Journal of Combinatorial Theory, Series A 179 (2021) 105386

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

On the classification of exceptional scattered polynomials

Daniele Bartoli [a], Maria Montanucci [b,*]

[a] *Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Italy*
[b] *Department of Applied Mathematics and Computer Science, Technical University of Denmark, Asmussens Allé, building 303B, DK-2800 Kongens Lyngby, Denmark*

ARTICLE INFO

Article history:
Received 27 May 2019
Received in revised form 10 November 2020
Accepted 2 December 2020
Available online 15 December 2020

Keywords:
Maximum scattered linear set
MRD code
Algebraic curve
Hasse-Weil bound

ABSTRACT

Let $f(X) \in \mathbb{F}_{q^r}[X]$ be a q-polynomial. If the $\mathbb{F}_q$-subspace $U = \{(x^{q^t}, f(x)) \mid x \in \mathbb{F}_{q^n}\}$ defines a maximum scattered linear set, then we call $f(X)$ a scattered polynomial of index t. The asymptotic behavior of scattered polynomials of index t is an interesting open problem. In this sense, exceptional scattered polynomials of index t are those for which U is a maximum scattered linear set in $\mathrm{PG}(1, q^{mr})$ for infinitely many m. The classifications of exceptional scattered monic polynomials of index 0 (for $q > 5$) and of index 1 were obtained in [1]. In this paper we complete the classifications of exceptional scattered monic polynomials of index 0 for $q \leq 4$. Also, some partial classifications are obtained for arbitrary t. As a consequence, the classification of exceptional scattered monic polynomials of index 2 is given.

* Corresponding author.
E-mail addresses: daniele.bartoli@unipg.it (D. Bartoli), marimo@dtu.dk (M. Montanucci).

https://doi.org/10.1016/j.jcta.2020.105386
0097-3165/

1. Introduction

Let q be a prime power and $r, n \in \mathbb{N}$. Let V be a vector space of dimension r over $\mathbb{F}_{q^n}$. For any k-dimensional $\mathbb{F}_q$-vector subspace U of V, the set $L(U)$ defined by the nonzero vectors of U is called an $\mathbb{F}_q$-*linear set* of $\Lambda = \mathrm{PG}(V, q^n)$ of *rank* k, i.e.

$$L(U) = \{\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U \setminus \{\mathbf{0}\}\}.$$

It is notable that the same linear set can be defined by different vector subspaces. Consequently, we always consider a linear set and the vector subspace defining it in pair.

Let $\Omega = \mathrm{PG}(W, \mathbb{F}_{q^n})$ be a subspace of Λ and $L(U)$ an $\mathbb{F}_q$-linear set of Λ. We say that Ω has *weight* i in $L(U)$ if $\dim_{\mathbb{F}_q}(W \cap U) = i$. Thus a point of Λ belongs to $L(U)$ if and only if it has weight at least 1. Moreover, for any $\mathbb{F}_q$-linear set $L(U)$ of rank k,

$$|L(U)| \leq \frac{q^k - 1}{q - 1}.$$

When the equality holds, i.e. all the points of $L(U)$ have weight 1, we call $L(U)$ a *scattered* linear set. A scattered $\mathbb{F}_q$-linear set of highest possible rank is called a *maximum scattered* $\mathbb{F}_q$-*linear set*. See [6] for the possible ranks of maximum scattered linear sets.

Maximum scattered linear sets have various applications in Galois geometry, including blocking sets [2,30,32], two-intersection sets [6,7], finite semifields [8,17,31,36], translation caps [5], translation hyperovals [16], etc. For more applications and related topics, see [27] and the references therein. For recent surveys on linear sets and particularly on the theory of scattered spaces, see [28,38].

In this paper, we are interested in maximum scattered linear sets in $\mathrm{PG}(1, q^n)$. Let f be an $\mathbb{F}_q$-linear function over $\mathbb{F}_{q^n}$ and

$$U = \{(x, f(x)) : x \in \mathbb{F}_{q^n}\}. \tag{1.1}$$

Clearly U is an n-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$ and f can be written as a q-polynomial $f(X) = \sum A_i X^{q^i} \in \mathbb{F}_{q^n}[X]$. A necessary and sufficient condition for $L(U)$ to define a maximum scattered linear set in $\mathrm{PG}(1, q^n)$ is

$$\frac{f(x)}{x} = \frac{f(y)}{y} \text{ if and only if } \frac{y}{x} \in \mathbb{F}_q, \quad \text{for } x, y \in \mathbb{F}_{q^n}^*. \tag{1.2}$$

In [41], such a q-polynomial is called a *scattered polynomial*.

Two linear sets $L(U)$ and $L(U')$ in $\mathrm{PG}(1, q^n)$ are *equivalent* if there exists an element of $\mathrm{P\Gamma L}(2, q^n)$ mapping $L(U)$ to $L(U')$. It is obvious that if U and U' are equivalent as $\mathbb{F}_{q^n}$-spaces, then $L(U)$ and $L(U')$ are equivalent. However, the converse is not true in general. For recent results on the equivalence issue and the classification of linear sets, we refer to [12,14,15].

There is a very interesting link between maximum scattered linear sets and the so called maximum rank distance (MRD for short) codes [14].

Given a scattered polynomial f over $\mathbb{F}_{q^n}$, an MRD code (see [41]) can be defined by the following set of $\mathbb{F}_q$-linear maps

$$C_f := \{aX + bf(X) : a, b \in \mathbb{F}_{q^n}\}. \tag{1.3}$$

In particular, a scattered polynomial over $\mathbb{F}_{q^n}$ defines an MRD code in $\mathbb{F}_q^{n\times n}$ of minimum distance $n-1$. To show that (1.3) defines an MRD code, we only have to prove that $aX+bf(X)$ has at most q roots for each $a, b \in \mathbb{F}_{q^n}$ with $(a, b) \neq (0, 0)$, which is equivalent to (1.2). For more details on MRD codes we refer to [1,35,37,12,41,6,34,33,13].

To the best of our knowledge, up to the equivalence of the associated MRD codes, almost all constructions of scattered polynomials for arbitrary n can be summarized as one family

$$f(X) = \delta X^{q^s} + X^{q^{n-s}}, \tag{1.4}$$

where s satisfies $\gcd(s, n) = 1$ and $\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\delta) = \delta^{(q^n-1)/(q-1)} \neq 1$.

