l - 1$	0	$\frac{m-1}{p^l} - d$	Lemma 7 Corollary 5
IIa	Affine $x_0 \ne y_0$, x_0, $y_0 \in \mathbb{F}^*_{p^l}$	$p^l + 1$	$\left(\frac{p^l+1}{2}\right)^2$	$(d-1)(d-2)$	Lemma 7 Corollary 6
IIb	Affine $x_0 \ne y_0$, x_0 or $y_0 \notin \mathbb{F}^*_{p^l}$	p^l	0	N_1[a]	Lemma 7 Corollary 7
IIc	Affine $x_0 \ne y_0$, x_0 and $y_0 \notin \mathbb{F}^*_{p^l}$	p^l	p^l[b]	N_2[c]	Lemma 7 Lemma 11
IIIa	$(1:1:0)$	$p^l - 1$	$\left(\frac{p^l-1}{2}\right)^2$	1	Lemma 7 Corollary 1
IIIb	$(\omega : 1 : 0)$, $\omega^d = 1$ and $\omega \ne 1$	p^l	$\frac{p^{2l}-1}{4}$	$d-1$	Lemma 7 Corollary 2
IIIc	$(\omega : 1 : 0)$, $\omega^{\frac{m-1}{p^l}}$ and $\omega^d \ne 1$	$p^l - 1$	0	$\frac{m-1}{p^l} - d$	Lemma 7 Corollary 3

[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] $I_t(u, v) = 0$ if $y_0(x_0+1)^{p^l}\left(y_0^{p^l-1} - 1\right)^{p^l+1} \ne x_0(y_0+1)^{p^l}\left(x_0^{p^l-1} - 1\right)^{p^l+1}$

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

3.1 Singular points at infinity

We have

$$\begin{cases} F_x = \dfrac{\partial F}{\partial x} = m(x+z)^{m-1} - m x^{m-1} \\ F_y = \dfrac{\partial F}{\partial y} = -m(y+z)^{m-1} + m y^{m-1} \\ F_z = \dfrac{\partial F}{\partial z} = m(x+z)^{m-1} - m(y+z)^{m-1} \end{cases}.$$

At infinity ($z = 0$), $F_x(x, y, 0) = F_y(x, y, 0) = 0$ and

$$F_z(x, y, 0) = m\left(x^{m-1} - y^{m-1}\right).$$

So $(x_0, y_0, 0)$ is a singular point of F if and only if $x_0^{m-1} = y_0^{m-1}$. If $y_0 = 0$ then $x_0 = 0$; so $y_0 \ne 0$ and we have to study the solutions of

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

Equation 1 is equivalent to $x_0^{\frac{m-1}{p^l}} = 1$. Since $\gcd(\frac{m-1}{p^l}, p) = 1$, there are $\frac{m-1}{p^l}$ solutions at (1) and $x_0 = 1$ is the only one such that $x_0 = y_0$.

Now, we want to find the multiplicity of these singularities:

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

Since $m - 1 \equiv 0 \mod p^l$, for all $2 \leq k < p^l$, $\binom{m}{k} = 0$. Consider the terms of degree $p^l - 1$ of $\widetilde{f}$:

$$\frac{1}{z}\binom{m}{p^l}\left(x_0^{m-p^l}(x+z)^{p^l} - x_0^{m-p^l}x^{p^l} - z^{p^l}\right) = \binom{m}{p^l}\left(x_0^{m-p^l} - 1\right) z^{p^l-1}. \tag{2}$$

This term vanishes (which means that $(x_0, y_0, 0)$ is a singular point of multiplicity greater than $p^l - 1$) if and only if

$$x_0^{m-p^l} = 1$$

that is to say if and only if

$$x_0^d = 1.$$

Now, consider the terms of degree p^l of $\widetilde{f}$:

$$\begin{aligned}&\tfrac{1}{z}\tbinom{m}{p^l+1}\left(x_0^{m-p^l-1}(x+z)^{p^l+1} - x_0^{m-p^l-1}x^{p^l+1} - z^{p^l+1}\right) \\ &= \tbinom{m}{p^l+1}\left(x_0^{m-p^l-1}x^{p^l} + x_0^{m-p^l-1}xz^{p^l-1} + \left(x_0^{m-p^l-1} - 1\right)z^{p^l}\right).\end{aligned} \tag{3}$$

Since $x_0^{m-p^l-1} \neq 0$, singular points of $\widehat{f}$ of multiplicity greater than $p^l - 1$ have multiplicity p^l.

We have just proved the following lemma:

Lemma 4 *Let ω such that $\omega^{\frac{m-1}{p^l}} = 1$. The point $(\omega : 1 : 0)$ is a singular point of $\widehat{h}$ with multiplicity*

$$\begin{cases} p^l & \text{if } \omega^d = 1, \omega \neq 1 \\ p^l - 1 & \text{otherwise} \end{cases}.$$

Furthermore, $\widehat{h}$ has $\frac{m-1}{p^l}$ singular points at infinity.

