

Document downloaded from:

<http://hdl.handle.net/10251/50613>

This paper must be cited as:

Hernando, F.; Mcguire, G.; Monserrat Delpalillo, FJ. (2014). On the classification of exceptional planar functions over F_p . *Geometriae Dedicata*. 173(1):1-35.
doi:10.1007/s10711-013-9926-2.



The final publication is available at

<http://link.springer.com/article/10.1007/s10711-013-9926-2>

Copyright Springer Verlag (Germany)

On the Classification of Exceptional Planar Functions over \mathbb{F}_p

Fernando Hernando*
Department of Mathematics
Universidad Jaume I
Spain

Gary McGuire†
School of Mathematical Sciences
University College Dublin
Ireland

Francisco Monserrat*
Instituto Universitario de Matemática Pura y Aplicada
Universidad Politécnica de Valencia
Spain

January 14, 2015

Abstract

We will present many strong partial results towards a classification of exceptional planar/PN monomial functions on finite fields. The techniques we use are the Weil bound, Bezout's theorem, and Bertini's theorem.

Keywords: Absolutely irreducible polynomial, planar function, perfect nonlinear function.

1 Introduction

We present some new results on the classification of perfect nonlinear (PN) or planar functions. These have connections to finite geometry, coding theory and cryptography.

*Research of the first author supported by Spain Ministry of Education MTM2007-64704 and Bancaixa P1-1B2009-03

†Research of the second author supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006.

Let p be a prime number, $t \geq 3$ an integer, and let $f_t(x, y)$ the polynomial

$$f_t(x, y) := (x + 1)^t - x^t - (y + 1)^t + y^t \in \mathbb{F}_p[x, y].$$

Notice that $x - y$ divides $f_t(x, y)$. We define another polynomial $g_t(x, y)$ by

$$g_t(x, y) := \frac{(x + 1)^t - x^t - (y + 1)^t + y^t}{x - y} \in \mathbb{F}_p[x, y].$$

In this paper we consider the following conjecture (see Section 2 for the background).

Conjecture PN3: *Suppose $t > 2$. The polynomial $g_t(x, y)$ has an absolutely irreducible factor defined over \mathbb{F}_p for all t not of the form $p^i + 1$ (when $p \geq 3$) and $(3^i + 1)/2$ (when $p = 3$).*

Let $t = p^i \ell + r$, where r is the remainder upon division of t by p , and $i = \max\{j : p^j \text{ divides } t - r\}$. We will see later that we may assume that t is relatively prime to p , i.e., we may assume $r \neq 0$.

The results in this paper are the following.

Theorem 1.1. *The polynomial $g_t(x, y)$ has an absolutely irreducible factor defined over \mathbb{F}_p in the following cases.*

(A) $t \not\equiv 1 \pmod{p}$.

- (a) Either $\gcd(p - 1, t) \geq 3$ or $\gcd(p - 1, t - 1) \geq 2$.
- (â) If there exists $m \in \mathbb{N}$ such that $g_t(x, y)$ does not factor over \mathbb{F}_{p^m} and, furthermore, either $\gcd(p^m - 1, t) \geq 3$ or $\gcd(p^m - 1, t - 1) \geq 2$.
- (b) The number of singular points of the curve defined by $g_t(x, y) = 0$ (over an algebraic closure of \mathbb{F}_p) is less than $\frac{(t-2)^2}{4}$.
- (c) t is even, $(s - 1)^{t-1} \notin \mathbb{F}_p$ and $(s - 1)^{(t-1)(p-1)} \neq -1$ for all $s \neq 1$ in the set of $(t - 1)$ -roots of unity in algebraic closure of \mathbb{F}_p .
- (d) t is even and $t - 1$ divides $p^{2e} + 1$ for some positive integer e .
- (e) $t - 1 \geq 3$ is a prime number such that the multiplicative order of p in $\mathbb{Z}/(t - 1)\mathbb{Z}$ is $(t - 2)/2$.
- (f) If $e := \gcd(e_{t-1}, e_t)$, e_n denoting the multiplicative order of p in $\mathbb{Z}/n\mathbb{Z}$,
 - (1) either there exists a divisor $d > 2$ of t such that $\gcd(e, e_d) = 1$ or
 - (2) there exists a divisor $d > 1$ of $t - 1$ such that $\gcd(e, e_d) = 1$.
- (g) The polynomial $g_t(x, y)$ is irreducible over \mathbb{F}_p and $\gcd(e_d \mid d \in E) = 1$, where e_d is defined as in (f) and $E := \{d \in \mathbb{N} \mid d > 2 \text{ and } d \text{ divides either } t \text{ or } t - 1\}$.

(B) $t \equiv 1 \pmod{p}$.

(B.1) $\gcd(\ell, p^i - 1) < \ell$ and at least one of these conditions holds:

- $p \geq 5$, $i \geq 1$ and $\ell > 3$,
- $p \geq 5$, $i \geq 2$ and $\ell \geq 3$,

- $p = 3$, $i \geq 2$ and $\ell \geq 3$,
- (B.2) $\gcd(\ell, p^i - 1) = \ell$ and $\ell < p^i - 1$.

The conditions of Case (A) in the above theorem satisfy the following implications:

$$(d) \vee (e) \Rightarrow (c) \Rightarrow (b).$$

Conditions (b) and (c) concern an algebraic closure of the field \mathbb{F}_p . Conditions (d) and (e) are weaker but they involve only integer arithmetic.

The layout of this paper is as follows. In Section 2 we give the background to the problem and explain the motivation and origin of Conjecture PN3. Section 3 gives a more detailed background of the results and techniques we use. In Section 4 we analyze the singular points of the curve defined by $g_t(x, y) = 0$, and in Section 5 we calculate or estimate the intersection multiplicities of hypothetical factors at the singular points. Section 6 proves the Case (B) results under the assumption that the curve is irreducible over \mathbb{F}_p . Section 7 removes this assumption using more careful analysis. Finally Section 8 proves our results on Case (A).

2 Background and Motivation

In this section we present background to the problems under consideration in this paper.

2.1 PN and Planar Functions

Let p be a prime number and let $q = p^n$. Recall that any function $\mathbb{F}_q \rightarrow \mathbb{F}_q$ can be expressed uniquely as a polynomial function (with coefficients in \mathbb{F}_q) of degree less than q . A polynomial function is called a permutation polynomial (PP) if it is a bijective function $\mathbb{F}_q \rightarrow \mathbb{F}_q$.

Definition 2.1. A function $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$ is said to be planar if the functions $f(x + a) - f(x)$ are PPs for all nonzero $a \in \mathbb{F}_q$.

Planar functions are used to construct finite projective planes, and have been studied by finite geometers since at least 1968 (Dembowski and Ostrom [6]). Note that planar functions cannot exist in characteristic 2, because if $D_a(x) := f(x + a) - f(x)$ and $D_a(x) = b$ then $D_a(x + a) = b$ also.

Definition 2.2. A function $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$ is said to be PN (Perfect Nonlinear) if for every $a, b \in \mathbb{F}_q$ with $a \neq 0$ we have

$$\#\{x \in \mathbb{F}_q \mid f(x + a) - f(x) = b\} \leq 1.$$

PN functions were first defined in 1992 by Nyberg and Knudsen [25], in a cryptography paper. Note that PN functions cannot exist in characteristic 2, because if x is a solution to $f(x + a) - f(x) = b$ then $x + a$ is another solution.

It is clear that PN functions and planar functions are the same thing! They have different origins; PN functions come from cryptography whereas planar functions come from finite geometry.

We consider monomial functions in this article. Because x^t is planar iff x^{pt} is planar, we may assume that t is relatively prime to p .

The known planar monomials $f(x) = x^t$ are in the following table.

Characteristic	Exponents t	Conditions	Proved by
odd	2	None	Classical
odd	$p^i + 1$	$n/(i, n)$ odd	Dembowski-Ostrom
3	$(3^i + 1)/2$	$(i, n) = 1, i$ odd	Coulter-Matthews

Table 1: Known PN exponents t

It is conjectured that this list is complete:

Conjecture PN1: *All planar functions of the form x^t are listed in Table 1.*

In this article we present some partial results towards this conjecture. We consider the classification of functions x^t that are planar/PN on \mathbb{F}_{p^n} for infinitely many n . The known examples in Table 1 all have this property. Therefore, a weaker conjecture than Conjecture 1 is the following:

Conjecture PN2: *If x^t is a planar function on \mathbb{F}_{p^n} for infinitely many n , then t is of the values listed in the table.*

For monomial functions $f(x) = x^t$, it was shown in [4] that x^t is planar over \mathbb{F}_q if and only if $(x+1)^t - x^t$ is a PP over \mathbb{F}_q , i.e., for monomial functions we only need consider the $a = 1$ case of Definition 1.

Definition 2.3. *A PP $f(x) \in \mathbb{F}_q[x]$ is called exceptional if f is a PP on infinitely many extension fields of \mathbb{F}_q .*

Exceptional PPs have been the subject of many papers, see [11] for example. Their monodromy groups are of great interest and have been classified.

To prove Conjecture PN2, we consider the function $f(x) = x^t$ on the base field \mathbb{F}_p , and we would like to prove that $(x+1)^t - x^t$ is not an exceptional PP on \mathbb{F}_p when t is not one of the values listed.

Observe that $(x+1)^t - x^t$ is not a PP over \mathbb{F}_{p^n} if there exist \mathbb{F}_{p^n} -rational points (x, y) on the curve defined by

$$f_t(x, y) = (x+1)^t - x^t - (y+1)^t + y^t$$

with $x \neq y$. It is obvious that $f_t(x, y)$ has $x - y$ as a factor. Therefore, we would like to know whether the curve defined by

$$g_t(x, y) = \frac{(x+1)^t - x^t - (y+1)^t + y^t}{x - y}$$

has rational points over \mathbb{F}_{p^n} with $x \neq y$. Note that $g_t(x, y)$ is defined over \mathbb{F}_p .

The following is easily proved using the Weil bound.

Theorem 2.4. *If $g_t(x, y)$ has an absolutely irreducible factor defined over \mathbb{F}_p then $g_t(x, y)$ has rational points $(\alpha, \beta) \in (\mathbb{F}_{p^n})^2$ with distinct coordinates for all n sufficiently large.*

Based on the known examples of PN functions in Table 1, we make the following conjecture.

Conjecture PN3: *Suppose $t > 2$. The polynomial $g_t(x, y)$ has an absolutely irreducible factor defined over \mathbb{F}_p for all t not of the form $p^i + 1$ (when $p \geq 3$) and $(3^i + 1)/2$ (when $p = 3$).*

Clearly Conjecture PN3 implies Conjecture PN2. Therefore, the topic of this paper is proving Conjecture PN3. We give some partial results, which are stated in the introduction; the full conjecture is still open.

2.2 Small values of p and t

To demonstrate the power of our results, we have implemented MAGMA functions for testing the conditions given in Theorem 1.1 and, using them, we have proved Conjecture PN3 for a great many values $t \leq 1000$ when p is either 3, 5 or 7. Condition (\hat{a}) has been checked only for $m = 2$ and $m = 3$ and, to implement Condition (d) , we have used the equivalent formulation given in Corollary 8.8. Condition (b) is quite strong but it involves computations with a variety which is computationally intensive and the MAGMA function that implements it does not finish; so we have not taken it into account for our tests.

Notice that the conditions concerning Case (B) involve only integer arithmetic. However, in Case (A) , conditions (a) , (d) , (e) and (f) are purely arithmetical conditions relating t and p (integer arithmetic) and the other conditions involve computations concerning elements in the algebraic closure of \mathbb{F}_p . Taking this observation into account, we consider separately the following groups of conditions associated with Case (A) :

- Group 1: (a) , (d) , (e) and (f) .
- Group 2: Conditions of Group 1 and (g) .
- Group 3: Conditions of Group 2 and (c) .
- Group 4: Conditions of Group 3 and (\hat{a}) (taking $m = 2$).
- Group 5: Conditions of Group 3 and (\hat{a}) (taking $m = 3$).

Note that each Group includes the previous Group (except 4 and 5).

Tables 2, 3 and 4 show, for $p = 3, 5, 7$, the values of t , $3 \leq t \leq 1000$, for which we are *not* able to prove Conjecture PN3 using the conditions in each group. Notice that for $p \in \{5, 7\}$ conditions in Group 5 cover every t from 3 to 1000 corresponding to Case (A) .

Of course we omit the exceptional values of t when doing these computations. Putting all our results together, these computations show the following.

Theorem 2.5. *Conjecture PN3 is proved by Theorem 1.1 in the following cases.*

1. $p = 3$, all values of $t < 1000$ except 758 and $t \equiv 4 \pmod{6}$
2. $p = 5$, all values of $t < 1000$ except 15 and 76
3. $p = 7$, all values of $t < 1000$ except 22 and 148

Conditions	Excluded values of t for $p = 3$
(B)	118 values of the form $4 + 6k$
(A): Group 1	79 values
(A): Group 2	69 values
(A): Group 3	482, 758
(A): Group 4	482, 758
(A): Group 5	758

Table 2: Not included values in Theorem 1.2 for $p = 3$

Conditions in Th 1.2	Excluded values of t for $p = 5$
(B)	16, 76
(A): Group 1	34 values
(A): Group 2	24 values
(A): Group 3	82, 218, 274, 322, 334, 442, 658, 898
(A): Group 4	218
(A): Group 5	

Table 3: Not included values in Theorem 1.2 for $p = 5$

We note that similar results involving Case (B) have also been achieved independently by Robert Coulter [5]. Moreover a preprint has been posted on the arxiv by Elodie Leducq [21] solving Case (B).

3 Detailed Background Results

We wish to prove Conjecture PN3. The idea is to show that Bezout's theorem cannot possibly hold, when applied to two (or more) putative factors of the polynomial g_t . This proof depends heavily on analyzing the singular points of the curve g_t .

Conditions in Th 1.2	Excluded values for $p = 7$
(B)	22, 148
(A): Group 1	54 values
(A): Group 2	41 values
(A): Group 3	362, 818
(A): Group 4	362, 818
(A): Group 5	

Table 4: Not included values in Theorem 1.2 for $p = 7$

3.1 Background on curves

Let $\overline{\mathbb{F}}_p$ be an algebraic closure of \mathbb{F}_p . A polynomial $h(x, y) \in \overline{\mathbb{F}}_p[x, y]$ defines an affine plane curve

$$C_h := \{(\alpha, \beta) \in \overline{\mathbb{F}}_p^2 \mid h(\alpha, \beta) = 0\}.$$

Given a point $P = (\alpha, \beta) \in \overline{\mathbb{F}}_p^2$ we write

$$h(x + \alpha, y + \beta) = H_0(x, y) + H_1(x, y) + H_2(x, y) + \cdots,$$

where each $H_i(x, y)$ is either 0 or a homogeneous polynomial of degree i .

Definition 3.1. *The multiplicity of h at P is the smallest m with $H_m \neq 0$, and is denoted by $m_P(h)$ or $m_P(C_h)$.*

In particular, $P \in C_h$ if and only if $m_P(h) \geq 1$.

We say that P is a *singular point* of h (or of C_h) if $m_P(h) \geq 2$. The linear factors of H_m are the tangent lines to the curve C_h at the point P . The collection of tangent lines is called the *tangent cone*.

We consider the projective plane \mathbb{P}^2 over $\overline{\mathbb{F}}_p$ and take homogeneous coordinates $(X : Y : Z)$ such that $x := X/Z$ and $y := Y/Z$ are affine coordinates in the chart defined by $Z \neq 0$. Let $F_t(X, Y, Z)$ (resp., $G_t(X, Y, Z)$) be the homogenization of the polynomial $f_t(x, y)$ (resp., $g_t(x, y)$) and denote by χ_t the projective curve over $\overline{\mathbb{F}}_p$ defined by the equation $G_t(X, Y, Z) = 0$. Notice that $g_t(x, y)$ has an absolutely irreducible factor over \mathbb{F}_p if and only if $G_t(X, Y, Z)$ does so.

3.2 Background on intersection multiplicity

Bezout's theorem is a classical result in algebraic geometry and appears frequently in the literature (see for example chapter 5 of [8]).