Besides the family of scattered polynomials defined in (1.4), very recently, Csajbók, Marino, Polverino and Zanella found another new family of scattered polynomials of index 0 of the form

$$f(X) = \delta X^{q^s} + X^{q^{n/2+s}}, \tag{1.5}$$

for $n = 6, 8$ and some $\delta \in \mathbb{F}_{q^n}^*$; see [13].

Remark 1.1. Due to the classification of exceptional scattered polynomials of index 0 in [1], the above family is not exceptional.

As scattered polynomials appear to be very rare, it is natural to look for some classifications of them. Given an integer $0 \leq t \leq n-1$ and a q-polynomial f whose coefficients are in $\mathbb{F}_{q^n}$, if

$$U_m = \{(x^{q^t}, f(x)) : x \in \mathbb{F}_{q^{mn}}\} \tag{1.6}$$

defines a maximum scattered linear set in $\mathrm{PG}(1, q^{mn})$ for infinitely many m, then we call f an *exceptional scattered polynomial of index t*. In particular, if U_1 is maximum scattered, then we say f is a scattered polynomial over $\mathbb{F}_{q^n}$ of index t.

Note that (1.6) is slightly different from (1.1): in this way we can describe the unique known family (1.4) as an exceptional one. Taking $t = s$, from (1.4) we get

$$\{(x^{q^s}, x + \delta x^{q^{2s}}) : x \in \mathbb{F}_{q^{mn}}\}$$

which defines a maximum scattered linear set for all mn satisfying $\gcd(mn, s) = 1$. This means $X + \delta X^{q^{2s}}$ is an exceptional scattered polynomial of index s.

Remark 1.2. Clearly the two formulas (1.6) and (1.1) describe equivalent objects: they are obtained just applying a Frobenius to each component. On the other hand, looking only at (1.1) does not give the whole information about one can expect an exceptional polynomial is. In fact, if one excludes the possibility of having general t's in formula (1.1), the unique non-monomial example of exceptional scattered polynomial cannot be obtained. The reason is that some of the exponents in $f(x)$ could depend on n (i.e. the size of the field $\mathbb{F}_{q^n}$) and therefore the "shape" of the polynomial $f(x)$ varies according to the field and therefore (by definition) cannot be exceptional. This happens for instance to the case $(x, \delta x^{q^s} + x^{q^{n-s}})$, which is morally speaking exceptional but does not fit the definition of being exceptional. The equivalent set $(x^{q^s}, \delta x^{q^{2s}} + x)$ is now described formally via the exceptional scattered polynomial of index s, $g(x) = \delta x^{q^{2s}} + x$.

Assume that U_m given by (1.6) defines a maximum scattered linear set for some m. Now, we want to normalize our research objects to exclude some obvious cases.

[C1] Without loss of generality, we assume that the coefficient of X^{q^t} in $f(X)$ is always 0. In fact $f(x)/x^{q^t} = f(y)/y^{q^t}$ if and only if

$$\frac{f(x) - \alpha x^{q^t}}{x^{q^t}} = \frac{f(x)}{x^{q^t}} - \alpha = \frac{f(y)}{y^{q^t}} - \alpha = \frac{f(y) - \alpha y^{q^t}}{y^{q^t}}$$

for any $\alpha \in \mathbb{F}_{q^n}^*$.

[C2] When $t > 0$, we assume that the coefficient of X in $f(X) = \sum A_i X^{q^i} \in \mathbb{F}_{q^n}[X]$ is nonzero; otherwise let $t_0 = \min\{i : A_i \neq 0\}$ and it is equivalent to consider

$$\left\{ \left(x^{q^{t-t_0}}, \sum_{i=t_0}^{n-1} A_i^{q^{n-t_0}} x^{q^{i-t_0}} \right) : x \in \mathbb{F}_{q^{mn}} \right\}$$

instead of U_m.

[C3] We assume that $f(X)$ is monic. To see this, it is enough to observe that $f(x)/x^{q^t} = f(y)/y^{q^t}$ if and only if $\alpha f(x)/x^{q^t} = \alpha f(y)/y^{q^t}$, for any $\alpha \in \mathbb{F}_{q^n}^*$.

The main results in [1] can be summarized as follows.

Theorem 1.3 *([1]).*

(1) *For $q > 5$, X^{q^k} is the unique exceptional scattered monic polynomial of index 0.*
(2) *The only exceptional scattered monic polynomials f of index 1 over $\mathbb{F}_{q^n}$ are X and $bX + X^{q^2}$ where $b \in \mathbb{F}_{q^n}$ satisfying $\mathrm{Norm}_{q^n/q}(b) \neq 1$. In particular, when $q = 2$, $f(X)$ must be X.*

In this paper we close the gaps left for $q \leq 4$ in the above classification of index 0 exceptional scattered polynomials, proving that Theorem 1.3 (1) holds also in these cases. We also obtain partial results for exceptional scattered polynomials of index larger than 1. More precisely, the following is the main result of the paper.

Theorem 1.4. *Let $t \geq 2$ be a natural number, $f(X) = \sum_{i=0}^{M} A_i X^{q^{k_i}} \in \mathbb{F}_{q^r}[X]$ where $A_M = 1$, $k_0 = 0$, and either*

- *$k_1 = 1$, $k_i \geq t$ for $i \geq 2$ and $k_M \geq t+2$, or*
- *$k_1 > t$.*

If either $k_M \geq 3t$ and $t \mid k_M$, or $k_M \geq 2t-1$ and $t \nmid k_M$ then $f(X)$ is not an exceptional scattered polynomial of index t.

Since for $t = 2$ only Condition i) in Theorem 1.4 can occur, the classification of exceptional scattered polynomials of index 2 is obtained.

Corollary 1.5. *Let $f(X) \in \mathbb{F}_{q^r}[X]$ be a monic q-linearized polynomial, q odd. Then $f(X)$ is exceptional scattered of index 2 if and only if r is odd and*

$$f(X) = X + \delta X^{q^4},$$

with $Norm_{q^r/q}(\delta) \neq 1$.

As in [1], the main idea consists in converting the original question into an investigation of a special type of algebraic curves. Then approaches based on intersection theory or function field theory together with the Hasse-Weil Theorem (see for instance [19, Theorem 5.4.1]) are used to get contradictions.

2. An approach based on intersection multiplicity

2.1. First properties of the curve $\mathcal{C}_f$ associated to a scattered polynomial f

Scattered polynomials are related with algebraic curves via the following straightforward result; see also [1, Lemma 2.1].