3.2 Affine singular points

We have:

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

So,

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

Finally, we have

Lemma 5 *Affine singular points of f are points satisfying*

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

From Lemma 5, we get that $x_0,\ y_0 \neq 0, -1$. Since p^l divides $m-1$,

$$(x_0, y_0) \text{ singular point of } f \Leftrightarrow \begin{cases} x_0^{\frac{m-1}{p^l}} = y_0^{\frac{m-1}{p^l}} \\ (x_0+1)^{\frac{m-1}{p^l}} = x_0^{\frac{m-1}{p^l}} \\ (y_0+1)^{\frac{m-1}{p^l}} = y_0^{\frac{m-1}{p^l}} \end{cases}. \tag{4}$$

There are at most $\frac{m-1}{p^l} - 1$ solutions to the second equation of (4). Let x_0 be one of these solutions, we want to know the number of y_0 such that (x_0, y_0) is a singular point of f.

We write $m = 1 + \sum_{j=1}^{b} m_j p^{i_j}$ with $1 \leq m_j \leq p-1,\ i_j > i_{j-1},\ i_1 = l$. Then,

$$(y_0+1)^{\frac{m-1}{p^l}} = y_0^{\frac{m-1}{p^l}} \Leftrightarrow \prod_{j=1}^{b} (y_0+1)^{m_j p^{i_j - l}} = y_0^{\frac{m-1}{p^l}}$$
$$\Leftrightarrow \sum_{(k_1,\ldots,k_b)\in\mathcal{I}} \left(\prod_{j=1}^{b} \binom{m_j}{k_j} \right) y_0^{\sum_{j=1}^{b} k_j p^{i_j - l}} = 0,$$

where $\mathcal{I} = \{(k_1,\ldots,k_b) \in \mathbb{Z}^b : \forall j = 1 \ldots b,\ 0 \leq k_j \leq m_j\} \setminus \{(m_1,\ldots,m_b)\}$. We multiply by $y_0^{\frac{m-1}{p^l} - m_b p^{i_b - l}}$ and we set $\alpha = y_0^{\frac{m-1}{p^l}}$:

$$\sum_{(k_1,\ldots,k_{b-1})\in\mathcal{I}'} \left(\prod_{j=1}^{b-1} \binom{m_j}{k_j} \right) \alpha y_0^{\sum_{j=1}^{b-1} k_j p^{i_j - l}}$$
$$+ \sum_{k_b=0}^{m_b-1} \sum_{\substack{0 \leq k_j \leq m_j \\ j \neq b}} \left(\prod_{j=1}^{b} \binom{m_j}{k_j} \right) y_0^{\frac{m-1}{p^l} - (m_b - k_b) p^{i_b - l} + \sum_{j=1}^{b-1} k_j p^{i_j - l}} = 0,$$

where $\mathcal{I}' = \{(k_1,\ldots,k_{b-1}) \in \mathbb{Z}^{b-1} : \forall j = 1 \ldots b-1,\ 0 \leq k_j \leq m_j\} \setminus \{(m_1,\ldots,m_{b-1})\}$.

The degree of this polynomial in y_0 is

$$\frac{m-1}{p^l} - p^{i_b-l} + \sum_{j=1}^{b-1} m_j p^{i_j-l} = 2\frac{m-1}{p^l} - (m_b+1)p^{i_b-l}.$$

Then, we obtain

Lemma 6 *The number of affine singularities of h is at most:*

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

where $m = 1 + \sum_{j=1}^{b} m_j p^{i_j}$ *with* $1 \le m_j \le p-1$, $i_j > i_{j-1}$, $i_1 = l$.

Now, we study the multiplicity of affine singularities:

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

Since $m-1 \equiv 0 \mod p^l$, for all $2 \le k < p^l$, $\binom{m}{k} = 0$. So (x_0, y_0) is a singularity of multiplicity at least p^l. Consider the terms of degree p^l+1:

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

Since (x_0, y_0) is a singular point, $(x_0+1)^{m-1} = x_0^{m-1}$ and $x_0 \neq -1, 0$. So,

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

Hence, affine singularities have multiplicity at most p^l+1. Then, we look at the terms of degree p^l:

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

However,

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

We can do the same for y_0.

We have just proved the following lemma.

Lemma 7 *There are at most:*

- $d-1$ *affine singularities of h such that* $x_0 = y_0 \in \mathbb{F}^*_{p^l}$. *Their multiplicity is* p^l *(*p^l+1 *for* f*);*
- $\frac{m-1}{p^l} - d$ *affine singularities of h such that* $x_0 = y_0 \notin \mathbb{F}^*_{p^l}$. *Their multiplicity is* $p^l - 1$ *(*p^l *for* f*);*
- $(d-1)(d-2)$ *affine singularities of h such that* $x_0 \neq y_0$ *and* $x_0, y_0 \in \mathbb{F}^*_{p^l}$. *Their multiplicity is* p^l+1 *(for h and f);*
- $\left(\frac{m-1}{p^l} - 1\right)\left(2\frac{m-1}{p^l} - (m_b+1)p^{i_b-l} - 1\right) - (d-1)(d-2)$ *affine singularities of h such that* $x_0 \neq y_0$ *and* x_0 *or* $y_0 \notin \mathbb{F}^*_{p^l}$ *(*$m = 1 + \sum_{j=1}^{b} m_j p^{i_j}$ *with* $1 \leq m_j \leq p-1$, $i_j > i_{j-1}$, $i_1 = l$*). Their multiplicity is* p^l *(for h and f).*

4 Intersection number bounds

We write $h = uv$; we want to bound the intersection number $I_t(u, v)$ for t a singularity of h.