Bezout's Theorem: Let r and s be two projective plane curves of degrees D_1 and D_2 over an algebraically closed field k having no components in common. Then,

$$\sum_P I(P, r, s) = D_1 D_2. \quad (1)$$

The sum runs over all points P in the projective plane $\mathbb{P}^2(k)$, and by $I(P, r, s)$ we mean the intersection multiplicity of the curves r and s at the point P . Notice that if r or s does not go through P , then $I(P, r, s) = 0$. Therefore, the sum in (1) runs over the singular points of the product rs . In our case, the sum will run over the singular points of g_t .

Using properties $I(P, r_1 r_2, s) = I(P, r_1, s) + I(P, r_2, s)$ and $\deg(r_1 r_2) = \deg(r_1) + \deg(r_2)$ one can generalize Bezout's Theorem to several curves f_1, f_2, \dots, f_r as follows:

$$\sum_P \sum_{1 \leq i < j \leq r} I(P, f_i, f_j) = \sum_{1 \leq i < j \leq r} \deg(f_i) \deg(f_j). \quad (2)$$

We refer the reader to chapter 5 of [8] for the definition of the intersection multiplicity $I(P, r, s)$ of two curves r, s at a point P . The following property of the intersection multiplicity will be useful for us. It is part of the definition of intersection multiplicity in [8]. We state it as a Corollary.

Corollary 3.2.

$$I(P, r, s) \geq m_P(r)m_P(s), \quad (3)$$

and equality holds if and only if the tangent cones of r and s do not share any linear factor.

We note that the degree of g_t is $t - 1$. Therefore, if $g_t = uv$ then our strategy is to show that $\sum_P I(P, u, v) < (\deg u)(\deg v)$ by analyzing the singular points P . We usually lower bound the product of the degrees, and upper bound the sum of intersection multiplicities, and show that the upper bound is strictly less than the lower bound, to obtain our contradiction.

3.3 Background on pencils and clusters of base points

Let \mathbb{P}^2 be the projective plane over $\overline{\mathbb{F}}_p$. Given a positive integer d , the projectivization of a vector subspace \mathcal{P} of $H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(d))$ with (projective) dimension 1 is called a *pencil* on \mathbb{P}^2 , where $\mathcal{O}_{\mathbb{P}^2}$ denotes the structure sheaf [17, II.2] of \mathbb{P}^2 as an algebraic variety over $\overline{\mathbb{F}}_p$.

Let us fix projective coordinates $(X : Y : Z)$ on \mathbb{P}^2 . Using them, such a pencil can be seen as the space of projective curves with equations $\alpha F(X, Y, Z) + \beta G(X, Y, Z) = 0$, where $F(X, Y, Z)$ and $G(X, Y, Z)$ are fixed homogeneous polynomials of $\overline{\mathbb{F}}_p[X, Y, Z]$ of degree d and $(\alpha : \beta)$ varies along \mathbb{P}^1 , the projective line over $\overline{\mathbb{F}}_p$. The pencil generated by polynomials F and G will be denoted by $\mathcal{P}(F, G)$. Also, from now on, we shall assume that all considered pencils have no fixed components, that is, there is no curve that is component of all the curves of the pencil. A *base point* of a pencil \mathcal{P} is a (closed) point $P \in \mathbb{P}^2$ that belongs to all the curves of \mathcal{P} .

Let us consider any sequence of morphisms

$$X_{n+1} \xrightarrow{\pi_n} X_n \xrightarrow{\pi_{n-1}} \dots \xrightarrow{\pi_2} X_2 \xrightarrow{\pi_1} X_1 := \mathbb{P}^2, \quad (4)$$

where π_i is the blow-up of X_i at a closed point $p_i \in X_i$, $1 \leq i \leq n$. The associated set of closed points $\mathcal{C} = \{p_1, p_2, \dots, p_n\}$ will be called a *cluster* (of infinitely near

points) over \mathbb{P}^2 . For each point $p \in \mathcal{C}$, set \tilde{E}_p (resp., E_p^*) the strict (resp., total) transform on X_{n+1} of the exceptional divisor created by the blowing-up at p . For any curve C on \mathbb{P}^2 it holds that

$$C^* = \tilde{C} + \sum_{p \in BP(\mathcal{P})} m_p(C) E_p^*, \quad (5)$$

where C^* (resp., \tilde{C}) denotes the total (resp., strict) transform of C on $Z_{\mathcal{P}}$ and $m_p(C)$ is the multiplicity at p of the strict transform of C on the surface to which p belongs. See, for instance, [7, IV.2], for the definition and properties of the blow-up, strict transforms and total transforms.

Given a pencil $\mathcal{P}(F, G)$, the quotient F/G gives rise to a rational map $f_{\mathcal{P}} : X \cdots \rightarrow \mathbb{P}^1$ that is independent from the chosen basis $\{F, G\}$ up to composition with an automorphism of \mathbb{P}^1 . The closures of the fibers of $f_{\mathcal{P}}$ are exactly the curves of the pencil \mathcal{P} . Moreover, there exists a minimal composition of blow-ups $\pi_{\mathcal{P}} : Z_{\mathcal{P}} \rightarrow X$ (as in (4)) eliminating the indeterminacies of the rational map $f_{\mathcal{P}}$, that is, the map $h_{\mathcal{P}} := f_{\mathcal{P}} \circ \pi_{\mathcal{P}} : Z_{\mathcal{P}} \rightarrow \mathbb{P}^1$ is a morphism [1, II.6]. The set of centers of the blow-ups giving rise to $\pi_{\mathcal{P}}$, that we denote by $BP(\mathcal{P})$, is called the *cluster of base points* of \mathcal{P} .

Set $(x := \frac{X}{Z}, y := \frac{Y}{Z})$ affine coordinates in the affine chart defined by $Z \neq 0$. Let us consider two homogeneous polynomials of the same degree $P(X, Y, Z), Q(X, Y, Z) \in \overline{\mathbb{F}}_p[X, Y, Z]$ (and without common components) and the associated pencil $\mathcal{P} = \mathcal{P}(P, Q)$. It is said that this pencil is *composite* if there exists a rational function of \mathbb{P}^1 , $r = \frac{R_1(X, Y)}{R_2(X, Y)}$ (R_1 and R_2 being homogeneous polynomials of the same degree ≥ 2) and a rational function g of \mathbb{P}^2 such that $f_{\mathcal{P}} = r \circ g$. Also, $\mathcal{P}(P, Q)$ is *irreducible* if all but finitely many curves of $\mathcal{P}(P, Q)$ are (absolutely) irreducible curves. A classical theorem of Bertini (valid in characteristic 0) that characterizes reducible linear systems was generalized for positive characteristic (see, for instance, either [19] and references therein, or [18, Th. 7.19], or [2, Th. 2.2]) giving rise, in the particular case of pencils (which are linear systems of dimension 1), to the following result:

Theorem 3.3. *Let $P(X, Y, Z)$ and $Q(X, Y, Z)$ as above. If the pencil $\mathcal{P}(P, Q)$ is not composite, then $\mathcal{P}(P, Q)$ is irreducible.*

The following corollary will be used in the proof of Lemma 8.10.

Corollary 3.4. *Let $P(X, Y, Z)$ and $Q(X, Y, Z)$ as above and let p be a base point of the pencil $\mathcal{P} = \mathcal{P}(P, Q)$ such that the multiplicities at p of all but finitely many of the curves in \mathcal{P} are equal to 1. Then \mathcal{P} is irreducible.*

Proof. We shall reason by contradiction. Therefore, assume that $\mathcal{P}(P, Q)$ is not irreducible. Then, by Theorem 3.3, $\mathcal{P}(P, Q)$ is a composite pencil. So, there exists a rational function r of \mathbb{P}^1 of degree ≥ 2 and a rational function $g = \frac{P'(X, Y, Z)}{Q'(X, Y, Z)}$ of \mathbb{P}^2 (P' and Q' are homogeneous polynomials of the same degree) such that $f_{\mathcal{P}} = r \circ g$. This implies that, on the one hand, p is a base point of the pencil $\mathcal{P}(P', Q')$ and, on the other hand, each element of $\mathcal{P}(P, Q)$ is a product of elements of $\mathcal{P}(P', Q')$.

These two facts lead to a contradiction because the multiplicity at p of a general element of $\mathcal{P}(P, Q)$ is 1. □

Consider a cluster of infinitely near points \mathcal{C} over \mathbb{P}^2 and a map $\mathbf{m} : \mathcal{C} \rightarrow \mathbb{N}$. For each positive integer d we shall denote by $\mathcal{L}_d(\mathcal{C}, \mathbf{m})$ the projectivisation of the vector space over $\overline{\mathbb{F}}_p$ of all homogeneous polynomials in $\overline{\mathbb{F}}_p[X, Y, Z]$ of degree d defining curves C of \mathbb{P}^2 such that the divisor $C^* - \sum_{p \in \mathcal{S}} \mathbf{m}(p)E_p^*$ (on the surface obtained after blowing-up the points in \mathcal{C}) is effective. The following lemma is proved in [3, Prop. 3.4] in a more general framework.

Lemma 3.5. *Assume that $\mathcal{P}(P, Q)$ is irreducible and set $d := \deg(P) = \deg(Q)$. Let $\mathbf{m} : BP(\mathcal{P}) \rightarrow \mathbb{N}$ be the map that assigns, to each $p \in BP(\mathcal{P})$, the multiplicity at p of a general element of $\mathcal{P}(P, Q)$. Then $\mathcal{L}_d(BP(\mathcal{P}), \mathbf{m}) = \mathcal{P}(P, Q)$.*

Lemma 3.6. *Let K be a subfield of $\overline{\mathbb{F}}_p$ and consider a cluster \mathcal{C} over \mathbb{P}^2 such that every $p \in \mathcal{C}$ is a K -rational point of the surface to which it belongs. Let d be a positive integer and let $\mathbf{m} : \mathcal{C} \rightarrow \mathbb{N}$ be a map. Then the projective space (over $\overline{\mathbb{F}}_p$) $\mathcal{L}_d(\mathcal{C}, \mathbf{m})$ has a basis whose elements are polynomials with coefficients in K .*

Proof. Consider an homogeneous polynomial of degree d with indeterminate coefficients. If one imposes the conditions defining $\mathcal{L}_d(\mathcal{C}, \mathbf{m})$ to this “generic” polynomial, it is obtained a system of linear equations with coefficients in K whose solution set is $\mathcal{L}_d(\mathcal{C}, \mathbf{m})$. The result follows trivially from this observation. □

4 Analysis of Singularities

Before we begin the proofs of our results towards Conjecture PN3, we need to study the singular points of the curve χ_t . The proof follows the same lines as the proof in [12], [13]. We first analyze the singular points, we find a description of them, count their number and multiplicity.

Let r be the residue of t modulo p , so we may write

$$t = p^i \ell + r \quad \text{with} \quad 0 \leq r < p$$

and where ℓ is not divisible by p . We similarly also write

$$\ell = ps + j \quad \text{with} \quad 0 < j < p$$

where this time s could be divisible by p .

Because x^t is planar iff x^{pt} is planar, we may assume that t is relatively prime to p , i.e., we may assume $r \neq 0$.

We proved Conjecture PN3 in the case that $t \equiv 1 \pmod{p}$ and $\ell \equiv 1 \pmod{p}$ in [13].

Theorem 4.1. *$x + y + 1$ divides $f_t(x, y)$ if and only if t is odd.*

Proof. We substitute $y = -x - 1$ in $f_t(x, y) = (x + 1)^t - x^t - (y + 1)^t + y^t$ obtaining $(x + 1)^t - x^t - (-1)^t(x)^t + (-1)^t(x + 1)^t$ which is identically zero if and only if t is odd. \square

Therefore, if t is odd then $g_t(x, y) = \frac{f_t(x, y)}{x - y}$ has an absolutely irreducible factor over \mathbb{F}_p , so x^t it is not a PN function over \mathbb{F}_{p^n} for infinitely many n .

We will assume from now that t is even. This implies that ℓ is odd. Moreover $\ell \geq 3$, because for $\ell = 1$, t is known to be PN (see Table 1).

Notice that

$$\begin{aligned} (x + a)^t &= (x^{p^i} + a^{p^i})^\ell (x + a)^r = \\ &= (x^{p^i\ell} + \binom{\ell}{1} x^{p^i(\ell-1)} a^{p^i} + \dots + \binom{\ell}{\ell-1} x^{p^i} a^{p^i(\ell-1)} + a^{p^i\ell}) \times \\ &= (x^r + \binom{r}{1} x^{r-1} a + \dots + \binom{r}{r-1} x a^{r-1} + a). \end{aligned}$$

To study the singularities we expand at the point $P = (\alpha, \beta)$, so then we need to study

$$f_t(x + \alpha, y + \beta) = (x + \alpha + 1)^t - (x + \alpha)^t - (y + \beta + 1)^t + (y + \beta)^t.$$

We write this as a sum of homogeneous parts

$$f_t(x + \alpha, y + \beta) = F_0 + F_1 + F_2 + \dots$$

where $F_i = F_i(x, y)$ is 0 or is a homogeneous polynomial of degree i . **This notation is fixed for the entire paper.** By definition, a point P is a *singular point* (or singularity) if and only if $F_0 = F_1 = 0$ at P . We compute that

$$\begin{aligned} F_0 &= ((\alpha + 1)^{p^i\ell+r} - \alpha^{p^i\ell+r} - (\beta + 1)^{p^i\ell+r} + \beta^{p^i\ell+r}), \\ F_1(x, y) &= \binom{r}{r-1} [((\alpha + 1)^{p^i\ell+r-1} - \alpha^{p^i\ell+r-1})x - ((\beta + 1)^{p^i\ell+r-1} - \beta^{p^i\ell+r-1})y], \\ F_2(x, y) &= \binom{r}{r-2} [((\alpha + 1)^{p^i\ell+r-2} - \alpha^{p^i\ell+r-2})x^2 - ((\beta + 1)^{p^i\ell+r-2} - \beta^{p^i\ell+r-2})y^2], \\ &\dots \\ F_u(x, y) &= \binom{r}{r-u} [((\alpha + 1)^{p^i\ell+r-u} - \alpha^{p^i\ell+r-u})x - ((\beta + 1)^{p^i\ell+r-u} - \beta^{p^i\ell+r-u})y], \\ &\dots \\ F_r(x, y) &= ((\alpha + 1)^{p^i\ell} - \alpha^{p^i\ell})x - ((\beta + 1)^{p^i\ell} - \beta^{p^i\ell})y, \\ F_{p^i}(x, y) &= jx^{p^i}((\alpha + 1)^{p^i(\ell-1)+r} - \alpha^{p^i(\ell-1)+r}) - jy^{p^i}((\beta + 1)^{p^i(\ell-1)+r} - \beta^{p^i(\ell-1)+r}), \\ F_{p^i+1}(x, y) &= \binom{r}{r-1} [jx^{p^i+1}((\alpha + 1)^{p^i(\ell-1)+r-1} - \alpha^{p^i(\ell-1)+r-1}) \\ &\quad - jy^{p^i+1}((\beta + 1)^{p^i(\ell-1)+r-1} - \beta^{p^i(\ell-1)+r-1})]. \end{aligned}$$

Lemma 4.2. *If $F_1(x, y) = F_2(x, y) = 0$ then $r = 0$ or 1.*

Proof. $F_1(x, y) = 0$ implies that $(\alpha + 1)^{p^i \ell + r - 1} - \alpha^{p^i \ell + r - 1} = 0 \Leftrightarrow (\frac{\alpha + 1}{\alpha})^{p^i \ell + r - 1} = 1$.

$F_2(x, y) = 0$ implies that $(\alpha + 1)^{p^i \ell + r - 2} - \alpha^{p^i \ell + r - 2} = 0 \Leftrightarrow (\frac{\alpha + 1}{\alpha})^{p^i \ell + r - 2} = 1$.

Hence

$$\left(\frac{\alpha + 1}{\alpha}\right)^{p^i \ell + r - 1} / \left(\frac{\alpha + 1}{\alpha}\right)^{p^i \ell + r - 2} = 1 \Leftrightarrow \left(\frac{\alpha + 1}{\alpha}\right) = 1 \Leftrightarrow 1 = 0.$$

But this is impossible. So, the only possibilities are:

- $F_1(x, y) \neq 0$ and the coefficient $\binom{r}{r-2} = 0$ in $F_2(x, y)$, i.e., $r = 0$ or 1 .
- Both coefficients are zero, $\binom{r}{r-2} = \binom{r}{r-1} = 0 \Leftrightarrow r = 0$.