Lemma 2.1. *The vector space $U = \{(x^{q^t}, f(x)) : x \in \mathbb{F}_{q^n}\}$ defines a maximum scattered linear set $L(U)$ in $\mathrm{PG}(1, q^n)$ if and only if the curve $\mathcal{C}_f$ defined by*

$$\frac{f(X)Y^{q^t} - f(Y)X^{q^t}}{X^q Y - XY^q} \tag{2.1}$$

in $\mathrm{PG}(2, q^n)$ contains no affine point (x, y) such that $\frac{y}{x} \notin \mathbb{F}_q$.

In this paper we investigate on singular points of curves $\mathcal{C}_f$ associated with scattered polynomials $f(X)$ (see Lemma 2.1 above) to get information on the existence of absolutely irreducible components of $\mathcal{C}_f$ defined over $\mathbb{F}_q$.

Hasse-Weil Theorem will be an essential tool for our purposes.

Theorem 2.2 *(Hasse-Weil Theorem). Let $\mathcal{C}$ be an absolutely irreducible curve defined by $F(X,Y)=0$, with $F(X,Y)\in\mathbb{F}_q[X,Y]$ and $\deg(F(X,Y))=d$. Then the number N_q of $\mathbb{F}_q$-rational points of $\mathcal{C}$ satisfies*

$$q+1-(d-1)(d-2)\sqrt{q}\leq N_q\leq q+1+(d-1)(d-2)\sqrt{q}.$$

The existence of a suitable component in $\mathcal{C}_f$ together with Hasse-Weil Theorem is enough to prove that $f(x)$ is not exceptional scattered of index t.

Theorem 2.3. *Let $f(x)\in\mathbb{F}_{q^n}[x]$. Suppose that the curve $\mathcal{C}_f$ defined by (2.1) contains an absolutely irreducible component $\mathcal{D}$ defined over $\mathbb{F}_{q^n}$ distinct from $X=0$, $Y=\alpha X$, with $\alpha\in\mathbb{F}_q$. Then $f(x)$ is not exceptional scattered of index t.*

Proof. Let d be the degree of $\mathcal{D}$. Consider a field $\mathbb{F}_{q^{nm}}$ for some positive integer m. Clearly, $\mathcal{D}$ is also $\mathbb{F}_{q^{nm}}$-rational. By Hasse-Weil Theorem there exist at least

$$q^{nm}+1-(d-1)(d-2)q^{nm/2}$$

$\mathbb{F}_{q^{nm}}$-rational points of $\mathcal{D}$ and at most $d(q+2)$ of them are not affine nor belong to lines $X=0$, $Y=\alpha X$, with $\alpha\in\mathbb{F}_q$. Let $\overline{m}$ be such that $q^{nm}+1-(d-1)(d-2)q^{nm/2}-d(q+2)$ is positive. Then for each $m\geq\overline{m}$, by Lemma 2.1 $f(x)$ is not scattered of index t over $\mathbb{F}_{q^{nm}}$ and therefore is not exceptional scattered. □

The machinery we adopt to prove that $\mathcal{C}_f$ contains a suitable absolutely irreducible component $\mathcal{D}$ defined over $\mathbb{F}_{q^n}$ has been used in [24,25,21,22,29,43,9–11,39,40,1].

As in [1], the main tool is the use of branches and local quadratic transformations of a plane curve to obtain a better estimate for the intersection number of two components of a fixed curve at one of its singular points. Recently, an approach based on local quadratic transformations which uses implicitly branches has been applied in [3] to classify exceptional planar functions in characteristic two.

Consider an algebraic curve $\mathcal{C}$ defined over $\mathbb{F}_q$. Suppose, by way of contradiction, that $\mathcal{C}$ has no absolutely irreducible components over $\mathbb{F}_q$. We divide our proof into four steps.

(1) We find all the singular points of $\mathcal{C}$.
(2) We assume that $\mathcal{C}$ splits into two components $\mathcal{A}$ and $\mathcal{B}$ sharing no common irreducible component. An upper bound on the total intersection number of $\mathcal{A}$ and $\mathcal{B}$ is then obtained. The main ingredient here will be branch investigation using quadratic transformations.

(3) Under the assumption that $\mathcal{C}$ has no absolutely irreducible components over $\mathbb{F}_q$, we decompose $F(X,Y)$ as $A(X,Y)B(X,Y)$ and obtain a lower bound on $(\deg A)(\deg B)$.
(4) Finally, by using Bézout's Theorem (see Theorem 2.4), we get a contradiction between the two bounds.

We now recall basic notions about algebraic curves. Let $\mathcal{C}$ be a plane curve defined by the polynomial $F(X,Y) \in \mathbb{F}_{q^n}[X,Y]$. For a point $P = (u,v) \in \mathcal{C}$ write

$$F(X+u, Y+v) = F_0(X,Y) + F_1(X,Y) + F_2(X,Y) + \cdots,$$

where $F_i(X,Y)$ is either zero or homogeneous of degree i. We define the multiplicity $m_P(\mathcal{C})$ of $P \in \mathcal{C}$ as the smallest integer m such that $F_m \neq 0$ and $F_i \equiv 0$ for $i < m$. We call F_m the tangent cone of $\mathcal{C}$ at P. If $m_P(\mathcal{C}) > 0$ then P belongs to $\mathcal{C}$; if $m_P(\mathcal{C}) = 1$ then P is called a simple point of $\mathcal{C}$; if $m_P(\mathcal{C}) > 1$ then P is called a singular point. The definition of multiplicity can be easily extended to points of $\mathcal{C}$ lying on the line infinity.

Given two plane curves $\mathcal{A}$ and $\mathcal{B}$ and a point $P \in \mathcal{A} \cap \mathcal{B}$, the intersection number $I(P, \mathcal{A} \cap \mathcal{B})$ of $\mathcal{A}$ and $\mathcal{B}$ at P is defined by seven axioms; see [20,23] for more details.

Theorem 2.4 *(Bézout's Theorem). Let $\mathcal{A}$ and $\mathcal{B}$ be two projective plane curves over an algebraically closed field $\mathbb{K}$, having no components in common. Let A and B be the polynomials associated with $\mathcal{A}$ and $\mathcal{B}$ respectively. Then*

$$\sum_P I(P, \mathcal{A} \cap \mathcal{B}) = (\deg A)(\deg B),$$

where the sum runs over all points in the projective plane $PG(2,\mathbb{K})$.