4.1 Singularities at infinity

Let $t = (\omega : 1 : 0)$ be a singular point of h at infinity ($\omega^{\frac{m-1}{p^l}} = 1$) of multiplicity m_t. We write $\widetilde{h}(x+\omega, z) = \widetilde{H}_{m_t} + \widetilde{H}_{m_t+1} + \cdots$ where $\widetilde{H}_i$ is the homogeneous polynomial composed of the terms of degree i of $\widetilde{h}(x+\omega, z)$ and $\widetilde{f}(x+\omega, z) = \widetilde{F}_{m_t} + \widetilde{F}_{m_t+1} + \cdots$ where $\widetilde{F}_i$ is the homogeneous polynomial composed of the terms of degree i of $\widetilde{f}(x+\omega, z)$. Then,

$$
\begin{aligned}
\widetilde{f}(x+\omega, z) &= \widetilde{h}(x+\omega, z)(x+\omega-1)\\
&= \left(R + \widetilde{H}_{m_t+1} + \widetilde{H}_{m_t}\right)(x+\omega-1)\\
&\quad \text{where if } R \text{ is non zero then, it is a polynomial of degree greater than } m_t+1\\
&= xR + (\omega-1)R + x\widetilde{H}_{m_t+1} + x\widetilde{H}_{m_t} + (\omega-1)\widetilde{H}_{m_t+1} + (\omega-1)\widetilde{H}_{m_t}.
\end{aligned}
$$

So,

- if $\omega \neq 1$, then $\widetilde{F}_{m_t} = (\omega-1)\widetilde{H}_{m_t}$ and $\widetilde{F}_{m_t+1} = x\widetilde{H}_{m_t} + (\omega-1)\widetilde{H}_{m_t+1}$;
- if $\omega = 1$, then $\widetilde{F}_{m_t+1} = x\widetilde{H}_{m_t}$.

Then, we have

Lemma 8 *If* $t = (\omega : 1 : 0)$, $\omega^{\frac{m-1}{p^l}} = 1$*, is a singular point at infinity of h with multiplicity* m_t *then*

- $\widetilde{F}_{m_t} = (\omega-1)\widetilde{H}_{m_t}$ *and* $\widetilde{F}_{m_t+1} = x\widetilde{H}_{m_t} + (\omega-1)\widetilde{H}_{m_t+1}$ *if* $\omega \neq 1$*;*
- $\widetilde{F}_{m_t+1} = x\widetilde{H}_{m_t}$ *if* $\omega = 1$.

Corollary 1 *If* $t = (1 : 1 : 0)$ *then*

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

Proof If $t = (1 : 1 : 0)$ then its multiplicity is $p^l - 1$. By Lemma 8 and Eq. 3, there exists $a \in \mathbb{F}^*_q$ such that

$$
\widetilde{H}_{m_t} = a\left(x^{p^l-1} + z^{p^l-1}\right).
$$

Since the factors of $\widetilde{H}_{m_t}$ are different, $I_t(u, v) = m_t(u)m_t(v)$. We get the result since $m_t(u) + m_t(v) = p^l - 1$. □

Corollary 2 *If* $t = (\omega : 1 : 0)$ *such that* $\omega^d = 1$, $\omega \neq 1$ *then*

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

Proof Suppose that $t = (\omega : 1 : 0)$ such that $\omega^d = 1$ and $\omega \neq 1$ then, the multiplicity of t is p^l. By Lemma 8 and Eq. 3, there exists $a \in \mathbb{F}_q^*$ such that

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

So all factors of $\widetilde{H}_{p^l}$ are simple and $I_t(u, v) = m_t(u)m_t(v)$. We get the result since $m_t(u) + m_t(v) = p^l$. □

Corollary 3 *If* $t = (\omega : 1 : 0)$ *with* $\omega^{\frac{m-1}{p^l}} = 1$, $\omega^d \neq 1$, *then*

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

Proof Suppose that $t = (\omega : 1 : 0)$ with $\omega^{\frac{m-1}{p^l}} = 1$ and $\omega^d \neq 1$ then, the multiplicity of t is $p^l - 1$. By Lemma 8 and Eq. 2, there exists $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q^*$ such that

$$(\omega - 1)\widetilde{H}_{p^l-1} = \widetilde{F}_{p^l-1} = az^{p^l-1}$$

and

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

So, $\gcd(\widetilde{H}_{p^l}, \widetilde{H}_{p^l-1}) = \gcd(\widetilde{F}_{p^l}, \widetilde{F}_{p^l-1}) = 1$. Since $\widetilde{H}_{p^l-1}$ has only one tangent line, by Lemma 1, $I_t(u, v) = 0$. □

4.2 Affine singularities

Let $t = (x_0, y_0)$ be an affine singular point of h of multiplicity m_t.