This completes the proof. \square

A point P is singular iff $F_0 = F_1 = 0$ at P . Thus, we need to expand the expression $((\alpha + 1)^{p^i \ell + r - 1} - \alpha^{p^i \ell + r - 1}) =$

$$\begin{aligned} & \alpha^{p^i \ell + r - 1} + j\alpha^{p^i(\ell-1) + r - 1} + \dots + j\alpha^{p^i + r - 1} + \alpha^{r-1} + \\ & \binom{r-1}{1} \alpha^{p^i \ell + r - 2} + j \binom{r-1}{1} \alpha^{p^i(\ell-1) + r - 2} + \dots + j \binom{r-1}{1} \alpha^{p^i + r - 2} + \binom{r-1}{1} \alpha^{r-2} + \\ & \dots \\ & \binom{r-1}{r-2} \alpha^{p^i \ell + 1} + j \binom{r-1}{r-2} \alpha^{p^i(\ell-1) + 1} + \dots + j \binom{r-1}{r-2} \alpha^{p^i + 1} + \binom{r-1}{r-2} \alpha + \\ & \alpha^{p^i \ell} + j\alpha^{p^i(\ell-1)} + \dots + j\alpha^{p^i} + 1 - \alpha^{p^i(\ell-1) + r}. \end{aligned}$$

This is a complicated expression, therefore we distinguish different cases. Recall $t = p^i \ell + r$. Because x^t is planar iff x^{pt} is planar, we may assume that t is relatively prime to p , i.e., $r \neq 0$.

(A) $r \neq 1$.

(B) $r = 1$. We divide this case into two subcases:

(B.1) $\gcd(\ell, p^i - 1) < \ell$.

(B.2) $\gcd(\ell, p^i - 1) = \ell$.

In this paper we will prove many cases of (A) and essentially all of case (B).

Next we describe the singular points in the various cases.

4.1 Affine Singular Points in Case (A)

The analysis is straightforward in this case.

Lemma 4.3. *If $P = (\alpha, \beta)$ is a singular point and we are in case (A), then the multiplicity is $m_P(f_t) = 2$ and $m_P(g_t) = 2$ if $\alpha \neq \beta$ and $m_P(g_t) = 1$ otherwise.*

Proof. Since P is a singular point we have $F_1(x, y) = 0$. The multiplicity must be two because otherwise $F_2(x, y) = 0$ and then Lemma 4.2 would be false.

Moreover, if $\alpha = \beta$ then P is a point on the curve $x - y$ so the multiplicity decreases by one for $g_t(x, y)$. \square

Lemma 4.4. *If $P = (\alpha, \beta)$ is a singular point and we are in case (A), then the homogeneous component $F_2(x, y)$ is a product of two different lines.*

Proof. Remember that

$$F_2(x, y) = \binom{r}{r-2} [((\alpha + 1)^{p^i \ell + r - 2} - \alpha^{p^i \ell + r - 2})x^2 - ((\beta + 1)^{p^i \ell + r - 2} - \beta^{p^i \ell + r - 2})y^2].$$

We can rewrite this as

$$F_2(x, y) = \binom{r}{r-2} [(ax + by) * (ax - by)],$$

where $a = ((\alpha + 1)^{p^i \ell + r - 2} - \alpha^{p^i \ell + r - 2})^{1/2}$ and $b = ((\beta + 1)^{p^i \ell + r - 2} - \beta^{p^i \ell + r - 2})^{1/2}$. \square

4.2 Affine Singular Points in Case (B)

We always use the notation $P = (\alpha, \beta)$. Looking at the homogeneous components in $f_t(x, y)$ we obtain equations for the singular points.

Lemma 4.5. *$P = (\alpha, \beta)$ is a singular point of f_t if and only if*

$$(\alpha + 1)^{p^i \ell + 1} - \alpha^{p^i \ell + 1} - (\beta + 1)^{p^i \ell + 1} + \beta^{p^i \ell + 1} = 0 \quad (6)$$

$$(\alpha + 1)^\ell - \alpha^\ell = 0; (\beta + 1)^\ell - \beta^\ell = 0 \quad (7)$$

It follows from it that $f_t(x, y)$ has at most $(\ell - 1)^2$ singular points.

We need to compute the multiplicity of the singular points. The homogeneous component $F_{p^i}(x, y)$ is non-zero except when

$$(\alpha + 1)^{p^i(\ell-1)+1} - \alpha^{p^i(\ell-1)+1} = 0. \quad (8)$$

and

$$(\beta + 1)^{p^i(\ell-1)+1} - \beta^{p^i(\ell-1)+1} = 0. \quad (9)$$

Hence we conclude the following.

Lemma 4.6. *Let $P = (\alpha, \beta)$ be a singular point of f_t . Then $F_{p^i} = 0$ if and only if equations (6) and (7) hold together with*

$$\alpha^\ell = \beta^\ell \quad (10)$$

$$\alpha^{p^i-1} = \beta^{p^i-1} \quad (11)$$

Proof. From (6) and (7) we clearly have that $\alpha^\ell = \beta^\ell$.

Using (8) and (9) in (6) we obtain

$$\alpha^{p^i(\ell-1)+1} [(\alpha + 1)^{p^i} - \alpha^{p^i}] - \beta^{p^i(\ell-1)+1} [(\beta + 1)^{p^i} - \beta^{p^i}] = 0,$$

which is equal to

$$\alpha^{p^i(\ell-1)+1} - \beta^{p^i(\ell-1)+1} = 0.$$

Multiplying it by $\alpha^{p^i} \beta^{p^i}$ we get,

$$\alpha^{p^i \ell + 1} \beta^{p^i} - \beta^{p^i \ell + 1} \alpha^{p^i} = 0.$$

Since $\alpha^\ell = \beta^\ell$ the latter is equivalent to $\alpha \beta^{p^i} = \beta \alpha^{p^i} = 0 \Leftrightarrow \alpha^{p^i-1} = \beta^{p^i-1}$. \square

Thus a singular point (α, β) has homogeneous component $F_{p^i} = 0$ if and only if $\alpha = \beta E$ where $E^d = 1$, and $d = \gcd(\ell, p^i - 1)$.

How many such points there are is the next issue.

Lemma 4.7. *In case (B) there are at most $(d-1)^2$ singular points (α, β) such that $F_{p^i} = 0$, where $d = \gcd(\ell, p^i - 1)$.*

Proof. $F_{p^i}(x + \alpha, y + \beta) = 0$ if and only if

$$\begin{aligned}\alpha^\ell &= \beta^\ell \\ (\alpha + 1)^\ell - \alpha^\ell &= 0; (\beta + 1)^\ell - \beta^\ell = 0 \\ (\alpha + 1)^{p^i(\ell-1)+1} - \alpha^{p^i(\ell-1)+1} &= 0. \\ (\beta + 1)^{p^i(\ell-1)+1} - \beta^{p^i(\ell-1)+1} &= 0.\end{aligned}$$

Equivalently

$$\begin{aligned}(\alpha/\beta)^\ell &= 1 \\ (1 + 1/\alpha)^\ell &= 1; (1 + 1/\beta)^\ell = 1 \\ (1 + 1/\alpha)^{p^i(\ell-1)+1} &= 1. \\ (1 + 1/\beta)^{p^i(\ell-1)+1} &= 1.\end{aligned}$$

Doing the change of coordinates $1/\alpha = a$ and $1/\beta = b$ we get

$$\begin{aligned}(b/a)^\ell &= 1 \\ (1 + a)^\ell &= 1; (1 + b)^\ell = 1 \\ (1 + a)^{p^i(\ell-1)+1} &= 1. \\ (1 + b)^{p^i(\ell-1)+1} &= 1.\end{aligned}$$

Doing the change of coordinates $a = a_1 - 1$ and $b = b_1 - 1$ we get

$$\begin{aligned}(b_1 - 1)^\ell &= (a_1 - 1)^\ell \\ (a_1)^\ell &= 1; (b_1)^\ell = 1 \\ (a_1)^{p^i(\ell-1)+1} &= 1. \\ (b_1)^{p^i(\ell-1)+1} &= 1.\end{aligned}$$

Moreover for any pair (a_1, b_1) satisfying this equations with $a_1, b_1 \neq 1$ there is a singular point (α, β) with $F_{p^i}(x + \alpha, y + \beta) = 0$.

Notice that

$$(a_1)^\ell / (a_1)^{p^i(\ell-1)+1} = a_1^{p^i-1} = 1$$

and

$$(b_1)^\ell / (b_1)^{p^i(\ell-1)+1} = b_1^{p^i-1} = 1.$$

Therefore $a_1^d = 1 = b_1^d$, where $d = \gcd(\ell, p^i - 1)$. So we conclude that there is at most $(d-1)^2$ singular points (α, β) with $F_{p^i} = 0$. \square

Corollary 4.8. *In case (B.1) there are at most $(\ell/3 - 1)^2$ singular points (α, β) with $\alpha \neq \beta$ and $F_{p^i} = 0$.*

Proof. Since $t = p^i\ell + 1$ is even then ℓ is odd, so d is odd as well. Since $\gcd(\ell, p^i - 1) < \ell$ both odd then $d \leq \ell/3$. Hence we have at most $(\ell/3 - 1)^2$ points. \square

Finally, we have a lemma concerning the component of degree $p^i + 1$. We will come back to use this in Section 4.5.

Lemma 4.9. *$F_{p^i+1} = Ax^{p^i+1} - By^{p^i+1}$, where $A = (\alpha + 1)^{p^i(\ell-1)} - \alpha^{p^i(\ell-1)}$ and $B = (\beta + 1)^{p^i(\ell-1)} - \beta^{p^i(\ell-1)}$.*

So the multiplicity is at most $p^i + 1$, and it is actually $p^i + 1$ unless equations (10) and (11) hold.

4.3 Singular Points at Infinity

Next we consider singular points at infinity. The projective curve we are working with is $f_t(x, y, z) = [(x + z)^t - x^t - (y + z)^t + y^t]/z$. After cancelling terms we get, $f_t(x, y, z) = tx^{t-1} - ty^{t-1} + z(\text{lower order terms})$. The next result explains when there are singular points at infinity (the chart where $z = 0$).

Lemma 4.10. *There are no singular points at infinity in case (A). In case (B.1) $(\alpha, 1, 0)$ is a singular point of $f_t(x, y, z)$ if and only if $\alpha^{t-1} = 1$, which is equivalent to $\alpha^\ell = 1$.*

Proof. The dehomogenization of $f_t(x, y, z) = [(x + z)^t - x^t - (y + z)^t + y^t]/z$ relative to y is $f'_t(x, z) = f_t(x, 1, z)/z$. We compute

$$\begin{aligned}
f'_t(x + \alpha, z) &= [(x + z + \alpha)^t - (x + \alpha)^t - (z + 1)^t + 1]/z \\
&= 1/z[(x + z)^t + \binom{t}{t-1}(x + z)^{t-1}\alpha + \dots + \binom{t}{1}(x + z)\alpha^{t-1} + \alpha^t \\
&\quad - x^t - \binom{t}{t-1}(x)^{t-1}\alpha - \dots - \binom{t}{1}(x)\alpha^{t-1} - \alpha^t \\
&\quad - z^t - \binom{t}{t-1}(z)^{t-1} - \binom{t}{t-2}(z)^{t-2} - \dots - \binom{t}{1}(z) - 1 + 1] \\
&= \binom{t}{1}(\alpha^{t-1} - 1) + \binom{t}{2}[(\alpha^{t-2} - 1)z + 2\alpha^{t-2}x] \\
&\quad + \text{higher order terms.}
\end{aligned}$$

Notice that the linear part cannot be zero, unless the coefficient $\binom{t}{2} = 0$, which implies $r = 0$ or 1 . Therefore, there are no singular points in case (A). And if $r = 1$, then P is a singular point iff $\alpha^{t-1} - 1 = 0$. \square

The $'$ notation always refers to expansions at infinity.

Lemma 4.11. *In case (B) let $(\alpha, 1, 0)$ be a singular point of $g'_t(x, z)$ at infinity. Then:*

$$F'_{p^{i-1}} = z^{p^i-1}(\alpha^{p^i(\ell-1)+1} - 1).$$

$$F'_{p^i} = z^{p^i}(\alpha^{p^i(\ell-1)} - 1) + (xz^{p^i-1} + x^{p^i})\alpha^{p^i(\ell-1)}.$$

Proof.

$$f_t(x + \alpha + 1, z) = 1/z[(x + z + \alpha)^t - (x + \alpha)^t - (z + 1)^t + 1] =$$

$$1/z[((x + z)^{p^i\ell+1} + j(x + z)^{p^i(\ell-1)+1}\alpha^{p^i} + \dots + j(x + z)^{p^i+1}\alpha^{p^i(\ell-1)} + (x + z)\alpha^{p^i\ell} +$$

$$(x + z)^{p^i\ell}\alpha + j(x + z)^{p^i(\ell-1)}\alpha^{p^i+1} + \dots + j(x + z)^{p^i}\alpha^{p^i(\ell-1)+1} + \alpha^{p^i\ell+1}$$

$$- (x)^{p^i\ell+1} - j(x)^{p^i(\ell-1)+1}\alpha^{p^i} - \dots - j(x)^{p^i+1}\alpha^{p^i(\ell-1)} - (x)\alpha^{p^i\ell}$$

$$- (x)^{p^i\ell}\alpha - j(x)^{p^i(\ell-1)}\alpha^{p^i+1} - \dots - j(x)^{p^i}\alpha^{p^i(\ell-1)+1} - \alpha^{p^i\ell+1}$$

$$- (z)^{p^i\ell+1} - j(z)^{p^i(\ell-1)+1} - \dots - j(z)^{p^i+1} - (z)$$

$$- (z)^{p^i\ell} - j(z)^{p^i(\ell-1)} - \dots - (z)^{p^i} - 1 + 1)].$$

Therefore we get:

$$F'_{p^{i-1}} = jz^{p^i-1}(\alpha^{p^i(\ell-1)+1} - 1).$$

$$F'_{p^i} = jz^{p^i}(\alpha^{p^i(\ell-1)} - 1) + j(xz^{p^i-1} + x^{p^i})\alpha^{p^i(\ell-1)}.$$

□

Lemma 4.12. *In case (B) let $(\alpha, 1, 0)$ be a singular point of $g'_t(x, z)$ at infinity. Then the multiplicity at P is p^i if $\alpha \in \mathbb{F}_{p^i}$, and is $p^i - 1$ otherwise.*

Proof. Since $P = (\alpha, 1, 0)$ is a singular point at the infinity we know that $\alpha^\ell = 1$. Moreover $F_{p^i} = 0$ iff $\alpha^{p^i(\ell-1)+1} - 1 = 0$. Multiplying the last equation by α^{p^i} we equivalently obtain $\alpha^{p^i(\ell)+1} - \alpha^{p^i} = 0 \Leftrightarrow \alpha^{p^i-1} = 1 \Leftrightarrow \alpha \in \mathbb{F}_{p^i}$. This completes the proof. □

4.4 The Multiplicities

Next we pin down the multiplicities of these singular points $P = (\alpha, \beta)$ on $f_t(x, y)$, and how things change for $g_t(x, y)$. Recall that the ' notation always refers to expansions at infinity.

We classify the points into the following types:

- (I) $\alpha^d = \beta^d$, i.e., $F_{p^i} = 0$.
- (II) $\alpha^d \neq \beta^d$, i.e., $F_{p^i} \neq 0$.
- (III) $(\alpha, 1, 0)$ is a singular point at infinity.
 - (III.A) $\alpha \in \mathbb{F}_{p^i}$, i.e., $F'_{p^{i-1}} = 0$.
 - (III.B) $\alpha \notin \mathbb{F}_{p^i}$, i.e., $F'_{p^{i-1}} \neq 0$.

We note that if $\ell = 1$ and $i > 1$, the only singular point is $(-2, -2)$.

Defining $w(x, y) := x - y$ we note the following multiplicities on w : $m_P(w) = 1$ if $P = (\alpha, \alpha)$ (Type II), and $m_P(w) = 0$ for all other singular points $P = (\alpha, \beta)$. We now have the multiplicities for $g_t(x, y)$.