Let $\overline{\mathbb{F}_q}$ be the algebraic closure of $\mathbb{F}_q$. Consider the set $\overline{\mathbb{F}_q}[[t]]$ of the formal power series on t. Let $(x_0, y_0) \in \overline{\mathbb{F}_q}^2$ be an affine point of $\mathcal{C} : F(X,Y) = 0$. A *branch* of center (x_0, y_0) of $\mathcal{C}$ is a point $(x(t), y(t)) \in (\overline{\mathbb{F}_q}[[t]])^2$ such that $F(x(t), y(t)) = 0$, where

$$x(t) = x_0 + u_1 t + u_2 t^2 + \cdots,$$
$$y(t) = y_0 + v_1 t + v_2 t^2 + \cdots.$$

See [23, Chapter 4] for more details on branches. There exists a unique branch centered at a simple point of $\mathcal{C}$.

Remark 2.5. In order to determine branches centered at singular points of a curve $\mathcal{C}$ we make use of quadratic transformations; see [23, Section 4] and [1, Section 2]. Consider a curve $\mathcal{C}$ defined by $F(X,Y) = F_r(X,Y) + F_{r+1}(X,Y) + \cdots = 0$, where each $F_i(X,Y)$ is homogeneous in X and Y and of degree i. First, we can suppose that the singular point under examination is the origin $O = (0,0)$ and that $X = 0$ is not a tangent line at

O. Let r be its multiplicity. The geometric transform of a curve $\mathcal{C}$ is the curve $\mathcal{C}'$ given by $F'(X,Y) = F(X,XY)/X^r$. (If $Y = 0$ is not a tangent line at O then we can also consider $\mathcal{C}'$ defined by $F'(X,Y) = F(XY,Y)/Y^r$.) By [23, Theorem 4.44], then there exists a bijection between the branches of $\mathcal{C}$ centered at the origin and the branches of $\mathcal{C}'$ centered at an affine point on $X = 0$. In our proofs we will perform chains of local quadratic transformations until the total number of branches is determined. In particular, if r is coprime with the characteristic of the ground field and the tangent cone $F_r(X,Y)$ at O splits into non-repeated linear factors (over the algebraic closure) distinct from X then there are precisely r distinct branches centered at O. In fact, distinct linear factors of $F_r(X,Y)$ correspond to distinct affine points of $\mathcal{C}'$ on $X = 0$.

The following technical results will be used to study the branches at singular points of the curve $\mathcal{C}_f$.

Proposition 2.6. *Let $\mathcal{C}$ be the curve defined given by $F(X,Y) = 0$, where*

$$F(X,Y) = AX^m + BY^n + \sum a_{ij} X^i Y^j, \tag{2.2}$$

with $n < m$, $AB \neq 0$, and

$$a_{ij} = 0 \qquad \text{if} \qquad \begin{cases} 0 < i < m; \ \text{or} \\ i = 0, j \leq n. \end{cases} \tag{2.3}$$

If $p \nmid \gcd(n,m)$ then $\mathcal{C}$ has (n,m) branches centered at the origin.

Proof. In order to determine the number of branches centered at the origin, we follow Remark 2.5. If $n \mid m$ then, after applying $m_1 = m/n - 1$ times $F \mapsto F_1(X,Y) = F(X,XY)/X^n$ we can easily see that the origin is the center of $n = \gcd(n,m)$ distinct branches, since the tangent cone in $F_1(X,Y)$ is $AX^n + BY^n$.

Suppose now that $n \nmid m$. Let us consider ℓ_1 the smallest integer such that $m_1 = m - \ell_1 n < n$. We apply ℓ_1 times the local quadratic transformation $F \mapsto F_1(X,Y) = F(X,XY)/X^n$. We have

$$F_1(X,Y) = AX^{m_1} + BY^n + \sum a_{ij} X^{i+\ell_1(j-n)} Y^j.$$

By Conditions (2.3) it is readily seen that the degree of each monomial $a_{ij} X^{i+\ell_1(j-n)} Y^j$ is larger than m_1. Also, all the branches centered at the origin in $\mathcal{C}$ are still centered at the origin in $F_1(X,Y)$.

Apply now k_1 times the transformation $G \mapsto G(XY,Y)/Y^{m_1}$, where k_1 is the smallest integer such that $n_1 = n - k_1 m_1 \leq m_1$.

We distinguish two cases.

(1) $m_1 \mid n$. In this case $F_2(X,Y) = F_1(XY,Y)/Y^{m_1} = AX^{m_1} + BY^{m_1} + \cdots$ and there are exactly $m_1 = \gcd(n,m)$ branches centered at the origin in $\mathcal{C}$.
(2) $m_1 \nmid n$. Then

$$F_2(X,Y) = AX^{m_1} + BY^{n_1} + \sum a_{ij} X^{i+\ell_1(j-n)} Y^{j+(i+\ell_1(j-n)-m_1)k_1}.$$

Note that $i + \ell_1(j-n) = 0$ implies $i = 0$ and $j = n$ and so $a_{ij} = 0$ and so no monomial Y^α appears in $F_2(X,Y)$ apart from BY^{n_1}. Also $i + \ell_1(j-n) < m_1$ if and only if $i + \frac{m-m_1}{n}(j-n) < m_1$ which yields $i + \frac{m-m_1}{n} j < m$ and so $i < m$. Since $a_{ij} = 0$ if $0 < i < m$, there is no monomial in $F_2(X,Y)$ with degree in X smaller than m_1 apart from BY^{n_1}. Finally, all the branches centered at the origin in $F_1(X,Y) = 0$ are centered at the origin in $F_2(X,Y) = 0$.

The polynomial $F_2(X,Y)$ satisfies Conditions (2.3) and we can proceed by induction. □

Proposition 2.7. *Let $\mathcal{C}$ be a curve of the affine equation*

$$Y^q + \alpha X^q + X^{q^r - q^{r-1} + q - 1} Y + L(X,Y),$$

where all the monomials in $L(X,Y)$ have degree at least $q^{r+1} + q - 1$. Then there is a unique branch centered at the origin.

Proof. By induction on r.

If $r = 1$, after applying the transformation $(X,Y) \mapsto (X, aX + Y)$, where $a^q + \alpha = 0$, and $\theta(F(X,Y)) = F(X,XY)/X^q$ one gets

$$Y^q + aX^{q-1} + X^{q-1}Y + L'(X,Y),$$

where $X \mid L'(X,Y)$ and $L'(X,Y)$ contains monomials of degree at least $q^2 - 1$. After applying $\eta(F(XY,Y))/Y^{q-1}$ one gets $Y + aX^{q-1} + L''(X,Y)$, with $Y \mid L''(X,Y)$, and therefore there is a unique branch centered at the origin.