We write $h(x+x_0, y+y_0) = H_{m_t} + H_{m_t+1} + \cdots$ where H_i is the homogeneous polynomial composed of the terms of degree i of $h(x + x_0, y + y_0)$.

Assume $x_0 = y_0$. Then, we write $f(x + x_0, y + y_0) = F_{m_t+1} + F_{m_t+2} + \cdots$ where F_i is the homogeneous polynomial composed of the terms of degree i of $f(x + x_0, y + y_0)$ and

$$\begin{aligned} f(x + x_0, y + y_0) &= h(x + x_0, y + y_0)(x + x_0 - y - y_0) \\ &= (R + H_{m_t+1} + H_{m_t})(x - y) \\ &\quad \text{where if } R \text{ is non zero then, it is a polynomial of degree} \\ &\quad \text{greater than } m_t + 1 \\ &= (x - y)R + (x - y)H_{m_t+1} + (x - y)H_{m_t}. \end{aligned}$$

So, $F_{m_t+2} = (x - y)H_{m_t+1}$ and $F_{m_t+1} = (x - y)H_{m_t}$. Furthermore, for some a, $F_{m_t+1} = a(x^{m_t+1} - y^{m_t+1})$ (see proof of Lemma 7).

So, we get

Lemma 9 *If* $t = (x_0, y_0)$ *is an affine singular point of* h *with multiplicity* m_t *such that* $x_0 = y_0$, *then* $F_{m_t+2} = (x - y)H_{m_t+1}$ *and* $F_{m_t+1} = (x - y)H_{m_t}$.

Furthermore, tangent lines to h *at* t *are the factors of* $\frac{x^{m_t+1} - y^{m_t+1}}{x - y}$.

Corollary 4 *If $t = (x_0, y_0)$ is an affine singular point of h such that $x_0 = y_0 \in \mathbb{F}^*_{p^l}$ then*

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

Proof Suppose that $t = (x_0, y_0)$ is an affine singular point of h such that $x_0 = y_0 \in \mathbb{F}^*_{p^l}$ then, the multiplicity of t is p^l. The factors of $\frac{x^{p^l+1} - y^{p^l+1}}{x-y}$ are all distinct. So, by Lemma 9, tangent lines to u or v are all distinct and

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

Since $m_t(u) + m_t(v) = p^l$, we get the result. □

Corollary 5 *If $t = (x_0, y_0)$ is an affine singular point of h such that $x_0 = y_0 \notin \mathbb{F}^*_{p^l}$ then,*

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

Proof Suppose that $t = (x_0, y_0)$ is an affine singular point of h such that $x_0 = y_0 \notin \mathbb{F}^*_{p^l}$ then, the multiplicity of t is $p^l - 1$. By Lemma 9,

$$H_{p^l-1} = a(x - y)^{p^l-1} \quad \text{and} \quad H_{p^l} = \frac{b\left(x^{p^l+1} - y^{p^l+1}\right)}{x - y}.$$

Hence, $\gcd(H_{p^l-1}, H_{p^l}) = 1$. Since H_{p^l-1} has only one tangent line, by Lemma 1, $I_t(u, v) = 0$. □

Assume now $x_0 \neq y_0$. Then, we write $f(x + x_0, y + y_0) = F_{m_t} + F_{m_t+1} + \cdots$ where F_i is the homogeneous polynomial composed of the terms of degree i of $f(x + x_0, y + y_0)$ and

$$\begin{aligned} f(x + x_0, y + y_0) &= h(x + x_0, y + y_0)(x + x_0 - y - y_0) \\ &= \left(R + H_{m_t+1} + H_{m_t}\right)(x + x_0 - y - y_0) \\ &\quad \text{where if } R \text{ is non zero then, it is a polynomial of degree} \\ &\quad \text{greater than } m_t + 1 \\ &= (x_0 - y_0)H_{m_t} + \left((x - y)H_{m_t} + (x_0 - y_0)H_{m_t+1}\right) \\ &\quad + \left((x - y + x_0 - y_0)R + (x - y)H_{m_t+1}\right). \end{aligned}$$

So, $F_{m_t} = (x_0 - y_0)H_{m_t}$ and $F_{m_t+1} = (x_0 - y_0)H_{m_t+1} + (x - y)H_{m_t}$.

Then, we obtain the following lemma.