Type	Number of Points	$m_P(f_k)$	$m_P(g_t)$
I	$N_1 \leq (\ell/3 - 1)^2$ if $\gcd(\ell, p^i - 1) < \ell$ $N_1 \leq (\ell - 1)^2$ if $\gcd(\ell, p^i - 1) = \ell$	$p^i + 1$	$\leq p^i + 1$
II	$\leq (\ell - 1)^2 - N_1$	p^i	$\leq p^i$
III.A	$N_2 \leq \ell$	p^i	$\leq p^i$
III.B	$\ell - N_2$	$p^i - 1$	$\leq p^i - 1$

4.5 Further Analysis

Next we need some further analysis of the singularities and the homogeneous components.

The following result is clear, because we are in characteristic p .

Lemma 4.13. $F_{p^i} = (\sigma x - \tau y)^{p^i}$ where $\sigma^{p^i} = ((\alpha + 1)^{p^i(\ell-1)+1} - \alpha^{p^i(\ell-1)+1})$ and $\tau^{p^i} = ((\beta + 1)^{p^i(\ell-1)+1} - \beta^{p^i(\ell-1)+1})$. $F'_{p^i} = (Uz)^{p^i}$ where $U^{p^i} = j(\alpha^{p^i(\ell-1)+1} - 1)$.

Lemma 4.14. $F_{p^{i+1}}$ (resp F'_{p^i}) consists of $p^i + 1$ (resp p^i) different linear factors.

Proof. We have seen that $F_{p^{i+1}} = Ax^{p^{i+1}} - By^{p^{i+1}}$. Consider $h(x) = F_{p^{i+1}}(x, 1) = Ax^{p^{i+1}} - B$. If $h(x)$ has a repeated root at a then $h'(a) = 0$. Consider the derivative $h'(x) = Ax^{p^i}$ which is never zero only for $x = 0$ which is not a root of h therefore there are no repeated factors in $F_{p^{i+1}}$. Same arguments may be used to prove the result for F'_{p^i} . \square

Next we make a crucial observation for our proofs. For the rest of this paper, we let $L = \sigma x - \tau y$, so that $F_{p^i} = L^{p^i}$. Suppose $g_t(x, y) = u(x, y)v(x, y)$, and suppose that the Taylor expansion at a singular point $P = (\alpha, \beta)$ is

$$u(x + \alpha, y + \beta) = L^{r_1} + u_1, \quad v(x + \alpha, y + \beta) = L^{r_2} + v_1$$

where wlog $r_1 \leq r_2$. Then $F_{p^{i+1}} = L^{r_1}(v_1 + L^{r_2-r_1}u_1)$. From Lemma 4.14 we deduce the following.

Lemma 4.15. *With the notation of the previous paragraph,*

- (i) *Either $r_1 = 1$ or $r_1 = 0$.*
- (ii) *If $r_1 = 1$ then $\gcd(L, v_1 + L^{r_2-r_1}u_1) = 1$.*

We next make two quick remarks to aid us in moving between $f_t(x, y)$ and $g_t(x, y)$. Suppose that $P = (\alpha, \beta) \neq (1, 1)$ is a singular point of $g_t(x, y)$ such that $F_{p^i}(x, y) \neq 0$ at P (type II). We will need to know the greatest common divisor

$(G_m(x, y), G_{m+1}(x, y))$ where $m = m_P(g_t)$. This can be found from $(F_{p^i}(x, y), F_{p^{i+1}}(x, y))$ as follows.

Again letting $w(x, y) = x - y$, we have

$$f_t(x + \alpha, y + \beta) = w(x + \alpha, y + \beta)g_t(x + \alpha, y + \beta),$$

and so

$$F_{p^i}(x, y) + F_{p^{i+1}}(x, y) + \cdots = (W_0 + W_1(x, y))(G_m(x, y) + G_{m+1}(x, y) + \cdots).$$

where polynomials with subscript i are 0 or homogeneous of degree i .

Remark 4.1. We get:

If $W_0 \neq 0$, i.e., $\alpha \neq \beta$

$$\begin{aligned} F_{p^i} &= W_0 G_{p^i} = (\sigma x + \tau y)^{2^i} \\ F_{p^{i+1}} &= W_1 G_{p^i} + W_0 G_{p^{i+1}} \end{aligned} \quad (12)$$

then it follows from these equations that $(F_{2^i}, F_{2^{i+1}}) = (G_{2^i}, G_{2^{i+1}})$.

If $W_0 = 0$, i.e., $\alpha = \beta$,

$$\begin{aligned} F_{p^i} &= W_1 G_{p^{i-1}} = (\sigma x + \tau y)^{2^i} \\ F_{p^{i+1}} &= W_1 G_{p^i}. \end{aligned} \quad (13)$$

it is clear that (up to scalars) $W_1 = \sigma x - \tau y$, and so $(F_{p^i}, F_{p^{i+1}}) = \sigma x - \tau y$ because $F_{p^{i+1}}(x, y)$ has distinct linear factors (Lemma 4.14). Hence $(G_{p^{i-1}}, G_{p^i}) = 1$. The same result is true for the points at infinity of type *III.B*, i.e., $(G'_{p^{i-1}}, G'_{p^i}) = 1$.

5 Intersection Multiplicity

In this section we compute and give bounds on the intersection multiplicities.

Lemma 5.1. *Let $h(x, y)$ be an affine curve. Write $h(x + \alpha, y + \beta) = H_m + H_{m+1} + \cdots$ where $P = (\alpha, \beta)$ is a point on $h(x, y)$ of multiplicity m . Suppose that H_m and H_{m+1} are relatively prime, and that there is only one tangent direction at P . If $h = uv$ is reducible, then $I(P, u, v) = 0$.*

Proof: See [16].

5.1 Type I

We upper bound the intersection multiplicity at the Type I point.

Lemma 5.2. *If $g_t(x, y) = u(x, y)v(x, y)$ and P is of Type I then $I(P, u, v) \leq (\frac{p^i+1}{2})^2$.*

Proof: Let P be of Type I. We know that $m_P(g_t) = p^i + 1 = m_P(u) + m_P(v)$. From Lemma 4.14 we know that $F_{p^{i+1}}$ has $p^i + 1$ different linear factors. Thus, $I(P, u, v) = m_p(u)m_p(v)$. This quantity is maximized when $m_P(u) = m_P(v)$ and in this case $m_p(u)m_p(v) = (\frac{p^i+1}{2})^2$.

5.2 Type II

We show that there are two possibilities for the intersection multiplicity at a Type II point.

Lemma 5.3. *Suppose we are in case (B). If $g_t(x, y) = u(x, y)v(x, y)$ and $P = (\alpha, \beta)$ is a point of type (II) then either $I(P, u, v) = p^i$ or $I(P, u, v) = 0$.*

Proof: Assume $g_t(x, y) = u(x, y)v(x, y)$. Since P is not on $w(x, y) = x - y$ by Lemma 4.15 we know that $m_P(u)$ is either 1 or 0. If $m_P(u) = 0$ then $I(P, u, v) = 0$. If $m_P(u) = 1$ we proceed as follows.

Let $L(x, y) = \sigma x + \tau y$ and suppose (from the proof of Lemma 4.15) we have the following Taylor expansions at P :

$$\begin{aligned} u(x + \alpha, y + \beta) &= L(x, y) + U_2(x, y) + \cdots \\ v(x + \alpha, y + \beta) &= L(x, y)^{p^i-1} + V_{p^i}(x, y) + \cdots \end{aligned}$$

It follows that

$$u(x + \alpha, y + \beta)L(x, y)^{p^i-2} - v(x + \alpha, y + \beta) = L(x, y)^{p^i-2}U_2(x, y) - V_{p^i}(x, y) + \cdots.$$

By definition of intersection multiplicity we have

$$I(P, u, v) = I(0, u(x + \alpha, y + \beta), u(x + \alpha, y + \beta)L(x, y)^{p^i-2} - v(x + \alpha, y + \beta))$$

so we compute the right-hand side. Notice that $L(x, y) \nmid L(x, y)^{p^i-2}U_2(x, y) - V_{p^i}(x, y)$ because if $L(x, y)$ divides $L(x, y)^{p^i-2}U_2(x, y) - V_{p^i}(x, y)$ then $L(x, y)$ also divides $V_{p^i}(x, y)$. Hence, $L(x, y)^2$ divides $L(x, y)(L(x, y)^{p^i-2}U_2(x, y) + V_{p^i}(x, y)) = G_{p^{i+1}}(x, y)$ which is a contradiction.

Therefore, $u(x + \alpha, y + \beta)$ and $u(x + \alpha, y + \beta)L^{p^i-2} - v(x + \alpha, y + \beta)$ have different tangent cones. It follows from a property of $I(P, u(x, y), v(x, y))$ that

$$\begin{aligned} I(0, u(x + \alpha, y + \beta), u(x + \alpha, y + \beta)L^{p^i-2} - v(x + \alpha, y + \beta)) &= \\ m_0(u(x + \alpha, y + \beta))m_0(u(x + \alpha, y + \beta)L^{p^i-2} - v(x + \alpha, y + \beta)) &= p^i. \end{aligned}$$

5.3 Type III

Next result is equivalent to Type I with using multiplicity p^i instead.

Lemma 5.4. *If $g_t(x, y) = u(x, y)v(x, y)$ and $P = (\alpha, \beta)$ is a point of type (III.A) then $I(P, u, v) \leq p^{2i}/4$.*

We show that intersection multiplicities at Type III.B points are 0, so these points may be disregarded.

Lemma 5.5. *If $g_t(x, y) = u(x, y)v(x, y)$ and $P = (\alpha, \beta)$ is a point of type (III.B) then $I(P, u, v) = 0$.*

Proof: Notice that $\gcd(F'_{p^{i-1}}, F'_{p^i}) = 1$ and therefore $\gcd(G'_{p^{i-1}}, G'_{p^i}) = 1$ by Remark 4.1. The proof concludes using Lemma 5.1.

5.4 Case A

Lemma 5.6. *If P is a singular affine point, and we are in case (A), and $g_t = g_1 \cdots g_r$ over the algebraic closure $\overline{\mathbb{F}_p}$, then there are at most two indices i, j such that $g_i(P) = g_j(P) = 0$ with multiplicity $m_P(g_i) = m_P(g_j) = 1$. Moreover $I(P, g_i, g_j) \leq 1$.*

Proof. From Lemma 4.3 we know that $m_P(g_t) \leq 2$ therefore there are at most 2 factors of g_t containing P , otherwise it would have more multiplicity. Moreover from Lemma 4.4 we know that the tangent cone of g_t at P is a pair of different lines, then $I(P, g_i, g_j) = m_p(g_i)m_p(g_j) \leq 1$. \square

6 Case B: Proof assuming $g_t(x, y)$ irreducible over \mathbb{F}_p

Here is a well known result, its proof can be found in [20].

Lemma 6.1. *Suppose that $p(\underline{x}) \in \mathbb{F}_q[x_1, \dots, x_n]$ is of degree t and is irreducible in $\mathbb{F}_q[x_1, \dots, x_n]$. Let \mathbb{K} be a finite field extension of \mathbb{F}_q . Then there exists a \mathbb{K} -irreducible polynomial $h(\underline{x})$ such that the factorization of $p(\underline{x})$ into \mathbb{K} -irreducible polynomials is*

$$p(\underline{x}) = c \prod_{\sigma \in G} \sigma(h(\underline{x})),$$

where $G = \text{Gal}(\mathbb{K}/\mathbb{F}_q)$ and $c \in \mathbb{F}_q$. Furthermore if $p(\underline{x})$ is homogeneous, then so is $h(\underline{x})$.

In particular, there exists $r \mid t$ and an absolutely irreducible polynomial $m(\underline{x}) \in \mathbb{F}_{q^r}[x_1, \dots, x_n]$ of degree $\frac{t}{r}$ such that

$$p(\underline{x}) = d \prod_{\sigma \in G'} \sigma(m(\underline{x})),$$

where $G' = \text{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ and $d \in \mathbb{F}_q$.

Remark 6.1. Notice that if $u(x, y) = \sum a_{i,j} x^i y^j$ then $\sigma(u(x, y)) = \sum \sigma(a_{i,j}) x^i y^j$ where $\sigma \in G$ is the Frobenius map (or a power of it). Therefore, u and $\sigma(u)$ have the same monomials and only differ in some coefficients. This means that both u and $\sigma(u)$ have the same degree.

Theorem 6.2. *Suppose we are in case (B.1) and that $g_t(x, y)$ is irreducible over \mathbb{F}_p . Then $g_t(x, y)$ is absolutely irreducible whenever:*

- either $p \geq 5$, $i \geq 1$ and $\ell > 1$,
- or $p = 3$, $i \geq 2$ and $\ell > 1$.

Proof. Suppose not, then $g_t(x, y, z) = u(x, y, z)v(x, y, z)$. Using Remark 6.1 we have that $\deg(u) = \deg(v) = (p^i \ell - 1)/2$. We apply Bezout's Theorem to u and v :

$$\sum_{P \in \text{Sin}(g)} I(P, u, v) = \deg(u)\deg(v) = ((p^i \ell - 1)/2)^2. \quad (14)$$

We can bound the left hand side as follows,

$$\sum_{P \in \text{Sing}(g_t)} I(P, u, v) = \sum_{P \in I} I(P, u, v) + \sum_{P \in II} I(P, u, v) + \sum_{P \in III.A} I(P, u, v) \quad (15)$$

$$\leq \frac{(p^i + 1)^2}{4}(\ell/3 - 1)^2 + \frac{4}{4}p^i[(\ell - 1)^2 - (\ell/3 - 1)^2] + \frac{p^{2i}}{4}\ell \quad (16)$$

We have that (14) \leq (16) by Bezout's Theorem, so if we prove that (14) $>$ (16) we get a contradiction. The inequality (14) $>$ (16) is

$$p^{2i}\ell^2 - 2p^i\ell + 1 > (p^{2i} + 2p^i + 1)(\ell^2/9 - 2/3\ell + 1) + 4p^i(\ell^2 - 2\ell + 1 - \ell^2/9 + 2/3\ell - 1) + p^{2i}\ell \quad (17)$$

$$p^{2i}(\ell^2 - \ell^2/9 + 2/3\ell - 1 - \ell) > p^i(2\ell - 2(\ell^2/9 - 2/3\ell + 1) + 4(\ell^2 - 2\ell + 1)) + (\ell^2/9 - 2/3\ell) \quad (18)$$

$$p^{2i}(\frac{8}{9}\ell^2 - \frac{1}{3}\ell - 1) > p^i(\frac{34}{9}\ell^2 - \frac{14}{3}\ell + 2) + (\ell^2/9 - 2/3\ell) \quad (19)$$

$$1 > \frac{(\frac{34}{9}\ell^2 - \frac{14}{3}\ell + 2)}{p^i(\frac{8}{9}\ell^2 - \frac{1}{3}\ell - 1)} + \frac{(\ell^2/9 - 2/3\ell)}{p^{2i}(\frac{8}{9}\ell^2 - \frac{1}{3}\ell - 1)} \quad (20)$$

Notice that in one hand we have that

$$\begin{aligned} \frac{(\frac{34}{9}\ell^2 - \frac{14}{3}\ell + 2)}{(\frac{8}{9}\ell^2 - \frac{1}{3}\ell - 1)} &\leq \frac{34}{8} \Leftrightarrow (\frac{34}{9}\ell^2 - \frac{14}{3}\ell + 2) \leq (\frac{34}{9}\ell^2 - \frac{34}{24}\ell - 34/8) \\ &\Leftrightarrow 78/24\ell \geq 50/8 \Leftrightarrow \ell \geq 150/78 \quad \ell \geq 3. \end{aligned}$$

In the other hand we have that

$$\begin{aligned} \frac{(\ell^2/9 - 2/3\ell)}{(\frac{8}{9}\ell^2 - \frac{1}{3}\ell - 1)} &< \frac{1}{8} \Leftrightarrow (\ell^2/9 - 2/3\ell) < (\frac{1}{9}\ell^2 - \frac{1}{24}\ell - \frac{1}{8}) \\ &\Leftrightarrow \frac{15}{24}\ell > \frac{1}{8} \Leftrightarrow \ell > \frac{1}{5} \quad \ell \geq 1 \end{aligned}$$

So the right hand side in equation (20) is less than $\frac{34}{8p^i} + \frac{1}{8p^{2i}}$ it is less than one if either $p > 4$ for any $i \geq 1$ or $p = 3$ for any $i \geq 2$. □

Theorem 6.3. *Suppose we are in case (B.2) but $\ell < p^i - 1$, and suppose that $g_t(x, y)$ is irreducible over \mathbb{F}_p then $g_t(x, y)$ is absolutely irreducible.*

Proof. First of all notice that since $\gcd(\ell, p^i - 1) = \ell < p^i - 1$ then $\ell \mid p^i - 1$, hence $p^i - 1 \geq 2\ell \Leftrightarrow p^i \geq 2(\ell - 1) + 3$.