Suppose that $r > 1$. One applies $(X,Y) \mapsto (X, aX + Y)$, where $a^q + \alpha = 0$, and $q^{r-1} - q^{r-2}$ times $\theta(F(X,Y)) = F(X,XY)/X^q$, obtaining

$$Y^q + aX^q + X^{q^{r-1} - q^{r-2} + q - 1} Y + L'(X,Y),$$

with monomials in $L'(X,Y)$ of degree at least $q^{r+1} - q^r + q^{r-1} + q - 1 \geq q^r + q - 1$ and the claim follows by the induction. □

3. Exceptional scattered polynomials of index t

In this section we investigate curves arising from index $t > 0$ scattered polynomials. We assume that Conditions [C1], [C2], [C3] hold.

In the following it will be useful to consider the homogenized version of the starting linearized polynomial $f(X) \in \mathbb{F}_{q^r}[X]$. We denote it by the same symbol $f(X,T)$. Namely

$$f(X,T) = \sum_{i=0}^{M} A_i X^{q^{k_i}} T^{q^{k_M}-q^{k_i}} \in \mathbb{F}_{q^r}[X,T],$$

where $k_0 = 0$, $A_0 \neq 0$ and $A_M = 1$.

Recall that to each polynomial $f(X)$ is associated a curve $\mathcal{C}_f$ as shown in Lemma 2.1. In order to apply the machinery described in Section 2, we will investigate the singular points of the curve $\mathcal{D}_f$ defined by $f(X)Y^{q^t} - f(Y)X^{q^t} = 0$. In fact, as it can be easily seen, the set of its singular points contains also the singular points of $\mathcal{C}_f$. A homogeneous equation of $\mathcal{D}_f$ is given by $F(X,Y,T) = 0$, where

$$\begin{aligned} F(X,Y,T) &= f(X,T)Y^{q^t} - f(Y,T)X^{q^t} \\ &= \sum_{i=0}^{M} A_i \left(X^{q^{k_i}} T^{q^{k_M}-q^{k_i}} Y^{q^t} - Y^{q^{k_i}} T^{q^{k_M}-q^{k_i}} X^{q^t} \right). \end{aligned} \tag{3.1}$$

The are no affine singular points in $\mathcal{D}_f$ apart from the origin. Note that the origin is, both in $\mathcal{C}_f$ and in $\mathcal{D}_f$, an ordinary singular point of multiplicity $q^t - q - 1$ and q^t respectively. The multiplicity of intersection of two putative components of $\mathcal{C}_f$ at such a point is therefore upperbounded by $(q^t - q - 1)^2/4$.

All the other singular points of $\mathcal{D}_f$ (and therefore $\mathcal{C}_f$) are contained in the ideal line.

A singular point of $\mathcal{D}_f$ is the point $P = (1,0,0)$, while the other ideal singular points are of type $(a,1,0)$.

In order to study such points it is useful to consider the change of variables $(X,Y,T) \mapsto (T,Y,X)$. The affine equation of the corresponding curve $\widetilde{\mathcal{D}}_f$ is given by $G(X,Y) = 0$, where

$$G(X,Y) = F(1,Y,X) = \sum_{i=0}^{M} A_i \left(X^{q^{k_M}-q^{k_i}} Y^{q^t} - Y^{q^{k_i}} X^{q^{k_M}-q^{k_i}} \right). \tag{3.2}$$

Apart from $(0,1,0), (1,0,0) \in \widetilde{\mathcal{D}}_f$, singular points of $\widetilde{\mathcal{D}}_f$ belong to three distinct groups:

- $S_\xi = (0,\xi)$, with $\xi \in \mathbb{F}_q$.
- $R_\xi = (0,\xi)$, with $\xi^{q^{k_M}} = \xi^{q^t}$, $\xi \notin \mathbb{F}_q$ and $\xi^{q^{k_i}} \neq \xi^{q^t}$ for at least one $i = 0, \ldots, M-1$.
- $Q_\xi = (0,\xi)$, with $\xi^{q^{k_i}} = \xi^{q^t}$ for all $i = 0, \ldots, M$ and $\xi \notin \mathbb{F}_q$.

Let $\xi \in \mathbb{F}_{q^\ell}^*$ with $\ell = GCD(t, k_1 - t, \ldots, k_M - t) = GCD(t, k_1, \ldots, k_M)$. Note that $G(X,Y) = G(X,\xi Y)$, that is $\zeta_\xi : (X,Y) \mapsto (X,\xi Y)$ is automorphism of $\widetilde{\mathcal{D}}_f$ sending S_1 to S_ξ or Q_ξ. This means that we need only to investigate branches centered at

S_1. Also $G(X,Y) = G(X,Y+1)$ and therefore S_0 and S_1 are equivalent too. Since $F(X,Y,T) = F(Y,X,T)$, $(1,0,0)$ and $(0,1,0)$ are equivalent points of $\mathcal{D}$ and therefore the corresponding points S_0 and $(0,1,0)$ are equivalent in $\tilde{\mathcal{D}}_f$. Hence we need to study just the singularities S_ξ and R_ξ of $\tilde{\mathcal{D}}_f$.

Remark 3.1. Note that $\mathcal{D}_f$ and $\tilde{\mathcal{D}}_f$ are projectively equivalent. This means that multiplicities of singular points as well as the intersection multiplicities of (putative) components of those curves at corresponding singular points are the same. Also, for a singular point P of $\mathcal{D}_f$, its multiplicity in $\mathcal{D}_f$, as the intersection multiplicities of (putative) components of $\mathcal{D}_f$ at P, is larger than or equal to its multiplicity as point of $\mathcal{C}_f$. Therefore, any upper bound on the multiplicity of intersection of two components of $\mathcal{D}_f$ can be applied to $\mathcal{C}_f$ as well. This motivates the statements of the lemmas below.

3.1. Study of the intersection multiplicities of branches at the singular points of $\tilde{\mathcal{D}}_f$

In this subsection we consider singular points of $\tilde{\mathcal{D}}_f$. In particular we study branches centered at those points and we determine upper bounds on the multiplicity of intersection of putative components of $\tilde{\mathcal{D}}_f$ (and therefore $\mathcal{C}$) at them. First of all we consider singular points contained in the second group.

Lemma 3.2. *Let $R_\xi = (0,\xi)$, $\xi \in \mathbb{F}_{q^{k_M-t}} \setminus \mathbb{F}_{q^t}$, be a singular point of $\widetilde{\mathcal{D}}_f$. If $k_i \geq t$ for each $i = 1,\dots,M$ then there is a unique branch centered at R_ξ. Thus, the multiplicity of intersection of two putative components of $\mathcal{C}_f$ in R_ξ is* 0.