Lemma 10 *If $t = (x_0, y_0)$ is an affine singular point of h with multiplicity m_t such that $x_0 \neq y_0$ then*

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

Corollary 6 *If $t = (x_0, y_0)$ is an affine singular point of h such that $x_0 \neq y_0$, x_0, $y_0 \in \mathbb{F}^*_{p^l}$ then*

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

Proof Suppose that $t = (x_0, y_0)$ is an affine singular point of h such that $x_0 \neq y_0$, $x_0, y_0 \in \mathbb{F}^*_{p^l}$ then, the multiplicity of t is $p^l + 1$. By Lemma 10,

$$(x_0 - y_0)H_{m_t} = F_{m_t} = c_1 x^{p^l+1} - c_2 y^{p^l+1} \quad \text{with } c_1, c_2 \neq 0.$$

Hence, all factors of H_{m_t} are simple and then $I_t(u, v) = m_t(u)m_t(v)$. Since $m_t(u)+m_t(v) = p^l + 1$, we get the result. □

Corollary 7 *If $t = (x_0, y_0)$ is an affine singular point of h such that $x_0 \neq y_0$ and $x_0 \in \mathbb{F}^*_{p^l}$ and $y_0 \notin \mathbb{F}^*_{p^l}$ or $x_0 \notin \mathbb{F}^*_{p^l}$ and $y_0 \in \mathbb{F}^*_{p^l}$ then*

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

Proof Suppose that $t = (x_0, y_0)$ is an affine singular point of h such that $x_0 \neq y_0$ and $x_0 \in \mathbb{F}^*_{p^l}$ and $y_0 \notin \mathbb{F}^*_{p^l}$ or $x_0 \notin \mathbb{F}^*_{p^l}$ and $y_0 \in \mathbb{F}^*_{p^l}$ then, the multiplicity of t is p^l. Then

$$F_{p^l} = \begin{cases} c_1 x^{p^l} & \text{if } y_0 \in \mathbb{F}^*_{p^l}, c_1 \neq 0 \\ c_2 y^{p^l} & \text{if } x_0 \in \mathbb{F}^*_{p^l}, c_2 \neq 0 \end{cases} \quad \text{and} \quad F_{p^l+1} = c'_1 x^{p^l+1} - c'_2 y^{p^l+1}, c'_1, c'_2 \neq 0.$$

So, by Lemma 10, $1 = \gcd(F_{p^l}, F_{p^l+1}) = \gcd(H_{p^l}, H_{p^l+1})$ and H_{p^l} has only one tangent line. Hence, by Lemma 1, $I_t(u, v) = 0$. □

Assume $x_0 \neq y_0$ and $x_0, y_0 \notin \mathbb{F}_{p^l}$. Then, t has multiplicity p^l. We have $F_{p^l} = c_1 x^{p^l} - c_2 y^{p^l} = (c_3 x - c_4 y)^{p^l}$, where $c_1 = (x_0 + 1)^{m-p^l} - x_0^{p^l}$ and $c_2 = (y_0 + 1)^{m-p^l} - y_0^{m-p^l}$. Since $x_0, y_0 \notin \mathbb{F}^*_{p^l}$, $c_1 \neq 0$ and $c_2 \neq 0$. By Lemma 10,

$$F_{p^l} = (x_0 - y_0)H_{p^l} \quad \text{and} \quad F_{p^l+1} = (x_0 - y_0)H_{p^l+1} + (x - y)H_{p^l}.$$

So, H_{p^l} has only one factor and $\gcd(F_{p^l}, F_{p^l+1}) = \gcd(H_{p^l}, H_{p^l+1})$. Furthermore, $F_{p^l+1} = d_1 x^{p^l+1} - d_2 y^{p^l+1}$ with $d_1 = (x_0 + 1)^{m-p^l-1} - x_0^{m-p^l-1} \neq 0$ and $d_2 = (y_0 + 1)^{m-p^l-1} - y_0^{m-p^l-1} \neq 0$. The polynomials F_{p^l} and F_{p^l+1} have a common factor if and only if $c_3 x - c_4 y$ divides F_{p^l+1}. So, F_{p^l} and F_{p^l+1} have a common factor if and only if

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

If (x_0, y_0) is a singular point of f, then

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

We have:

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

Similarly, $d_2 = \frac{-y_0^{m-p^l-1}}{(y_0+1)^{p^l}}$. Hence,

$$\frac{d_1}{d_2} = \frac{x_0^{m-p^l-1}(y_0+1)^{p^l}}{y_0^{m-p^l-1}(x_0+1)^{p^l}} = \frac{x_0^{m-1}y_0^{p^l}(y_0+1)^{p^l}}{y_0^{m-1}x_0^{p^l}(x_0+1)^{p^l}} = \frac{y_0^{p^l}(y_0+1)^{p^l}}{x_0^{p^l}(x_0+1)^{p^l}}.$$

On the other hand, we have:

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

Similarly, $c_2 = \frac{y_0^{m-p^l}(y_0^{p^l-1}-1)}{(y_0+1)^{p^l}}$. Hence,

$$\frac{c_1}{c_2} = \frac{x_0^{m-p^l}\left(x_0^{p^l-1}-1\right)(y_0+1)^{p^l}}{y_0^{m-p^l}\left(y_0^{p^l-1}-1\right)(x_0+1)^{p^l}} = \frac{y_0^{p^l-1}(y_0+1)^{p^l}\left(x_0^{p^l-1}-1\right)}{x_0^{p^l-1}(x_0+1)^{p^l}\left(y_0^{p^l-1}-1\right)}.$$

After simplification, we get that F_{p^l} and F_{p^l+1} have a common factor if and only if

$$y_0(x_0+1)^{p^l}\left(y_0^{p^l-1}-1\right)^{p^l+1} = x_0(y_0+1)^{p^l}\left(x_0^{p^l-1}-1\right)^{p^l+1}. \tag{5}$$

If (x_0, y_0) is not a solution of (5), then $\gcd(H_{p^l}, H_{p^l+1}) = 1$ and by Lemma 1, $I_t(u, v) = 0$.