Suppose not, then $g_t(x, y, z) = u(x, y, z)v(x, y, z)$. Using Remark 6.1 we have that $\deg(u) = \deg(v) = (p^i\ell - 1)/2$. We apply Bezout's Theorem to u and v :

$$\sum_{P \in \text{Sin}(g)} I(P, u, v) = \deg(u)\deg(v) = ((p^i\ell - 1)/2)^2. \quad (21)$$

We can bound the left hand side as follows,

$$\sum_{P \in \text{Sing}(g_t)} I(P, u, v) = \sum_{P \in I} I(P, u, v) + \sum_{P \in II} I(P, u, v) + \sum_{P \in III.A} I(P, u, v) \quad (22)$$

Since $d = \ell$ then all the singular points are of type I and no points of type II . Between the points of type I we have $(\ell - 1)(\ell - 2)$ with both coordinates different and $(\ell - 1)$ with both coordinates equal and therefore intersection multiplicity at most $p^{2i}/4$.

$$(22) \leq \frac{(p^{2i} + 2p^i + 1)(\ell - 1)(\ell - 2)}{4} + \frac{p^{2i}(\ell - 1)}{4} + \frac{p^{2i}\ell}{4} \quad (23)$$

We have that (21) \leq (23) by Bezout's Theorem, so if we prove that (21) $>$ (23) we get a contradiction.

$$p^{2i}\ell^2 - 2p^i\ell + 1 > (p^{2i} + 2p^i + 1)(\ell^2 - 3\ell + 2) + p^{2i}(\ell - 1) + p^{2i}\ell \quad (24)$$

$$p^{2i}(\ell - 1) > 2p^i(\ell^2 - 2\ell + 2) + (\ell^2 - 3\ell + 2) = 2p^i(\ell - 1)^2 + 2p^i + (\ell^2 - 3\ell + 2) \quad (25)$$

$$p^i > 2(\ell - 1) + \frac{2}{\ell - 1} + \frac{\ell - 2}{p^i} \quad (26)$$

Remember that $p^i \geq 2(\ell - 1) + 3$ and $\ell \geq 3$ then .

$$2(\ell - 1) + \frac{2}{\ell - 1} + \frac{\ell - 2}{p^i} \leq 2(\ell - 1) + 1 + \frac{1}{2} < 2(\ell - 1) + 3 \leq p^i.$$

□

Remark 6.2. Notice that the latter proof does not hold for $\ell = 1$ as it should be, because it is already known that $t = p^i + 1$ is a exceptional number.

Remark 6.3. Only left to prove the case $\ell = p^i - 1$, i.e., $t = p^{2i} - p^i + 1$.

7 Case B: Proof assuming $g_t(x, y)$ not irreducible over \mathbb{F}_p

Suppose $g_t = f_1 \cdots f_r$ is the factorization into irreducible factors over \mathbb{F}_p . Let $f_j = f_{j,1} \cdots f_{j,n_j}$ be the factorization of f_j into n_j absolutely irreducible factors. Each $f_{j,s}$ has degree $\deg(f_j)/n_j$.

Lemma 7.1. *If P is a point of type II then one of the following holds:*

1. $m_P(f_{j,s}) = 0$ for all $j \in \{1, \dots, r\}$ and $s \in \{1, \dots, n_j\}$ except for a pair (j_1, s_1) with $m_P(f_{j_1, s_1}) = p^i$.

2. $m_P(f_{j,s}) = 0$ for all $j \in \{1, \dots, r\}$ and $s \in \{1, \dots, n_j\}$ except for two pair (j_1, s_1) and (j_2, s_2) with $m_P(f_{j_1, s_1}) = 1$ and $m_P(f_{j_2, s_2}) = p^i - 1$.

Proof. This is a consequence of Lemma 4.13 and Lemma 4.15. Consider $u = f_{a,b}$ and $v = \prod_{j \neq a, s \neq b} f_{j,s}$ from Lemma 4.15 we know that $m_P(f_{a,b})$ is either 0 or 1 or $p^i - 1$ or p^i (resp $m_p(v)$ is either p^i or $p^i - 1$ or 1 or 0). But this is true for any pair (a, b) .

Clearly no two components $f_{a,b}$ and $f_{a',b'}$ has multiplicity greater than or equal to $p^i - 1$ because the total multiplicity $m_P(g_t) = p^i$. And there are no two components $f_{a,b}$ and $f_{a',b'}$ with multiplicity equal to 1, because then $u = f_{a,b}f_{a',b'}$ has L two times in the tangent cone and $v = g/u$ has L^{p^i-2} in the tangent cone which is impossible. Hence the only possibilities are:

- (i) There exists (a, b) with $m_P(f_{a,b}) = p^i$, and $m_P(f_{j,s}) = 0$ for $(j, s) \neq (a, b)$.
- (ii) There exist (a, b) and (a', b') with $m_P(f_{a,b}) = 1$ and $m_P(f_{a',b'}) = p^i - 1$, and $m_P(f_{j,s}) = 0$ for $(j, s) \neq (a, b)$, $(j, s) \neq (a', b')$.

□

Lemma 7.2. *If P is a point of type I or III.A, then for any two components $f_{a,b}$ and $f_{a',b'}$ we have that $I(P, f_{a,b}, f_{a',b'}) = m_P(f_{a,b})m_P(f_{a',b'})$.*

Proof. From Lemma 4.14 the tangent cones of $f_{a,b}$ and $f_{a',b'}$ has no common factors. □

Lemma 7.3. *If P is a point of type III.B, then for any two components $f_{a,b}$ and $f_{a',b'}$ we have that $I(P, f_{a,b}, f_{a',b'}) = 0$.*

Proof. Consider $u = f_{a,b}$ and $v = g_m/u$. From Lemma 5.3 we know that $I(P, u, v) = 0 = \sum_{(j,s) \neq (a,b)} I(P, u, f_{j,s})$, then $I(P, f_{a,b}, f_{a',b'}) = 0$. □

Lemma 7.4. *Let P is a point of type II and $g_t(x, y) = \prod_{j=1}^r \prod_{s=1}^{n_j} f_{j,s}$. The intersection multiplicity $I(P, f_{a,b}, f_{a',b'})$ of any two components $f_{a,b}$ and $f_{a',b'}$ is either 0 or p^i .*

Proof. Consider $u = f_{a,b}$ and $v = g_m/u$. From Lemma 5.3 we know that either $I(P, u, v) = 0 = \sum_{(j,s) \neq (a,b)} I(P, u, f_{j,s})$, then $I(P, f_{a,b}, f_{a',b'}) = 0$ or $I(P, u, v) = 2^i = \sum_{(j,s) \neq (a,b)} I(P, u, f_{j,s})$ using Lemma 7.1 we have that there exists (a', b') with $I(P, f_{a,b}, f_{a',b'}) = p^i$. □

We need some more technical results for the main theorem, which give us some upper bounds.

Lemma 7.5.

- (i) *If $g_t(x, y)$ does not have an absolutely irreducible factor over \mathbb{F}_p , then,*

$$\sum_{j=1}^r \deg(f_j)^2 / n_j < \deg(g_t)^2 / 2. \quad (27)$$

(ii)

$$\begin{aligned} \sum_{j=1}^r \sum_{1 \leq i < s \leq n_j} \sum_{P \in \text{Sing}(g_t)} I(P, f_{j,i}, f_{j,s}) + \sum_{1 \leq j < l \leq r} \sum_{\substack{1 \leq i \leq n_j \\ 1 \leq s \leq n_l}} \sum_{\substack{P \in \text{Sing}(g_t) \\ P \in II}} I(P, f_{j,i}, f_{l,s}) \\ \leq p^i((\ell - 1)^2 - N_1) \end{aligned}$$

(iii)

$$\begin{aligned} \sum_{j=1}^r \sum_{1 \leq i < s \leq n_j} \sum_{P \in \text{Sing}(g_t)} I(P, f_{j,i}, f_{j,s}) + \sum_{1 \leq j < l \leq r} \sum_{\substack{1 \leq i \leq n_j \\ 1 \leq s \leq n_l}} \sum_{P \in I} I(P, f_{j,i}, f_{l,s}) \\ \leq (p^i + 1)(p^i)/2 - N_1 \end{aligned}$$

(iv)

$$\begin{aligned} \sum_{j=1}^r \sum_{1 \leq i < s \leq n_j} \sum_{P \in \text{Sing}(g_t)} I(P, f_{j,i}, f_{j,s}) + \sum_{1 \leq j < l \leq r} \sum_{\substack{1 \leq i \leq n_j \\ 1 \leq s \leq n_l}} \sum_{P \in III.A} I(P, f_{j,i}, f_{l,s}) \\ \leq p^i(p^i - 1)/2 - N_2. \end{aligned}$$

Proof. (i)

$$\sum_{j=1}^r \deg(f_j)^2/n_j \leq \sum_{j=1}^r \deg(f_j)^2/2 = 1/2(\deg(f_1)^2 + \dots + \deg(f_r)^2) \leq 1/2 \deg(g_t)^2$$

- (ii) From Lemma 7.4 we know that if P is a point of type II then $I(P, f_{j,i}, f_{l,s}) = 0$ for every $j, l \in \{1, \dots, r\}$ and $1 \leq i \leq n_j, 1 \leq s \leq n_l$. From Lemma 7.4 we now that for each point P of type II there is at most two components $f_{a,b}$ and $f_{a',b'}$ for which $I(P, f_{a,b}, f_{a',b'}) = p^i$ and zero otherwise. Taking into account that there are $((\ell - 1)^2 - N_1)$ points of type II we get the result.
- (iii) From Lemma 7.2 we have that if P is a point of type I, then for any two components $f_{a,b}$ and $f_{a',b'}$ we have $I(P, f_{a,b}, f_{a',b'}) = m_P(f_{a,b})m_P(f_{a',b'})$. Hence we have to prove the following,

$$\begin{aligned} \sum_{j=1}^r \sum_{1 \leq i < s \leq n_j} m_P(f_{j,i})m_P(f_{j,s}) + \sum_{1 \leq j < l \leq r} \sum_{\substack{1 \leq i \leq n_j \\ 1 \leq s \leq n_l}} m_P(f_{j,i})m_P(f_{l,s}) \\ \leq (p^i + 1)(p^i)/2. \end{aligned}$$

Notice that the left hand side is a maximum when $m_P(f_{j,s}) = 1$ for every $j \in \{1, \dots, r\}$, $s \in \{1, \dots, n_j\}$. The latter equation is

$$\sum_{j=1}^r \sum_{1 \leq i < s \leq n_j} m_P(f_{j,i})m_P(f_{j,s}) + \sum_{1 \leq j < l \leq r} \sum_{\substack{1 \leq i \leq n_j \\ 1 \leq s \leq n_l}} m_P(f_{j,i})m_P(f_{l,s})$$

$$\begin{aligned}
&\leq \sum_{j=1}^r \sum_{1 \leq i < s \leq n_j} 1 + \sum_{1 \leq j < l \leq r} \sum_{\substack{1 \leq i \leq n_j \\ 1 \leq s \leq n_l}} 1 \\
&= \binom{p^i + 1}{2} = (p^i + 1)(p^i)/2
\end{aligned}$$

(iv) Same proof as (iii) but taking on account that has N_2 singular points of this type with multiplicity p^i . □

Lemma 7.6. *Let $f_t(x, y) = f_1 f_2 \dots f_r = (f_{1,1} \dots f_{1,n_1})(f_{2,1} \dots f_{2,n_2}) \dots (f_{r,1} \dots f_{r,n_r})$ then*

$$\begin{aligned}
&\sum_{j=1}^r \sum_{1 \leq i < s \leq n_j} \deg(f_{j,i}) \deg(f_{j,s}) + \sum_{1 \leq j < l \leq r} \sum_{\substack{1 \leq i \leq n_j \\ 1 \leq s \leq n_l}} \deg(f_{j,i}) \deg(f_{l,s}) \\
&= \frac{1}{2} \left(\deg(g_t)^2 - \sum_{j=1}^r \frac{\deg(f_j)^2}{n_j} \right) > \deg(g_t)^2/4.
\end{aligned}$$

Proof.

$$\sum_{j=1}^r \sum_{1 \leq i < s \leq n_j} \deg(f_{j,i}) \deg(f_{j,s}) + \sum_{1 \leq j < l \leq r} \sum_{\substack{1 \leq i \leq n_j \\ 1 \leq s \leq n_l}} \deg(f_{j,i}) \deg(f_{l,s}). \quad (28)$$

Since each $f_{j,s}$ has the same degree for all s , the first term is equal to

$$\sum_{j=1}^r \deg(f_j)^2 \frac{n_j - 1}{2n_j} = \frac{1}{2} \sum_{j=1}^r \deg(f_j)^2 - \frac{1}{2} \sum_{j=1}^r \frac{\deg(f_j)^2}{n_j}.$$

Note that

$$\begin{aligned}
(\deg(g_t))^2 &= \left(\sum_{j=1}^r \deg(f_j) \right)^2 \\
&= \sum_{j=1}^r \deg(f_j)^2 + 2 \left(\sum_{1 \leq j < l \leq r} \deg(f_j) \deg(f_l) \right) \\
&= \sum_{j=1}^r \deg(f_j)^2 + 2 \sum_{1 \leq j < l \leq r} \left(\sum_{s=1}^{n_j} \deg(f_{j,s}) \right) \left(\sum_{i=1}^{n_l} \deg(f_{l,i}) \right) \\
&= \sum_{j=1}^r \deg(f_j)^2 + 2 \sum_{1 \leq j < l \leq r} \sum_{\substack{1 \leq i \leq n_j \\ 1 \leq s \leq n_l}} \deg(f_{j,i}) \deg(f_{l,s}).
\end{aligned}$$

Substituting both of these into (28) shows that (28) is equal to

$$\frac{1}{2} \left(\deg(g_t)^2 - \sum_{j=1}^r \frac{\deg(f_j)^2}{n_j} \right). \quad (29)$$

Using (27) we get

$$\frac{1}{2} \left(\deg(g_t)^2 - \sum_{j=1}^r \frac{\deg(f_j)^2}{n_j} \right) > \frac{1}{2} \left(\deg(g_t)^2 - \deg(g_t)^2/2 \right) = \deg(g_t)^2/4. \quad (30)$$

□

Finally, here is our main result.

Theorem 7.7. *In case (B.1) $g_t(x, y)$ always has an absolutely irreducible factor over \mathbb{F}_p , if either $p \geq 5$, $i \geq 1$ and $\ell > 3$ or $p \geq 5$, $i \geq 2$ and $\ell \geq 3$ or $p = 3$, $i \geq 2$ and $\ell \geq 3$.*

Proof. We apply Bezout's Theorem one more time to the product

$$f_1 f_2 \dots f_r = (f_{1,1} \dots f_{1,n_1})(f_{2,1} \dots f_{2,n_2}) \dots (f_{r,1} \dots f_{r,n_r}).$$

The sum of the intersection multiplicities can be written

$$\sum_{j=1}^r \sum_{1 \leq i < s \leq n_j} \sum_{P \in \text{Sing}(g_t)} I(P, f_{j,i}, f_{j,s}) + \sum_{1 \leq j < l \leq r} \sum_{\substack{1 \leq i \leq n_j \\ 1 \leq s \leq n_l}} \sum_{P \in \text{Sing}(g_t)} I(P, f_{j,i}, f_{l,s})$$

where the first term is for factors within each f_j , and the second term is for cross factors between f_j and f_l . Using Lemma 7.5, part (ii), (iii) and (iv), the previous sums can be bounded by

$$\leq (p^i + 1)(p^i)/2 N_1 + p^i((l-1)^2 - N_1) + p^i(p^i - 1)/2 N_2 \quad (31)$$

Since $N_1 \leq (\ell/3 - 1)^2$ and $N_2 \leq \ell$ we get

$$\leq (p^i + 1)(p^i)/2 (\ell/3 - 1)^2 + p^i((l-1)^2 - (\ell/3 - 1)^2) + p^i(p^i - 1)/2 \ell \quad (32)$$

On the other hand, we know from Lemma 7.6 that the right-hand side of Bezout's Theorem is bigger than $\deg(g_t)^2/4$.