Proof. In order to study branches centered at R_ξ we consider the polynomial

$$\begin{aligned} H(X,Y) = G(X,Y+\xi) = G(X,Y) + G(X,\xi) &= \sum_{i=0}^{M} A_i X^{q^{k_M}-q^{k_i}} \left(Y^{q^t} - Y^{q^{k_i}} + \eta_i\right) \\ &= Y^{q^t} - Y^{q^{k_M}} + B_0 X^{q^{k_M}-1} + \sum_{i=0}^{M-1} A_i X^{q^{k_M}-q^{k_i}} \left(Y^{q^t} - Y^{q^{k_i}}\right) \\ &\quad + \sum_{i=1}^{M-1} B_i X^{q^{k_M}-q^{k_i}}, \end{aligned}$$

where $\eta_i = \xi^{q^t} - \xi^{q^{k_i}}$ and $B_i = A_i\eta_i$. Note that, since $\xi \notin \mathbb{F}_{q^t}$, $B_0 \neq 0$.

The point R_ξ is mapped to the origin and its tangent cone in $\mathcal{C}$ (the homogeneous polynomial defined by $H(X,Y) = 0$) is Y^{q^t}. In what follows we will perform a number of quadratic transformations.

Let M_1 be the largest index such that $B_{M_1} \neq 0$. Note that, since R_ξ belongs to the second group, actually such M_1 exists. If $M_1 = 0$, then all $B_i = 0$, $i = 1,\dots,M-1$. We consider $q^{k_M-t} - 1$ times the transformation $\theta(H(X,Y)) = H(X,XY)/X^{q^t}$ and we can easily see that

$$H_1(X,Y) = Y^{q^t} - Y^{q^{k_M}} + B_0 X^{q^t-1} + L(X,Y).$$

The argument follows as in Step 3.1.1 and Step 3.1.2 below. Thus we consider now the case $M_1 \neq 0$.

Step 1. Let us consider the transformation $\theta(H(X,Y)) = H(X,XY)/X^{q^t}$. Let

$$u_1 = \frac{q^{k_M} - q^{k_{M_1}}}{q^t} - 1.$$

After u_1 applications of θ, one gets

$$\begin{aligned} H_1(X,Y) = {} & Y^{q^t} - Y^{q^{k_M}} X^{u_1(q^{k_M}-q^t)} + B_{M_1} X^{q^t} + B_0 X^{q^{k_{M_1}}+q^t-1} \\ & + \sum_{i=0}^{M-1} A_i X^{q^{k_M}-q^{k_i}} Y^{q^t} - \sum_{i=0}^{M-1} A_i X^{q^{k_{M_1}}+q^t+(u_1-1)q^{k_i}} Y^{q^{k_i}} \\ & + \sum_{i=1}^{M_1-1} B_i X^{q^{k_{M_1}}+q^t-q^{k_i}}. \end{aligned} \tag{3.3}$$

Step 2. Let $\rho_1(X,Y) = (X, \alpha_1 X + Y)$ such that $\alpha_1^{q^t} + B_{M_1} = 0$. After applying ρ_1 one gets

$$\begin{aligned} H_1'(X,Y) = {} & Y^{q^t} - (\alpha_1 X + Y)^{q^{k_M}} X^{u_1(q^{k_M}-q^t)} + B_0 X^{q^{k_{M_1}}+q^t-1} \\ & + \sum_{i=0}^{M-1} A_i \alpha_1^{q^t} X^{q^{k_M}-q^{k_i}+q^t} \\ & + \sum_{i=0}^{M-1} A_i X^{q^{k_M}-q^{k_i}} Y^{q^t} - \sum_{i=0}^{M-1} A_i X^{q^{k_{M_1}}+q^t+(u_1-1)q^{k_i}} Y^{q^{k_i}} \\ & - \sum_{i=0}^{M-1} A_i \alpha_1^{q^{k_i}} X^{q^{k_{M_1}}+q^t+u_1 q^{k_i}} + \sum_{i=1}^{M_1-1} B_i X^{q^{k_{M_1}}+q^t-q^{k_i}}. \end{aligned} \tag{3.4}$$

Let us order the indices k_i in such that $B_i \neq 0$ as $k_{M_1} > k_{M_2} > k_{M_3} > \cdots > k_{M_s}$. We distinguish two subcases.

(1) Suppose that $M_2 = 0$.
Step 3.1.1. In $H_1'(X,Y)$, the monomials of smallest degree are Y^{q^t} and $B_0 X^{q^{k_{M_1}}+q^t-1}$. If we apply θ exactly $q^{k_{M_1}-t}$ times we get

$$\overline{H}(X,Y) = Y^{q^t} + B_0 X^{q^t-1} + \overline{L}(X,Y),$$

where L is a linearized polynomial in Y with all the degrees in X larger than $q^t - 1$. Also, 0 is the unique root of $\overline{H}(0,Y)$.

Step 3.1.2. Now perform $\tau(H(X,Y)) = H(XY,X)/Y^{q^t-1}$: this gives

$$\widetilde{H}(X,Y) = Y + B_0X^{q^t-1} + \widetilde{L}(X,Y),$$

where all the monomials in $\widetilde{L}$ have degree in X larger than 1 and then 0 is the unique root of $\widetilde{H}(0,Y)$. The tangent cone has degree one now and there is a unique branch centered at the origin in the curve defined by $\widetilde{H}(X,Y)=0$ and so in $\mathcal{C}$. This also shows that the multiplicity of intersection of two putative components of $\mathcal{C}_f$ in the corresponding point is 0.