Otherwise, we write $u(x + x_0, y + y_0) = U_r + U_{r+1} + \cdots$, where U_i is the homogeneous polynomial composed of the terms of degree i of $u(x + x_0, y + y_0)$ and $U_r \neq 0$ and $v(x + x_0, y + y_0) = V_s + V_{s+1} + \cdots$, where V_i is the homogeneous polynomial composed of the terms of degree i of $v(x + x_0, y + y_0)$ and $V_s \neq 0$. If $r = 0$ or $s = 0$ then t is not a point of u or v and $I_t(u, v) = 0$. Assume that $r, s > 0$. Since (x_0, y_0) satisfies (5), F_{p^l} and F_{p^l+1} have a common factor that we denote by e. We have $H_{p^l} = U_r V_s = e^{p^l}$ and $H_{p^l+1} = U_r V_{s+1} + U_{r+1} V_s$. Furthermore, $\gcd(F_{p^l}, F_{p^l+1}) = e$ and thus $\gcd(H_{p^l}, H_{p^l+1}) = e$. Since $r \geq 1$ and $s \geq 1$, e divides U_r and V_s and consequently $\gcd(U_r, V_s)$. If $\gcd(U_r, V_s) = e^k$, e^k divides $\gcd(H_{p^l}, H_{p^l+1})$ thus $\gcd(U_r, V_s) = e$. We can assume without loss of generality that $U_r = e^{p^l-1}$ and $V_s = e$. Since $m_t(v) = 1$, $I_t(u, v) = \mathrm{ord}_t^v(u)$. Since e^2 does not divide H_{p^l+1}, e does not divide U_{p^l} and we can write U_{p^l} as the product of p^l linear factors distinct from e. Each factor is not tangent to v, so the order of each factor is 1 (see [4, p. 70]). Thus the order of U_{p^l} is p^l and $\mathrm{ord}_t^v(u) \leq p^l$.

Finally, we get

Lemma 11 *If $t = (x_0, y_0)$ is an affine singular point of h such that x_0 and $y_0 \notin \mathbb{F}_{p^l}^*$ and $x_0 \neq y_0$ then*

- $I_t(u, v) = 0$ *if* $y_0(x_0+1)^{p^l}\left(y_0^{p^l-1}-1\right)^{p^l+1} \neq x_0(y_0+1)^{p^l}\left(x_0^{p^l-1}-1\right)^{p^l+1}$
- *otherwise,* $I_t(u, v) \leq p^l$*; and there are at most* $((p^l-2)(p^l+1)+1)\left(\frac{m-1}{p^l}-1\right)$ *such singular points.*

5 Proof of Theorem 3

The following theorems prove Theorem 3. From now, assume $m \neq 1 + p^l$. We write $m = 1 + \sum_{j=1}^{b} m_j p^{i_j}$ with $1 \leq m_j \leq p-1,\ i_j > i_{j-1},\ i_1 = l$.

Theorem 4 *If $d = 1$ then h has an absolutely irreducible factor over $\mathbb{F}_p$.*

Proof Suppose that $d = 1$. Assume h has no absolutely irreducible factor over $\mathbb{F}_p$, then by Lemma 2 we have $e = \frac{I_{tot}}{\frac{(m-2)^2}{4}} \geq \frac{8}{9}$ where I_{tot} is an upper bound on the global intersection number for any factorization $h = u \cdot v$. Since $d = 1$, we only have singularities of type Ib, IIc, IIIa and IIIc (see Table 1). So, by Table 1, we can take

$$I_{tot} = p^l\left(\frac{m-1}{p^l} - 1\right)\left(2\frac{m-1}{p^l} - (m_b+1)p^{i_b - l} - 1\right) + \left(\frac{p^l-1}{2}\right)^2. \tag{6}$$

Since $m = 1 + p^l k$ and $m \neq 1 + p^l,\ k \geq 2$; thus $\frac{m-3}{4} = \frac{p^l k - 2}{4} \geq \frac{p^l - 1}{2}$. Hence

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

For $p^l \neq 3$ or 5, we have $e < \frac{8}{9}$ which is a contradiction.