Hence, so far we have shown that Bezout's Theorem implies the following inequality:

$$\deg(g_t)^2/4 \leq (p^i + 1)(p^i)/2 (\ell/3 - 1)^2 + p^i((l-1)^2 - (\ell/3 - 1)^2) + p^i(p^i - 1)/2 \ell$$

Let us now show that the opposite is true, to get a contradiction. Suppose

$$\frac{p^{2i}\ell^2 - 2p^i\ell + 1}{4} > \frac{2(p^{2i} + p^i)}{4} (\ell/3 - 1)^2 + \frac{4p^i}{4} ((l-1)^2 - (\ell/3 - 1)^2) + \frac{2(p^{2i} - p^i)}{4} \ell$$

$$p^{2i}(\ell^2 - 2(\ell/3 - 1)^2 - 2\ell) > p^i(-2(\ell/3 - 1)^2) + 4(\ell - 1)^2 - 1$$

$$p^{2i} \left(\frac{7\ell^2}{9} - \frac{2\ell}{3} - 2 \right) > p^i \left(\frac{34\ell^2}{9} - \frac{20\ell}{3} + 2 \right) - 1$$

Is enough to see when

$$p^i > \frac{\frac{34\ell^2}{9} - \frac{20\ell}{3} + 2}{\frac{7\ell^2}{9} - \frac{2\ell}{3} - 2} = \frac{\frac{35\ell^2}{9} - \frac{10\ell}{3} - 10}{\frac{7\ell^2}{9} - \frac{2\ell}{3} - 2} + \frac{\frac{-\ell^2}{9} - \frac{10\ell}{3} + 12}{\frac{7\ell^2}{9} - \frac{2\ell}{3} - 2}$$

$$p^i > 5 + \frac{\frac{-\ell^2}{9} - \frac{10\ell}{3} + 12}{\frac{7\ell^2}{9} - \frac{2\ell}{3} - 2}$$

Notice that if $\ell = 3$ the numerator is positive and if $\ell > 3$ then it is negative. Therefore, we need $p \geq 5$, $i \geq 1$ and $\ell > 3$ or $p \geq 5$, $i \geq 2$ and $\ell \geq 3$ or $p = 3$, $i \geq 2$ and $\ell \geq 3$. □

Lemma 7.8. *If $\ell \mid p^i - 1$ but $\ell \neq p^i - 1$, then*

$$p^i \geq 2(\ell - 1) + 3.$$

Proof. Since $\ell \mid p^i - 1$ but $\ell \neq p^i - 1$, then $p^i - 1 \geq 2\ell \Leftrightarrow p^i \geq 2(\ell - 1) + 3$. □

Here are some more lemmata we will use.

Lemma 7.9. *Given $N \in \mathbb{N}$ the values x_1, \dots, x_n that maximize the function $H(x_1, \dots, x_n) = \sum_{\substack{1 \leq i < j \leq n \\ i \neq j}} x_i x_j$ subject to the constraint $x_1 + \dots + x_n = N$ are $x_1 = \dots = x_n = N/n$.*

Lemma 7.10. *If $\ell \mid p^i - 1$ but $\ell \neq p^i - 1$, then*

$$\deg(g_t)^2 > \sum_{P \in \text{Sing}(g_t)} m_p(g_t)^2.$$

Proof: We are going to prove that $\deg(g_t)^2 = (p^i \ell - 1)^2$ is bigger than an upper bound of $\sum_{P \in \text{Sing}(g_t)} m_p(g_t)^2$

$$\sum_{P \in \text{Sing}(g_t)} m_p(g_t)^2 \leq (p^i + 1)^2(\ell - 1)^2 + p^{2i}\ell$$

Notice that all the singular affine points are of type I. We have to prove that ,

$$(p^{2i}\ell^2 - 2p^i\ell + 1) > (p^{2i} + 2p^i + 1)(\ell - 1)^2 + p^{2i}\ell$$

Equivalently,

$$p^{2i}(\ell - 1) > p^i(2(\ell - 1)^2 + 2\ell) + (\ell - 1)^2 - 1$$

Dividing by $p^i(\ell - 1)$ we get

$$p^i > 2(\ell - 1) + 2 + \frac{1}{\ell - 1} + \frac{(\ell - 1)}{p^i} - \frac{1}{p^i(\ell - 1)}$$

We know from Lemma 7.8 that $p^i \geq 2(\ell - 1) + 3$ so is enough to prove that

$$2(\ell - 1) + 3 > 2(\ell - 1) + 2 + \frac{1}{\ell - 1} + \frac{(\ell - 1)}{p^i} - \frac{1}{p^i(\ell - 1)},$$

or

$$1 > \frac{1}{\ell - 1} + \frac{(\ell - 1)}{p^i} - \frac{1}{p^i(\ell - 1)}.$$

Since $\ell \geq 3$ then $\frac{1}{\ell - 1} + \frac{(\ell - 1)}{p^i} - \frac{1}{p^i(\ell - 1)} \leq 1/2 + \frac{(\ell - 1)}{p^i} - \frac{1}{p^i(\ell - 1)}$.

Again since $p^i \geq 2(\ell - 1) + 3$ we get

$$1/2 + \frac{(\ell - 1)}{p^i} - \frac{1}{p^i(\ell - 1)} \leq 1 - \frac{1}{p^i(\ell - 1)} < 1.$$

□

Let us prove an auxiliary result.

Lemma 7.11. *All \mathbb{F}_p -irreducible components $f_k(x, y)$ of $g_t(x, y)$ satisfy the following conditions:*

•

$$\deg(f_k)^2 \leq \sum_{P \in \text{Sing}(g_t)} m_P(f_k)^2. \quad (33)$$

•

$$\sum_{1 \leq i < j \leq n_k} m_P(f_{k,i})m_P(f_{k,j}) \leq m_P(f_k)^2 \frac{n_k - 1}{2n_k}. \quad (34)$$

Proof: Applying Bezout's theorem to f_k gives

$$\sum_{1 \leq i < j \leq n_k} \sum_{P \in \text{Sing}(f_k)} I(P, f_{k,i}, f_{k,j}) = \sum_{1 \leq i < j \leq n_k} \deg(f_{k,i}) \deg(f_{k,j}) = \deg(f_k)^2 \frac{n_k - 1}{2n_k}. \quad (35)$$

Since for every $i, j \in \{1, \dots, n_k\}$ the tangent cones of $f_{k,i}$ and $f_{k,j}$ consist of different lines by Lemma 4.14, the left hand side of (35) is

$$\sum_{1 \leq i < j \leq n_k} \sum_{P \in \text{Sing}(f_k)} I(P, f_{k,i}, f_{k,j}) = \sum_{P \in \text{Sing}(f_k)} \sum_{1 \leq i < j \leq n_k} m_P(f_{k,i})m_P(f_{k,j}) \quad (36)$$

because $I(P, u, v) \geq m_P(u)m_P(v)$. We fix P a singular point. Applying Lemma 7.9 to

$$\sum_{1 \leq i < j \leq n_k} m_P(f_{k,i})m_P(f_{k,j})$$

subject to $\sum_{i=1}^{n_k} m_P(f_{k,i}) = m_P(f_k)$ we get that

$$\sum_{1 \leq i < j \leq n_k} m_P(f_{k,i})m_P(f_{k,j}) \leq m_P(f_k)^2 \frac{n_k - 1}{2n_k}$$

which proves (34). Summing over P then proves (33). □

Theorem 7.12. *If $\gcd(\ell, p^i - 1) = \ell$ (case B.2) and $\ell < p^i - 1$, $g_t(x, y)$ always has an absolutely irreducible factor over \mathbb{F}_p .*

We apply Bezout's Theorem one more time to the product

$$f_1 f_2 \cdots f_r = (f_{1,1} \cdots f_{1,n_1})(f_{2,1} \cdots f_{2,n_2}) \cdots (f_{r,1} \cdots f_{r,n_r}).$$

The sum of the intersection multiplicities can be written

$$\sum_{k=1}^r \sum_{1 \leq i < j \leq n_k} \sum_{P \in \text{Sing}(g_t)} I(P, f_{k,i}, f_{k,j}) + \sum_{1 \leq k < l \leq r} \sum_{\substack{1 \leq i \leq n_k \\ 1 \leq j \leq n_l}} \sum_{P \in \text{Sing}(g_t)} I(P, f_{k,i}, f_{l,j})$$

where the first term is for factors within each f_k , and the second term is for cross factors between f_k and f_l . Since for every k and i the tangent cones of the $f_{k,i}$ consist of different lines by Lemma 4.14, the previous sums can be written

$$\sum_{P \in \text{Sing}(g_t)} \left[\sum_{k=1}^r \sum_{1 \leq i < j \leq n_k} m_P(f_{k,i}) m_P(f_{k,j}) + \sum_{1 \leq k < l \leq r} \sum_{\substack{1 \leq i \leq n_k \\ 1 \leq j \leq n_l}} m_P(f_{k,i}) m_P(f_{l,j}) \right]. \quad (37)$$

Note that

$$\begin{aligned} (m_P(g_t))^2 &= \left(\sum_{k=1}^r m_P(f_k) \right)^2 \\ &= \sum_{k=1}^r m_P(f_k)^2 + 2 \left(\sum_{1 \leq k < l \leq r} m_P(f_k) m_P(f_l) \right) \\ &= \sum_{k=1}^r m_P(f_k)^2 + 2 \sum_{1 \leq k < l \leq r} \left(\sum_{i=1}^{n_k} m_P(f_{k,i}) \right) \left(\sum_{j=1}^{n_l} m_P(f_{l,j}) \right) \\ &= \sum_{k=1}^r m_P(f_k)^2 + 2 \sum_{1 \leq k < l \leq r} \sum_{\substack{1 \leq i \leq n_k \\ 1 \leq j \leq n_l}} m_P(f_{k,i}) m_P(f_{l,j}). \end{aligned}$$

Substituting, (37) becomes

$$\sum_{P \in \text{Sing}(g_t)} \left[\sum_{k=1}^r \sum_{1 \leq i < j \leq n_k} m_P(f_{k,i}) m_P(f_{k,j}) + \frac{1}{2} \left(m_P(g_t)^2 - \sum_{k=1}^r m_P(f_k)^2 \right) \right]. \quad (38)$$

Substituting (34) this is

$$\leq \sum_{P \in \text{Sing}(g_t)} \left[\sum_{k=1}^r m_P(f_k)^2 \frac{n_k - 1}{2n_k} + \frac{1}{2} \left(m_P(g_t)^2 - \sum_{k=1}^r m_P(f_k)^2 \right) \right] \quad (39)$$

$$= \frac{1}{2} \sum_{P \in \text{Sing}(g_t)} \left[m_P(g_t)^2 - \sum_{k=1}^r \frac{m_P(f_k)^2}{n_k} \right]. \quad (40)$$

On the other hand, from Lemma 7.6 we know that the right-hand side of Bezout's Theorem

$$\sum_{k=1}^r \sum_{1 \leq i < j \leq n_k} \deg(f_{k,i}) \deg(f_{k,j}) + \sum_{1 \leq k < l \leq r} \sum_{\substack{1 \leq i \leq n_k \\ 1 \leq j \leq n_l}} \deg(f_{k,i}) \deg(f_{l,j}). \quad (41)$$

is equal to

$$\frac{1}{2} \left(\deg(g_t)^2 - \sum_{k=1}^r \frac{\deg(f_k)^2}{n_k} \right). \quad (42)$$

Comparing (42) and (40), so far we have shown that Bezout's Theorem implies the following inequality:

$$\deg(g_t)^2 - \sum_{k=1}^r \frac{\deg(f_k)^2}{n_k} \leq \sum_{P \in \text{Sing}(g_t)} \left[m_P(g_t)^2 - \sum_{k=1}^r \frac{m_P(f_k)^2}{n_k} \right].$$

Finally, using (33) and Lemma 7.10 to compare both sides term by term, this is a contradiction. \square

Remark 7.1. $t = \frac{3^k+1}{2}$ is an exceptional number over \mathbb{F}_{3^m} whenever $p \nmid k$ and $(m,k) = 1$. The latter result it is not a contradiction because we are assuming $t = p^i(\ell) + 1$.

Notice that then $\frac{3^k+1}{2} = p^i(\ell) + 1 \Leftrightarrow 3^k = p^i(2\ell) + 1$ which is impossible since the right hand side it is not divisible by 3.

Remark 7.2. Note that this proof fails if $\ell = p^i - 1$. This case remains still unproven.

8 Results on Case (A)

Throughout this section we shall assume that we are in case (A), i.e., p does not divide either t nor $t - 1$.

The proofs in this section use the theory of pencils and Bertini's theorem. The background was given in section 3.3. We also use some of the previous methods, singularities and Bezout's theorem.

Let us consider the projective plane \mathbb{P}^2 over $\overline{\mathbb{F}}_p$ and take homogeneous coordinates $(X : Y : Z)$ such that $x := X/Z$ and $y := Y/Z$ are affine coordinates in the chart defined by $Z \neq 0$. Let $F_t(X, Y, Z)$ (resp., $G_t(X, Y, Z)$) be the homogenization of the polynomial $f_t(x, y)$ (resp., $g_t(x, y)$) and denote by χ_t the projective curve over $\overline{\mathbb{F}}_p$ defined by the equation $G_t(X, Y, Z) = 0$. Notice that $g_t(x, y)$ has an absolutely irreducible factor over \mathbb{F}_p if and only if $G_t(X, Y, Z)$ does so. For any subfield $K \subseteq \overline{\mathbb{F}}_p$, $\chi_t(K)$ will denote the set of K -rational points of χ_t .

By Lemma 4.3 one has that, in case (A), the singularities of χ_t are exactly those singular points of the curve $F_t(X, Y, Z) = 0$ which do not belong to the line $X = Y$; moreover all of them are in the chart $Z \neq 0$. As a consequence the singular locus of χ_t is defined (in the affine coordinates x, y) by the condition $x \neq y$ and the equations

$$(x + 1)^{t-1} - x^{t-1} = 0, \quad (43)$$

$$(y+1)^{t-1} - y^{t-1} = 0 \quad \text{and} \quad (44)$$

$$x^{t-1} - y^{t-1} = 0 \quad (45)$$

Taking into account that all the coordinates of a singular point must be non-zero, set

$$r := \frac{x+1}{x}, \quad s := \frac{y+1}{y}.$$

Conditions (43) and (44) mean that

$$r^{t-1} = 1, \quad s^{t-1} = 1. \quad (46)$$

Condition (45) means that

$$(r-1)^{t-1} = (s-1)^{t-1}. \quad (47)$$

From these considerations it is straightforward that the map defined by

$$(r, s) \mapsto \left(\frac{1}{r-1} : \frac{1}{s-1} : 1 \right)$$

provides a bijection between the set

$$\Omega_t := \left\{ (r, s) \in \overline{\mathbb{F}}_p^2 \mid r^{t-1} = s^{t-1} = 1, (r-1)^{t-1} = (s-1)^{t-1}, r \neq 1, s \neq 1, r \neq s \right\}$$

and the set of singular points of χ_t . Moreover, by Lemma 4.4, all these singularities are nodal. The following lemma will be a key tool for our results.