(2) Suppose now that $M_2 \neq 0$.
First note that $q^{k_{M_1}} + q^t - q^{k_{M_2}}$ is the smallest degree of a monomial in H_1' apart from Y^{q^t}.
Step 3.2.1. Let

$$u_2 = \frac{q^{k_{M_1}} - q^{k_{M_2}}}{q^t}.$$

We apply u_2 times θ and get

$$\begin{aligned}
H_2(X,Y) = {} & Y^{q^t} + B_0X^{q^{k_{M_2}}+q^t-1} + \sum_{i=0}^{M-1} A_i\alpha_1^{q^t}X^{q^{k_M}-q^{k_{M_1}}+q^{k_{M_2}}-q^{k_i}+q^t} \\
& + \sum_{i=0}^{M-1} A_iX^{q^{k_M}-q^{k_i}}Y^{q^t} - \sum_{i=0}^{M-1} A_iX^{q^{k_{M_2}}+q^t+(u_1+u_2-1)q^{k_i}}Y^{q^{k_i}} \\
& - \sum_{i=0}^{M-1} A_i\alpha_1^{q^{k_i}}X^{q^{k_{M_2}}+q^t+u_1q^{k_i}} + \sum_{i=1}^{M_2} B_iX^{q^{k_{M_2}}+q^t-q^{k_i}} \\
& - (\alpha_1X + X^{u_2}Y)^{q^{k_M}}X^{u_1(q^{k_M}-q^t)-u_2q^t}.
\end{aligned}$$

Step 3.2.2. After $\rho_2(X,Y) = (X, \alpha_2X+Y)$ with $\alpha_2^{q^t} + B_{M_2} = 0$, one gets $H_2'(X,Y)$ equal to

$$\begin{aligned}
& Y^{q^t} + B_0X^{q^{k_{M_2}}+q^t-1} + \sum_{i=0}^{M-1} A_i\alpha_1^{q^t}X^{q^{k_M}-q^{k_{M_1}}+q^{k_{M_2}}-q^{k_i}+q^t} \\
& + \sum_{i=0}^{M-1} A_iX^{q^{k_M}-q^{k_i}}(Y^{q^t} + \alpha_2^{q^t}X^{q^t}) \\
& - \sum_{i=0}^{M-1} A_iX^{q^{k_{M_2}}+q^t+(u_1+u_2-1)q^{k_i}}(Y^{q^{k_i}} + \alpha_2^{q^{k_i}}X^{q^{k_i}}) \\
& - \sum_{i=0}^{M-1} A_i\alpha_1^{q^{k_i}}X^{q^{k_{M_2}}+q^t+u_1q^{k_i}} + \sum_{i=1}^{M_2-1} B_iX^{q^{k_{M_2}}+q^t-q^{k_i}} \\
& - (\alpha_1X + \alpha_2X^{u_2+1} + X^{u_2}Y)^{q^{k_M}}X^{u_1(q^{k_M}-q^t)-u_2q^t}.
\end{aligned}$$

Now H_2' can be described as

$$Y^{q^t} + B_0 X^{q^{k_{M_2}}+q^t-1} + \sum_{i=1}^{M_2-1} B_i X^{q^{k_{M_2}}+q^t-q^{k_i}} + L(X,Y),$$

where $L(X,Y)$ is a linearized polynomial in Y such that the monomials have degree in Y either 0 or larger than q^t-1 and in X larger than $k_{M_2}+q^t-1$. Note that also H_1' can be described in this way.

Step 3.2.3. We perform

$$u_j = \frac{q^{k_{M_{j-1}}} - q^{k_{M_j}}}{q^t}$$

times θ and $\rho_j(X,Y) = (X, \alpha_j X + Y)$ with $\alpha_j^{q^t} + B_{M_j} = 0$ and we obtain

$$H_j'(X,Y) = Y^{q^t} + B_0 X^{q^{k_{M_j}}+q^t-1} + \sum_{i=1}^{M_j-1} B_i X^{q^{k_{M_j}}+q^t-q^{k_i}} + L'(X,Y).$$

At the s-th step

$$H_s'(X,Y) = Y^{q^t} + B_0 X^{q^{k_{M_s}}+q^t-1} + L'(X,Y).$$

Step 3.2.4. Note that at each step, 0 is the unique root of $H_j'(0,Y)$ and therefore all the branches centered at the origin in $\mathcal{C}$ correspond to the branches centered at the origin in the curve defined by $H_s'(X,Y) = 0$. Another application of $u = q^{k_{M_s}}/q^t$ times θ gives

$$\overline{H}(X,Y) = Y^{q^t} + B_0 X^{q^t-1} + \overline{L}(X,Y),$$

where L is a linearized polynomial in Y with all the degrees in X larger than q^t-1. Now the assertion follows from point (1). □

We now analyze the case in which $k_1 = 1$ and all the other $k_i \geq t$. Note that, using the same notation as in Lemma 3.2, $B_1 \neq 0$, since $\xi \notin \mathbb{F}_q$.

Lemma 3.3. *Suppose $1 = k_1 < t < k_2 < \cdots < k_M$, with $k_M \geq t+2$. Let $R_\xi = (0,\xi)$, $\xi \in \mathbb{F}_{q^{k_M-t}} \setminus \mathbb{F}_{q^t}$, be a singular point of $\widetilde{\mathcal{D}}_f$. Then there is a unique branch centered in R_ξ. Thus, the multiplicity of intersection of two putative components of $\mathcal{C}_f$ in R_ξ is 0.*

Proof. We proceed as in Lemma 3.2. Now $H(X,Y) = G(X,Y+\xi) = G(X,Y) + G(X,\xi)$ reads

$$Y^{q^t} - Y^{q^{k_M}} + B_0 X^{q^{k_M}-1} + B_1 X^{q^{k_M}-q} + \sum_{i=0}^{M-1} A_i X^{q^{k_M}-q^{k_i}} \left(Y^{q^t} - Y^{q^{k_i}}\right) + \sum_{i=2}^{M-1} B_i X^{q^{k_M}-q^{k_i}},$$

where $\eta_i = \xi^{q^t} - \xi^{q^{k_i}}$ and $B_i = A_i \eta_i$. Recall that, since $\xi \notin \mathbb{F}_{q^t}$, $B_0 \neq 0$.

Case $B_2 = \cdots = B_{M-1} = 0$.