First, consider the case where $p^l = 3$. We have $1 = d = \gcd(2, k)$ so k is odd and 3 does not divide k by definition of l. Hence $k \geq 5$, thus, by Lemma 11

$$e \leq \frac{p^l((p^l-2)(p^l+1)+1)\left(\frac{m-1}{p^l} - 1\right) + \left(\frac{p^l-1}{2}\right)^2}{\frac{(m-2)^2}{4}} = \frac{15(k-1)+1}{\frac{(3k-1)^2}{4}}.$$

However, for $k \geq 5,\ k \mapsto \frac{15(k-1)+1}{\frac{(3k-1)^2}{4}}$ is a decreasing function. So, for $k \geq 11,\ e < \frac{8}{9}$. Now we have to consider the case where $k = 5$ and $k = 7$. Using Eq. 6, we have

k	5	7
m	16	22
I_{tot}	37	73
e	$\frac{37}{7^2}$	$\frac{73}{11^2}$

In all cases we get a contradiction since $e < \frac{8}{9}$.

If $p^l = 5$, then $1 = d = \gcd(4, k)$ and k is odd. Hence, $k = 3$ or $k \geq 7$. As in the case where $p^l = 3,\ e \leq \frac{95(k-1)+4}{\frac{(5k-1)^2}{4}}$. However $k \mapsto \frac{95(k-1)+4}{\frac{(5k-1)^2}{4}}$ is a decreasing function for $k \geq 3$. so, for $k \geq 17,\ e < \frac{8}{9}$ which is a contradiction. We now have to consider the case where $k = 3, 7, 9, 11, 13$. Using Eq. 6, we have

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

In all case, $e < \frac{8}{9}$ which is a contradiction. □

Theorem 5 *If* $1 < d < \frac{m-1}{p^l}$, *h has an absolutely irreducible factor over* $\mathbb{F}_p$.

Proof Suppose that $1 < d < \frac{m-1}{p^l}$. Assume h has no absolutely irreducible factor over $\mathbb{F}_p$, then by Lemma 2, we have $e = \frac{I_{tot}}{\frac{(m-2)^2}{4}} \geq \frac{8}{9}$ where I_{tot} is an upper bound on the global intersection number for any factorization of $h = u \cdot v$. By Table 1, we can take:

$$
\begin{aligned}
I_{tot} &= \frac{p^{2l}-1}{4}(d-1) + \left(\frac{p^l-1}{2}\right)^2 \\
&\quad + p^l \left(\left(\frac{m-1}{p^l} - 1\right)\left(2\frac{m-1}{p^l} - (m_b+1)p^{i_b-l} - 1\right) - (d-1)(d-2)\right) \\
&\quad + \left(\frac{p^l+1}{2}\right)^2 (d-1)(d-2) + (d-1)\frac{p^{2l}-1}{4} \\
&\leq \frac{p^{2l}-1}{2}(d-1) + \left(\frac{p^l-1}{2}\right)^2 (d-1)(d-2) \\
&\quad + p^l \left(\frac{m-1}{p^l} - 1\right)^2 + \left(\frac{p^l-1}{2}\right)^2.
\end{aligned}
$$

However, $m = 1 + kp^l$ with $k \neq 1$. Since d divides k and $d < k$, we have $d \leq \frac{m-1}{2p^l}$. Hence,

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

Since $e \geq \frac{8}{9}$, $1 < d < k$ and $\gcd(k, p) = 1$, the only possibilities are:

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 one hand, we have

$$
\begin{aligned}
e \leq\; & \frac{2(p^{2l}-1)(d-1) + (p^l+1)^2(d-1)(d-2)}{(p^l k - 1)^2} \\
& + \frac{4p^l(k-1)((p^l-2)(p^l+1)+1) + (p^l-1)^2}{(p^l k - 1)^2}. \qquad (7)
\end{aligned}
$$

On the other hand, we have:

$$
\begin{aligned}
e \leq\; & \frac{2(p^{2l}-1)(d-1) + (p^l+1)^2(d-1)(d-2)}{(p^l k - 1)^2} \\
& + \frac{4p^l(k-1)(2k - (m_b+1)p^{i_b-l} - 1) + (p^l-1)^2}{(p^l k - 1)^2}. \qquad (8)
\end{aligned}
$$

First, consider the case where $k \geq 16$. In inequality (7), e is bounded by a decreasing function of k. Furthermore, if $p^l = 3$ and $k = 16$ or if $k = 17$ and $p^l = 5$ the upper bound in (7) is less than $\frac{8}{9}$ which leaves only the case $k = 16$ and $p^l = 5$. But replacing in Eq. 8, we also get a contradiction. In the other cases, using inequality (7) or inequality (8), we have $e < \frac{8}{9}$ which is a contradiction. □

Theorem 6 *If* $d = \frac{m-1}{p^l} \neq p^l - 1$ *then* h *has an absolutely irreducible factor over* $\mathbb{F}_p$.