Lemma 8.1. *Let K be a finite subfield of $\overline{\mathbb{F}}_p$. If there exists $P \in \chi_t(K)$ such that P is not a singular point of χ_t then there exists an absolutely irreducible homogeneous polynomial $H(X, Y, Z) \in K[X, Y, Z]$ such that $H(X, Y, Z)$ divides $G_t(X, Y, Z)$.*

Proof. Let $G_t(X, Y, Z) = R_1(X, Y, Z) \cdots R_m(X, Y, Z)$ be the decomposition of $G_t(X, Y, Z)$ as a product of irreducible homogeneous polynomials $R_i \in K[X, Y, Z]$, $1 \leq i \leq m$. Assume, without loss of generality, that $R_1(P) = 0$. By Lemma 6.1 there exists a finite extension L of K and an absolutely irreducible homogeneous polynomial $H(X, Y, Z) \in L[X, Y, Z]$ such that

$$R_1(X, Y, Z) = c \prod_{\sigma \in G} \sigma(H(X, Y, Z)),$$

where $c \in L$ and $G = \text{Gal}(L/K)$. The point P must be a zero of any of the above factors $\sigma(H(X, Y, Z))$. But, since P is a non-singular point of χ_t , it holds that $L = K$ and, therefore, $R_1(X, Y, Z)$ is absolutely irreducible. \square

Theorem 8.2. *If either $\gcd(p-1, t) \geq 3$ or $\gcd(p-1, t-1) \geq 2$ then $G_t(X, Y, Z)$ has an absolutely irreducible factor over \mathbb{F}_p .*

Proof. Assume first that $\gcd(p-1, t) \geq 3$. Then the equation $z^t - 1 = 0$ has, at least, 3 solutions in \mathbb{F}_p . This implies the existence of $r_1, r_2 \in \mathbb{F}_p \setminus \{1\}$ such that $r_1 \neq r_2$ and $r_1^t = r_2^t = 1$. It is straightforward that $P = (1/(r_1 - 1) : 1/(r_2 - 1) : 1)$ is an \mathbb{F}_p -rational point of the curve χ_t . Moreover it is clearly non-singular (see the paragraph before Lemma 8.1). Therefore $G_t(X, Y, Z)$ has an absolutely irreducible factor over \mathbb{F}_p by Lemma 8.1.

Assume now that $\gcd(p-1, t-1) \geq 2$. Then the equation $z^{t-1} - 1 = 0$ has, at least, 2 solutions in \mathbb{F}_p , say 1 and $r \neq 1$. It is straightforward that the \mathbb{F}_p -rational point $(r : 1 : 0)$ belongs to χ_t ; moreover it is non-singular because it is on the line at infinity $Z = 0$. Applying again Lemma 8.1 one has that $G_t(X, Y, Z)$ has an absolutely irreducible factor over \mathbb{F}_p . \square

A natural generalization is given in the following result:

Theorem 8.3. *If there exist $m \in \mathbb{N}$ such that $G_t(X, Y, Z)$ does not factor over \mathbb{F}_{p^m} and furthermore either $\gcd(p^m - 1, t) \geq 3$ or $\gcd(p^m - 1, t-1) \geq 2$ then $G_t(X, Y, Z)$ has an absolutely irreducible factor over \mathbb{F}_p .*

The next result shows an upper bound for the number of singular points of χ_t :

Proposition 8.4. *If t is even then the number of singular points of χ_t is, at most, $\frac{(t-2)(t-4)}{2}$.*

Proof. Let us define

$$\Omega'_t := \left\{ (r, s) \in \overline{\mathbb{F}}_p^2 \mid r^{t-1} = s^{t-1} = 1, r \neq 1, s \neq 1, (r-1)^{t-1} = (s-1)^{t-1} \right\}$$

and $\Delta := \{(r, r) \in \overline{\mathbb{F}}_p^2 \mid r^{t-1} = 1, r \neq 1\}$. Observe that $\Delta \subseteq \Omega'_t$ and $\Omega_t = \Omega'_t \setminus \Delta$.

From the sequence of equalities $(1/s-1)^{t-1} = -(s-1)^{t-1}/s^{t-1} = -(s-1)^{t-1} = -(r-1)^{t-1}$, it follows the implication

$$(r, s) \in \Omega'_t \Rightarrow (r, 1/s) \notin \Omega'_t.$$

Then $\#\Omega'_t \leq \frac{t-2}{2}(t-2)$ and therefore

$$\#\Omega_t = \#\Omega'_t - \#\Delta \leq \frac{(t-2)^2}{2} - (t-2) = \frac{(t-2)(t-4)}{2}.$$

The result holds because there is a bijection between Ω_t and the set of singular points of χ_t . \square

Theorem 8.5. *If the number of singular points of χ_t is less than $\frac{(t-2)^2}{4}$ then $g_t(x, y)$ has an absolutely irreducible factor over \mathbb{F}_p .*

Proof. As in the proof of Theorem 7.7, let $g_t(x, y) = \prod_{j=1}^r f_j$ be the decomposition of $g_t(x, y)$ as a product of irreducible polynomials in $\mathbb{F}_p[x, y]$. Let also $f_j = \prod_{i=1}^{n_j} f_{j,i}$

be the decomposition of f_j as a product of absolutely irreducible polynomials, $1 \leq j \leq r$. Applying Bezout's Theorem we have that

$$\sum_{(j_1, k_1) \neq (j_2, k_2)} \sum_P I(P, f_{j_1, k_1}, f_{j_2, k_2}) = \sum_{(j_1, k_1) \neq (j_2, k_2)} \deg(f_{j_1, k_1}) \deg(f_{j_2, k_2}),$$

where P varies over the set of singular points of the affine curve $g_t(x, y) = 0$ (notice these are all the singular points of χ_t). Since all the singularities are nodal, each intersection number $I(P, f_{j_1, k_1}, f_{j_2, k_2})$ is equal to 1 (resp., 0) if $f_{j_1, k_1}(P) = f_{j_2, k_2}(P) = 0$ (resp., otherwise). Therefore we have the inequality

$$N_t \geq \sum_{(j_1, k_1) \neq (j_2, k_2)} \deg(f_{j_1, k_1}) \deg(f_{j_2, k_2}),$$

where N_t denotes the number of singular points of χ_t . Taking into account that, for each $j = 1, \dots, r$, all the absolutely irreducible components of f_j have the same degree, we know from Lemma 7.6 that the right hand side of the above inequality is

$$\begin{aligned} & \sum_{j=1}^r \sum_{1 \leq i < s \leq n_j} \deg(f_{j,i}) \deg(f_{j,s}) + \sum_{1 \leq j < l \leq r} \sum_{\substack{1 \leq i \leq n_j \\ 1 \leq s \leq n_l}} \deg(f_{j,i}) \deg(f_{l,s}) \\ &= \frac{1}{2} \left(\deg(g_t)^2 - \sum_{j=1}^r \frac{\deg(f_j)^2}{n_j} \right) > \deg(g_t)^2 / 4 = \frac{(t-2)^2}{4} \end{aligned}$$

and this is a contradiction with our assumption $N_t < (t-2)^2/4$. □

Denote by $\mu(t-1)$ the set of $(t-1)$ -roots of unity in $\overline{\mathbb{F}}_p$. We define the following equivalence relation in $\mu(t-1) \setminus \{1\}$:

$$r \mathcal{R}_t s \text{ if } (r-1)^{t-1} = (s-1)^{t-1}.$$

Lemma 8.6. *Let $\{R_1, \dots, R_\ell\}$ be the quotient set of \mathcal{R}_t . Assume that $\ell \geq 4$ and, for each $j_1 \in \{1, 2, \dots, \ell\}$, there exists a subset $\{j_1, j_2, j_3, j_4\} \subseteq \{1, 2, \dots, \ell\}$ of cardinality 4 such that the equivalence classes $R_{j_1}, R_{j_2}, R_{j_3}$ and R_{j_4} have the same cardinality. Then $g_t(x, y)$ has an absolutely irreducible factor over \mathbb{F}_p .*

Proof. For each $m \in \{\#R_1, \#R_2, \dots, \#R_\ell\}$ let A_m be the union of all those classes R_i with cardinality m . Consider the partition of $\mu(t-1) \setminus \{1\}$ given by $\mathcal{A} := \{A_m \mid \#R_i = m \text{ for some } i\}$. Notice that, by hypothesis, each $A \in \mathcal{A}$ is the union of, at least, 4 equivalence classes R_i . Then the number of singular points of the curve χ_t admits the following expression:

$$\#\Omega_t = \sum_{A \in \mathcal{A}} c(A) n(A)^2 - (t-2),$$

where $c(A) \geq 4$ denotes the number of equivalence classes R_i whose union is A and $n(A)$ denotes the cardinality of any of these classes. Notice that $\sum_{A \in \mathcal{A}} c(A) = \ell$ and $\sum_{A \in \mathcal{A}} c(A)n(A) = t - 2$. Using repeatedly the inequality $(x + y)^2 \geq x^2 + y^2$ for $x, y \in \mathbb{R}$, it is not hard to prove that the sum $\sum_{A \in \mathcal{A}} c(A)n(A)^2$ achieves (for fixed t) the maximum value when there is only one summand and with coefficient 4. Therefore:

$$\#\Omega_t \leq 4 \left(\frac{t-2}{4} \right)^2 - (t-2) < \frac{(t-2)^2}{4}.$$

Now the result follows from Theorem 8.5. □

Remark 8.1. Assume that $t = \frac{p^\ell + 1}{2}$ for some $\ell \geq 1$ and that t is even. Then $2(t-1) = p^\ell - 1$ and, therefore, the set of $2(t-1)$ -roots of unity of $\overline{\mathbb{F}}_p$ is the multiplicative group $\mathbb{F}_{p^\ell}^*$. Hence $(r-1)^{2(t-1)} = 1$ for any $r \in \mu(t-1) \setminus \{1\}$ because $r-1 \in \mathbb{F}_{p^\ell}^*$. Since $(r-1)^{t-1} = -(1/r-1)^{t-1}$ this means that $(r-1)^{t-1} = 1$ (resp., $(r-1)^{t-1} = -1$) for $\frac{t-2}{2}$ elements r of $\mu(t-1) \setminus \{1\}$. So, the relation \mathcal{R}_t has exactly two equivalence classes; then Lemma 8.6 cannot be applied to this case. Further, the number of singular points of χ_t is

$$\#\Omega_t = 2 \left(\frac{t-2}{2} \right)^2 - (t-2) = \frac{(t-2)(t-4)}{2},$$

which is the maximum number of possible singular points by Proposition 8.4. Then the existence of an absolutely irreducible (over \mathbb{F}_p) factor of $g_t(x, y)$ cannot be proved, for these values of t , by bounding the number of singular points (that is, applying Theorem 8.5).

Theorem 8.7. *If t is even, $(s-1)^{t-1} \notin \mathbb{F}_p$ and $(s-1)^{(t-1)(p-1)} \neq -1$ for all $s \in \mu(t-1) \setminus \{1\}$ then $g_t(x, y)$ has an absolutely irreducible factor over \mathbb{F}_p .*

Proof. Fix $r \in \mu(t-1) \setminus \{1\}$ and set $b := (r-1)^{t-1}$. Denote by $R(r)$ the equivalence class of r with respect to the relation \mathcal{R}_t (analogously with $R(1/r)$, $R(r^p)$ and $R(1/r^p)$). These 4 classes are distinct because the elements b , $(1/r-1)^{t-1} = -b$, $(r^p-1)^{t-1} = b^p$ and $(1/r^p-1)^{t-1} = -b^p$ are distinct due to the hypothesis in the statement. The map $\varphi_1 : R(r) \rightarrow R(1/r)$ (resp., $\varphi_2 : R(r) \rightarrow R(r^p)$) (resp., $\varphi_3 : R(1/r) \rightarrow R(1/r^p)$) defined by $s \mapsto 1/s$ (resp., $s \mapsto s^p$) (resp., $s \mapsto s^p$) is injective. φ_1 is clearly surjective. Conjugation provides injective maps $R(r^{p^{e-1}}) \rightarrow R(r^{p^e})$ for $e \geq 1$; taking e as the cardinality of the conjugacy class of r one has an injective map $R(r^{p^{e-1}}) \rightarrow R(r)$, and this implies that the map φ_2 is a bijection. Analogously φ_3 is bijective. Therefore $R(r)$, $R(1/r)$, $R(r^p)$ and $R(1/r^p)$ are 4 distinct equivalence classes of the relation \mathcal{R}_t with the same cardinality. Since all these facts are valid for an arbitrary element $r \in \mu(t-1) \setminus \{1\}$, applying Lemma 8.6 we have that $g_t(x, y)$ has an absolutely irreducible factor over \mathbb{F}_p . □

Remark 8.2. Notice that the following condition implies the hypothesis of Theorem 8.7: $(s-1)^{t-1} \notin \mathbb{F}_{p^2}$ for all $s \in \mu(t-1) \setminus \{1\}$.

Corollary 8.8. *Assume that t is even. Then $g_t(x, y)$ has an absolutely irreducible factor over \mathbb{F}_p if the following equivalent conditions are satisfied:*

- (a) $t - 1$ divides $p^{2e} + 1$ for some positive integer e .
- (b) The order u of p in $\mathbb{Z}/(t - 1)\mathbb{Z}$ is a multiple of 4 and $t - 1$ divides $p^{u/2} + 1$.

Proof. Let us prove first that (a) implies that $g_t(x, y)$ has an absolutely irreducible factor over \mathbb{F}_p . If $(s - 1)^{t-1} \notin \mathbb{F}_{p^2}$ for all $s \in \mu(t - 1) \setminus \{1\}$ then, by Theorem 8.7 and Remark 8.2, $g_t(x, y)$ has an absolutely irreducible factor over \mathbb{F}_p . Otherwise, there exists $r \in \mu(t - 1) \setminus \{1\}$ such that $(r - 1)^{t-1} = b \in \mathbb{F}_{p^2}$. Consider the polynomial $P(x) = (x - 1)^{t-1} - b \in \mathbb{F}_{p^2}$. Notice that $r^{p^{2e}} = 1/r$ because, by assumption, $t - 1$ divides $p^{2e} + 1$. So, $1/r$ is a conjugate of r over \mathbb{F}_{p^2} and, then, $1/r$ must be a root of $P(x)$. But this is a contradiction because $P(1/r) = -2b \neq 0$.

Finally we will prove that (a) implies (b) (the converse implication is trivial). So, assume that $t - 1$ divides $p^{2e} + 1$ for some positive integer e . A clear consequence of this is that $4e$ is a multiple of u .

We claim that $4e = uk$, where k is odd (and, in particular, 4 divides u). Indeed, reasoning by contradiction, if k is even then $2e$ is a multiple of u and, therefore, $p^{2e} \equiv 1 \pmod{t - 1}$, a contradiction. Then $4e = u(2m + 1)$ for some $m \in \mathbb{N}$. Therefore

$$-1 \equiv p^{2e} \equiv \frac{u}{2}(2m + 1) \equiv p^{um} p^{u/2} \equiv p^{u/2} \pmod{t - 1}.$$

□

Corollary 8.9. *If $t - 1 \geq 3$ is a prime number such that the multiplicative order of p in $\mathbb{Z}/(t - 1)\mathbb{Z}$ is $(t - 2)/2$ then $g_t(x, y)$ has an absolutely irreducible factor over \mathbb{F}_p .*

Proof. On the one hand, since $t - 1$ is prime and, by [23, Ex. 3.36], the $(t - 1)$ -th cyclotomic polynomial Q_{t-1} is irreducible over \mathbb{F}_{p^2} , we have that all the elements in $\mu(t - 1) \setminus \{1\}$ are conjugate over \mathbb{F}_{p^2} . On the other hand, by Theorem 8.7 and Remark 8.2, we can assume that there exists $r \in \mu(t - 1) \setminus \{1\}$ such that $b := (r - 1)^{t-1} \in \mathbb{F}_{p^2}$. These two facts imply that the $t - 2$ elements of $\mu(t - 1) \setminus \{1\}$ are roots of the polynomial $(x - 1)^{t-1} - b \in \mathbb{F}_{p^2}[x]$ and, therefore, the equivalence relation \mathcal{R}_t has only one equivalence class. Then the number of singular points of χ_t , that is, $\#\Omega_t$, is $(t - 2)^2 - (t - 2) = (t - 2)(t - 3)$. This is a contradiction with Proposition 8.4 because this number is strictly greater than $(t - 2)(t - 4)/2$.

□

For each natural number n denote by $K^{(n)}$ the cyclotomic extension of \mathbb{F}_p given by the splitting field of the polynomial $x^n - 1 \in \mathbb{F}_p[x]$.

Lemma 8.10. *Set $g_t(x, y) = h_1(x, y)h_2(x, y) \cdots h_\ell(x, y)$, where $h_i(x, y) \in \overline{\mathbb{F}_p}$ is an absolutely irreducible polynomial for each $i \in \{1, 2, \dots, \ell\}$, and consider the field $K_t := K^{(t)} \cap K^{(t-1)}$.*

- (a) For each $i \in \{1, 2, \dots, \ell\}$, it holds that $h_i(x, y) = \gamma_i h'_i(x, y)$, where $h'_i(x, y) \in K_t[x, y]$ and $\gamma_i \in \overline{\mathbb{F}_p}$.

- (b) For each positive divisor d of t such that $d > 2$, there exists $i \in \{1, 2, \dots, \ell\}$ such that $h_i(x, y) = \alpha_1 h_{i,1}(x, y)$, where $h_{i,1}(x, y) \in K^{(d)}[x, y]$ and $\alpha_1 \in \overline{\mathbb{F}}_p$.
- (c) For each divisor $d > 1$ of $t-1$ there exists $i \in \{1, 2, \dots, \ell\}$ such that $h_i(x, y) = \alpha_2 h_{i,2}(x, y)$, where $h_{i,2}(x, y) \in K^{(d)}[x, y]$ and $\alpha_2 \in \overline{\mathbb{F}}_p$.

Proof. Let us consider the pencil $\mathcal{P}(P, Q)$, where

$$P(X, Y, Z) := \frac{(X + Z)^t - X^t}{Z} \quad \text{and} \quad Q(X, Y, Z) := \frac{(Y + Z)^t - Y^t}{Z}.$$

Notice that $P - Q = F_t$, where $F_t(X, Y, Z)$ is the homogeneization of the (affine) polynomial $f_t(x, y)$. It is straightforward to show that the cluster of base points of $\mathcal{P}(P, Q)$ is

$$\mathcal{C}_1 := \left\{ \left(\frac{1}{r-1} : \frac{1}{s-1} : 1 \right) \mid r^t = s^t = 1 \text{ and } r, s \neq 1 \right\} \subseteq \mathbb{P}^2.$$

The curve defined by $P(X, Y, Z) = 0$ (resp., $Q(X, Y, Z) = 0$) is a union of lines which are transversal to those defined by $P(X, Y, Z) = 0$ (resp., $Q(X, Y, Z) = 0$). Therefore, the multiplicity of a general curve of the pencil at each one of the base points is 1 and, by Corollary 3.4, $\mathcal{P}(P, Q)$ is an irreducible pencil.

Let $h_i(x, y)$ be any of the (absolutely) irreducible components of $g_t(x, y)$ and denote by $H_i(X, Y, Z)$ its homogeneization. Let d_i be the degree of H_i and let $\nu : \mathcal{C}_1 \rightarrow \mathbb{N}$ be the map such that, for each points $p \in \mathcal{C}_1$, $\nu(p)$ is equal to 1 if H_i vanishes at p and 0 otherwise.

We claim that the vector space $\mathcal{L}_{d_i}(\mathcal{C}_1, \nu)$ is spanned by H_i . Indeed, it is obvious that $H_i \in \mathcal{L}_{d_i}(\mathcal{C}_1, \nu)$ and we shall reason by contradiction assuming that $\dim_{\overline{\mathbb{F}}_p} \mathcal{L}_{d_i}(\mathcal{C}_1, \nu) \geq 2$. In this case, there exists $T(X, Y, Z) \in \mathcal{L}_{d_i}(\mathcal{C}_1, \nu)$ such that $\{H_i, T\}$ is linearly independent over $\overline{\mathbb{F}}_p$. This contradicts the irreducibility of the pencil $\mathcal{P}(P, Q)$ because $[\alpha H_i + \beta T](X - Y) \prod_{j \neq i} H_j$ belongs to $\mathcal{L}_d(\mathcal{C}_1, \mathbf{m})$ for any $(\alpha, \beta) \in \mathbb{P}^1$ (where $\mathbf{m}(p) := 1$ for each base point p) and this space is equal to $\mathcal{P}(P, Q)$ by Lemma 3.5. Now, applying Lemma 3.6 to $\mathcal{L}_{d_i}(\mathcal{C}_1, \nu)$, one has that $h_i(x, y) = \gamma'_i h'_i(x, y)$, where $h'_i(x, y) \in K^{(t)}[x, y]$ and $\gamma'_i \in \overline{\mathbb{F}}_p$.

Let us consider now the pencil $\mathcal{P}(F_t, Z^{t-1})$. The set of its base points is $\{s_r := (r, 1, 0) \mid r^{t-1} = 1\}$ and, localizing a general member of the pencil at any of the points s_r and analyzing the evolution by blow-ups, it is easy to deduce that the cluster of base points of $\mathcal{P}(F_t, Z^t)$ is $\mathcal{C}_2 := \cup_r \mathcal{S}_r$, where r varies in the set of $(t-1)$ -roots of unity of $\overline{\mathbb{F}}_p$ and

$$\mathcal{S}_r := \{s_{r,1} := s_r, s_{r,2}, \dots, s_{r,t-1}\},$$

$s_{r,i}$ being the intersection point of the exceptional divisor of the blow-up centered at $s_{r,i-1}$ and the strict transform of the line at infinity $Z = 0$, $2 \leq i \leq t-1$. Therefore any point of \mathcal{C}_2 is $K^{(t-1)}$ -rational. Using a similar reasoning as above (but now considering the strict transforms at the points of \mathcal{C}_2 of the curves $H_i = 0$ in the definition of the map ν) it holds that, for any $i \in \{1, 2, \dots, \ell\}$, $h_i(x, y) = \gamma''_i h''_i(x, y)$, where $h''_i(x, y) \in K^{(t-1)}[x, y]$ and $\gamma''_i \in \overline{\mathbb{F}}_p$.

Hence, we have deduced that, for each $i \in \{1, 2, \dots, \ell\}$,

$$h_i(x, y) = \gamma'_i h'_i(x, y) = \gamma''_i h''_i(x, y),$$

where $h'_i(x, y) \in K^{(t)}[x, y]$ and $h''_i(x, y) \in K^{(t-1)}[x, y]$ and $\gamma'_i, \gamma''_i \in \overline{\mathbb{F}}_p$. If $\alpha \in K^{(t)}$ is one of the coefficients of h'_i it is clear from the above equalities that $\beta := \frac{\gamma'_i}{\gamma''_i} \alpha \in K^{(t-1)}$. Taking $\hat{h}_i(x, y) := \frac{1}{\alpha} h'_i(x, y) \in K^{(t)}[x, y]$ one has that $\hat{h}_i(x, y) = \frac{1}{\beta} h''_i(x, y) \in K^{(t-1)}[x, y]$ and, therefore, $\hat{h}_i(x, y) \in K_t[x, y]$. Part (a) follows by observing that $h_i(x, y) = \gamma'_i \alpha \hat{h}_i(x, y)$.

To prove (b), observe that \mathcal{C}_1 contains non-singular $K^{(d)}$ -rational points of the curve χ_t for any cyclotomic field $K^{(d)}$ with d dividing t and $d > 2$ (specifically the points $(1/(r-1) : 1/(s-1) : 1)$, $r \neq 1$ and $s \neq 1$ being two *distinct* d -roots of unity). Now the result follows by Lemma 8.1.

The proof of (c) is similar taking into account that \mathcal{C}_2 contains non-singular $K^{(d)}$ -rational points of the curve χ_t for any cyclotomic field $K^{(d)}$ with d dividing $t-1$ and $d > 1$ (specifically the points $(r : 1 : 0)$, $r \neq 1$ being a d -root of unity). \square

In the next theorem, for every positive integer n that is not divisible by p , we shall denote by e_n the degree of the cyclotomic extension $K^{(n)}/\mathbb{F}_p$, that is, the multiplicative order of p in $\mathbb{Z}/n\mathbb{Z}$.

Theorem 8.11. *Set $e := \gcd(e_{t-1}, e_t)$ and assume that at least one of these conditions holds:*

- (1) *There exists a divisor $d > 2$ of t such that $\gcd(e, e_d) = 1$.*
- (2) *There exists a divisor $d > 1$ of $t-1$ such that $\gcd(e, e_d) = 1$.*

Then the polynomial $g_t(x, y)$ has an absolutely irreducible factor in $\mathbb{F}_p[x, y]$.

Proof. Let K_t be as in Lemma 8.10. Then $e = |K_t : \mathbb{F}_p|$ and, therefore, $K_t = \mathbb{F}_{p^e}$. Suppose that there exists a divisor $d > 2$ of t such that $\gcd(e, e_d) = 1$. This implies that $K^{(d)} \cap K_t = \mathbb{F}_{p^{e_d}} \cap \mathbb{F}_{p^e} = \mathbb{F}_p$. On the one hand, by Part (b) of Lemma 8.10, there exists an absolutely irreducible factor $h(x, y)$ of $g_t(x, y)$ such that $h(x, y) \in K^{(d)}[x, y]$. On the other hand, by Part (a) of Lemma 8.10, $\beta h(x, y) \in K_t[x, y]$ for some $\beta \in \overline{\mathbb{F}}_p$. Take a coefficient α of $h(x, y)$ and define $\hat{h}(x, y) := \frac{1}{\alpha} h(x, y) \in K^{(d)}[x, y]$. Then $\hat{h}(x, y) = \frac{1}{\alpha\beta} \beta h(x, y) \in K_t[x, y]$ because $\beta\alpha \in K_t$ and, therefore, $\hat{h}(x, y) \in \mathbb{F}_p[x, y]$. Hence, $\hat{h}(x, y)$ is an absolutely irreducible factor of $g_t(x, y)$ in $\mathbb{F}_p[x, y]$. The reasoning is similar assuming that condition (2) holds. \square

Assuming the irreducibility of $g_t(x, y)$ in \mathbb{F}_p it is possible to relax the hypotheses involving the numbers e_d (associated with the divisors of t and $t-1$) given in Theorem 8.11. This is shown in the next lemma and theorem.

Lemma 8.12. *Assume that $g_t(x, y)$ is irreducible over \mathbb{F}_p . Let K be an extension of \mathbb{F}_p such that there exists a non-singular point $P \in \chi_t(K)$. Then the absolutely irreducible factors of $g_t(x, y)$ have coefficients in K .*

Proof. Applying Lemma 6.1 we have that there exists a K -irreducible polynomial $H(X, Y, Z)$ such that the factorization of $G_t(X, Y, Z)$ into K -irreducible polynomials is

$$G_t(X, Y, Z) = c \prod_{\sigma \in G} \sigma(H(X, Y, Z)),$$

where $G = \text{Gal}(K/\mathbb{F}_q)$ and $c \in \mathbb{F}_p$. We can assume, without loss of generality, that $H(P) = 0$.

We claim that $H(X, Y, Z)$ is absolutely irreducible. Indeed, reasoning by contradiction we have that, if we assume that $H(X, Y, Z)$ is not absolutely irreducible and applying again Lemma 6.1 to H , it holds that $H(X, Y, Z)$ factorizes into $n \geq 2$ absolutely irreducible polynomials which are conjugate over $\text{Gal}(K'/K)$ for some extension K' of K . Since P is a K -rational point, this implies that any of these n factors vanishes at P and, therefore, the multiplicity of H at P must be greater than 2. This is a contradiction because P is a non-singular point of χ_t .

Therefore the above given factorization of $G_t(X, Y, Z)$ is, in fact, its factorization into absolutely irreducible polynomials. The result follows taking affine coordinates. \square

Theorem 8.13. *Assume that $g_t(x, y)$ is irreducible over \mathbb{F}_p and consider the set*

$$E := \{d \in \mathbb{N} \mid d > 2 \text{ and } d \text{ divides either } t \text{ or } t - 1\}.$$

If $\gcd(e_d \mid d \in E) = 1$ then $g_t(x, y)$ is absolutely irreducible.

Proof. Let $d \in E$ and assume first that d is a divisor of t . Let η be a primitive d -root of unity. Since $d > 2$ one has that $\eta \notin \{1, -1\}$ and, then, it is clear that the point $(-2^{-1} : \frac{1}{\eta-1} : 1) \in \mathbb{P}^2$ is a non-singular point of $\chi_t(\mathbb{F}_{e_d})$.

Assume now that d divides $t - 1$ and let δ be a primitive d -root of unity. Since $d > 2$ we have that $\delta \neq 1$ and, then, $(\delta : 1 : 0)$ is a non-singular point of $\chi_t(\mathbb{F}_{e_d})$.

By Lemma 8.12, the absolutely irreducible factors of $g_t(x, y)$ have coefficients in the intersection of all the fields \mathbb{F}_{e_d} for $d \in E$, that is \mathbb{F}_p taking into account our assumptions. \square

References

- [1] A. Beauville, *Complex Algebraic Surfaces*, London Math. Society, Student Texts 34, Cambridge University Press, 1996.
- [2] A. Bodin, Reducibility of rational functions in several variables, *Israel J. Math.* **164** (2008), 333–347.
- [3] A. Campillo; G. Gonzalez-Sprinberg; F. Monserrat, Configurations of infinitely near points, *Sao Paulo J. Math. Sci.* **3** (2009), no. 1, 115–160.
- [4] Coulter, R; Matthews, R; *Planar Functions and Planes of Lenz-Barlotti Class II* Designs Codes and Cryptography, 10 (1997) 167–184.

- [5] Coulter, R., private communication.
- [6] P. Dembowski and T.G. Ostrom, Planes of order n with collineation groups of order n^2 , *Math. Z.* 103 (1968), 239–258.
- [7] D. Eisenbud; J. Harris, *The Geometry of Schemes*, Grad. Texts Math., vol. 197, Springer, New York-Heidelberg-Berlin, 1999.
- [8] W. Fulton, *Algebraic Curves*, Benjamin, New York, 1969.
- [9] D. G. Glynn, “Two New Sequences of Ovals in Finite Desarguesian Planes of Even Order,” in *Combinatorial Mathematics X*, Springer Lecture Notes in Mathematics **1036**, Springer-Verlag, 1983, 217–229.
- [10] D. G. Glynn, “A Condition for the Existence of Ovals in $PG(2, q)$, q even,” *Geometriae Dedicata* **32** (1989), 247–252.
- [11] R. Guralnick, J. Rosenberg and M. Zieve, A new family of exceptional polynomials in characteristic two, *Annals of Math.* 172 (2010), 13671396.
- [12] F. Hernando, G. McGuire, Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions. *J. Algebra* **343** (2011), 7892.
- [13] F. Hernando, G. McGuire, Proof of a conjecture of Segre and Bartocci on monomial hyperovals in projective planes. *Designs, Codes and Cryptography* **65** (2012), Issue 3, pp 275-289.
- [14] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Clarendon Press, Oxford, 1989.
- [15] J. W. P. Hirschfeld, “Ovals in Desarguesian Planes of Even Order,” *Ann. Mat. Pura Appl.* **102** (1975), 79–89.
- [16] Janwa, H.; McGuire, G.; Wilson, R. M.; *Double-error-correcting cyclic codes and absolutely irreducible polynomials over $GF(2)$.*; *J. Algebra* 178 (1995), no. 2, 665–676.
- [17] R. Hartshorne, *Algebraic Geometry*, Grad. Texts Math., vol.52, Springer, New York-Heidelberg-Berlin, 1977.
- [18] S. Iitaka, *Algebraic Geometry*. Grad. Texts Math., vol.76, Springer, New York-Heidelberg-Berlin, 1982.
- [19] S.L. Kleiman, *Bertini and his two fundamental theorems*. Studies in the history of modern mathematics, III. *Rend. Circ. Mat. Palermo* (2) Suppl. No. 55 (1998), 9–37. .
- [20] S. Kopparty; S. Yekhanin; *Detecting Rational Points on Hypersurfaces over Finite Fields*; Computational Complexity, 2008. CCC '08. 23rd Annual IEEE Conference 2008, 311 - 320.
- [21] Leducq, E., Functions which are PN on infinitely many extensions of F_p , p odd, <http://arxiv.org/abs/1006.2610>
- [22] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., vol.20, Addison-Wesley, Reading, MA, 1983.

- [23] R. Lidl and H. Niederreiter, *Finite Fields*, Introduction to finite fields and their applications. Revision of the 1986 first edition. Cambridge University Press, Cambridge, 1994. xii+416 pp.
- [24] R. Matthews, "Permutation Properties of the Polynomials $1 + x + \dots + x^k$ over a Finite Field," *Proc. A.M.S.*, **120** (1994), 47–51.
- [25] K. Nyberg and L.R.Knudsen, *Provable security against differential cryptanalysis*, Advances in Cryptology CRYPTO92, LNCS 740, pp. 566-574, Springer-Verlag, 1992.
- [26] W. M. Schmidt, *Equations over Finite Fields*, Springer Lecture Notes in Mathematics, **536**, Springer-Verlag, 1976, 210.