Proof Suppose that $d = \frac{m-1}{p^l} \neq p^l - 1$. First, we make some remarks. Since $d = \frac{m-1}{p^l}$, there are only singularities of type Ia, IIa, IIIa, IIIb (see Table 1). In all these cases, the tangent lines of h in any singular point are simple. So, for all factorization $h = uv,\ I_t(u, v) = m_t(u)m_t(v)$. Furthermore, since $\frac{m-1}{p^l} \neq p^l - 1,\ \frac{m-1}{p^l} \leq \frac{p^l-1}{2}$. Assume that h has no absolutely irreducible factor over $\mathbb{F}_p$. We write $h = h_1 \dots h_r$ where each h_i factorizes into $c_i \geq 2$ factors on an algebraic closure of $\mathbb{F}_p$ and its factors are all of degree $\frac{\deg(h_i)}{c_i}$. We write $h_i = h_{i,1} \dots h_{i,c_i}$. Then

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

$$= \sum_{k=1}^{r} \sum_{1 \leq i < j \leq c_k} \sum_t m_t(h_{k,i}) m_t(h_{k,j}) + \sum_{1 \leq k < l \leq r} \sum_{\substack{1 \leq i \leq c_k \\ 1 \leq j \leq c_l}} \sum_t m_t(h_{k,i}) m_t(h_{l,j}).$$

However,

$$(m_t(h))^2 = \left(\sum_{k=1}^{r} m_t(h_k) \right)^2$$

$$= \sum_{k=1}^{r} m_t(h_k)^2 + 2 \sum_{1 \leq k < l \leq r} m_t(h_k) m_t(h_l)$$

$$= \sum_{k=1}^{r} m_t(h_k)^2 + 2 \sum_{1 \leq k < l \leq r} \sum_{\substack{1 \leq i \leq c_k \\ 1 \leq j \leq c_l}} m_t(h_{k,i}) m_t(h_{l,j}).$$

So, by Lemma 3,

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

thus

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

On the other hand, by Bézout's theorem,

$$A = \sum_{k=1}^{r} \sum_{1 \le i < j \le c_k} \deg(h_{k,i}) \deg(h_{k,j}) + \sum_{1 \le k < l \le r} \sum_{\substack{1 \le i \le c_k \\ 1 \le j \le c_l}} \deg(h_{k,i}) \deg(h_{l,j})$$

$$= \sum_{k=1}^{r} \frac{\deg(h_k)^2}{c_k^2} \frac{c_k(c_k-1)}{2} + \sum_{1 \le k < l \le r} \deg(h_k) \deg(h_l)$$

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

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

Hence,

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

Then, by Lemma 3,

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

We set $k = \frac{m-1}{p^l}$. Then

$$\deg(h)^2 \le \sum_{t} m_t(h)^2 \Leftrightarrow (m-2)^2 \le 2(k-1)p^{2l}$$
$$+ (k-1)(k-2)(1+p^l)^2 + (p^l-1)^2$$
$$\Leftrightarrow -(2p^l+1)k^2 + (p^{2l}+4p^l+3)k - (p^{2l}+2p^l+2) \le 0$$
$$\Leftrightarrow k \le 1 \text{ or } k \ge \frac{p^{2l}+2p^l+2}{2p^l+1}.$$

However, $k \ge 2$ ($m \ne 1 + p^l$) and $k \le \frac{p^l-1}{2} < \frac{p^{2l}+2p^l+2}{2p^l+1}$ which is a contradiction. □

References

1. Coulter R.S., Matthews R.W.: Planar functions and planes of Lenz-Barlotti class II. Des. Codes Cryptogr. **10**(2), 167–184 (1997).
2. Dembowski P., Ostrom T.G.: Planes of order n with collineation groups of order n^2. Math. Z. **103**, 239–258 (1968).
3. Dobbertin H., Mills D., Müller E.N., Pott A., Willems A.: APN functions in odd characteristic. Discrete Math. **267**(13), 95–112 (2003). Combinatorics 2000 (Gaeta).
4. Fulton W.: Algebraic Curves. Advanced Book Classics. Addison-Wesley Publishing Company Advanced Book Program, Redwood City (1989). An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original.
5. Hernando F., McGuire G.: Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions. J. Algebra **343**, 78–92 (2011).

6. Hernando F., McGuire G., Monserrat F.: On the classification of exceptional planar functions over $\mathbb{F}_p$. ArXiv e-prints (2013).
7. Janwa H., McGuire G.M., Wilson R.M.: Double-error-correcting cyclic codes and absolutely irreducible polynomials over GF(2). J. Algebra **178**(2), 665–676 (1995).
8. Jedlicka D.: APN monomials over GF(2^n) for infinitely many n. Finite Fields Appl. **13**(4), 1006–1028 (2007).
9. Lidl R., Niederreiter H.: Finite Fields, Volume 20 of Encyclopedia of Mathematics and its Applications, 2nd edn. Cambridge University Press, Cambridge (1997). With a foreword by P. M. Cohn.
10. Sorensen A.B.: A note on algorithms deciding rationality and absolutely irreducibility based on the number of rational solutions. RISC report series 91-37, Research Institute for Symbolic Computation (RISC), University of Linz, Hagenberg (1991).
11. Zieve M.: Planar functions and perfect nonlinear monomials over finite fields. ArXiv e-prints (2013).