We perform $u = q^{k_M - t} - 1$ transformations $\theta(H(X,Y)) = H(X, XY)/X^{q^t}$ and we get

$$H_1 = Y^{q^t} + B_0 X^{q^t-1} + B_1 X^{q^t-q} + Y^{q^t} \sum_{i=0}^{M-1} A_i X^{q^{k_M}-q^{k_i}} - \sum_{i=0}^{M} A_i X^{q^t+q^{k_i}(q^{k_M-t}-2)} Y^{q^{k_i}}.$$

Now we perform one time $\eta(H(X,Y)) = H(XY, Y)/Y^{q^t-q}$ and we get

$$H_2 = Y^q + B_0 X^{q^t-1} Y^{q-1} + B_1 X^{q^t-q} + \sum_{i=0}^{M-1} A_i X^{q^{k_M}-q^{k_i}} Y^{q^{k_M}-q^{k_i}+q} - \sum_{i=0}^{M} A_i X^{q^t+q^{k_i}(q^{k_M-t}-2)} Y^{q+q^{k_i}(q^{k_M-t}-1)}.$$

It is readily seen that all the branches centered at the origin in $H_1 = 0$ are mapped to branches centered at the origin in $H_2 = 0$. Apply $v = q^{t-1} - 2$ times $\theta(H(X,Y)) = H(X, XY)/X^q$ obtaining

$$H_3 = Y^q + B_0 X^{q^t - q^{t-1}+1} Y^{q-1} + B_1 X^q + L(X,Y).$$

Now $H_4 = H_3(X, \alpha_1 X + Y)$, where $\alpha_1^q + B_1 = 0$, reads

$$H_4 = Y^q + B_0 X^{q^t - q^{t-1}+1} (\alpha_1 X + Y)^{q-1} + L_2(X, \alpha_1 X + Y).$$

All the monomials in $L(X, \alpha_1 X + Y)$ have degree at least $q^{t+1} + q^t - q^{t-1} + q - 1$ (consider the case $k_M = t+2$ and $i = 0$). After $w = q^{t-1} - q^{t-2}$ applications of $\theta(H(X,Y)) = H(X, XY)/X^q$ we have

$$H_5 = Y^q + B_0 X^q - B_0 \alpha_1^{q-2} X^{q^{t-1} - q^{t-2} + q - 1} Y + \cdots$$

where the other terms have degree in X at least $q^{t+1} + q - 1$. By Proposition 2.7 there is a unique branch centered at the origin.

Case $B_i \neq 0$ **for some** $i > 1$.

Let $M_1 = \max\{i > 1 : B_i \neq 0\}$. Such M_1 is well defined. We now consider steps as in the proof of Proposition 3.3. The main difference here is the presence of the monomial $B_1 X^{q^{k_M}-q}$. After **Step 1** this monomial is mapped to $B_1 X^{q^{k_{M_1}}-q}$ and it is fixed by

Step 2. If $M_2 = 0$ then we use the same approach as in **Case** $B_2 = \cdots = B_{M-1} = 0$ and the claim follows. Suppose now $M_2 \neq 0$. We perform **Step 3.2.1**, **Step 3.2.2**, **Step 3.2.3**, and **Step 3.2.4**: $B_1 X^{q^{k_{M_1}}-q}$ becomes $B_1 X^{q^{k_{M_s}}-q}$. Now we proceed as in **Case** $B_2 = \cdots = B_{M-1} = 0$ and the claim follows. □

Lemma 3.4. *Let $R_\xi = (0,\xi)$, $\xi \in \mathbb{F}_{q^t}$, be a singular point of $\widetilde{\mathcal{D}}_f$. If $k_i \geq t$ for each $i = 1,\dots,M$ then there is a unique branch centered in R_ξ. Thus, the multiplicity of intersection of two putative components of $\mathcal{C}_f$ in R_ξ is 0.*

Proof. We proceed as in Lemma 3.4. The difference here is that $B_0 = 0$. Also, let

$$j = \max\{i = 1,\dots,M-1 \ : \ B_i \neq 0\}.$$

Note that B_j is well defined. So

$$\begin{aligned} H(X,Y) = G(X,Y+\xi) = G(X,Y) + G(X,\xi) &= \sum_{i=0}^{M} A_i X^{q^{k_M}-q^{k_i}} \left(Y^{q^t} - Y^{q^{k_i}} + \eta_i\right) \\ &= Y^{q^t} - Y^{q^{k_M}} + \sum_{i=0}^{M-1} A_i X^{q^{k_M}-q^{k_i}} \left(Y^{q^t} - Y^{q^{k_i}}\right) + B_j X^{q^{k_M}-q^{k_j}} \\ &+ \sum_{i=1}^{j-1} B_i X^{q^{k_M}-q^{k_i}}, \end{aligned} \tag{3.5}$$

where $\eta_i = \xi^{q^t} - \xi^{q^{k_i}}$ and $B_i = A_i \eta_i$.

We apply $u_1 = \frac{q^{k_M}-q^{k_j}}{q^t} - 1$ times the transformation $F(X,Y) \mapsto F(X,XY)/X^{q^t}$ and then

$$\begin{aligned} H_1(X,Y) = Y^{q^t} - Y^{q^{k_M}} X^{u_1(q^{k_M}-q^t)} + B_j X^{q^t} + \sum_{i=0}^{M-1} A_i X^{q^{k_M}-q^{k_i}} Y^{q^t} \\ + A_0 X^{q^{k_j}+q^t+q^{k_M-t}-q^{k_j-t}-2} Y - \sum_{i=1}^{M-1} A_i X^{q^{k_j}+q^t+(u_1-1)q^{k_i}} Y^{q^{k_i}} \\ + \sum_{i=1}^{j-1} B_i X^{q^{k_j}+q^t-q^{k_i}}. \end{aligned} \tag{3.6}$$

Let $\rho_1(X,Y) = (X, \alpha_1 X + Y)$ such that $\alpha_1^{q^t} + B_j = 0$. After applying ρ_1 one gets

$$\begin{aligned} H_1'(X,Y) = Y^{q^t} + \sum_{i=1}^{j-1} B_i X^{q^{k_j}+q^t-q^{k_i}} + A_0 X^{q^{k_j}+q^t+q^{k_M-t}-q^{k_j-t}-1} \\ + A_0 X^{q^{k_j}+q^t+q^{k_M-t}-q^{k_j-t}-2} Y + L(X,Y), \end{aligned} \tag{3.7}$$

where $L(X,Y)$ is a polynomial containing only terms of degree in X larger than $q^{k_j} + q^t + q^{k_M - t} - q^{k_j - t} - 1$. Note that $q^t \mid (q^{k_j} + q^t - q^{k_i})$. Suppose that the indices i such that $B_i \neq 0$ are ordered as

$$i_1 < i_2 < \cdots < i_s = j.$$

We continue performing each time

$$\frac{q^{k_{i_\ell}} - q^{k_{i_{\ell-1}}}}{q^t}$$

times $F(X,Y) \mapsto F(X, XY)/X^{q^t}$ and $\rho_1(X,Y) = (X, \alpha_1 X + Y)$. Doing so, in a similar way as in Lemma 3.2 we obtain

$$\widetilde{H}(X,Y) = Y^{q^t} + A_0 X^\beta + \cdots$$

where $(\beta, q^t) = 1$. We now apply Proposition 2.6 and we deduce that there is a unique branch centered at the origin. □

This completes the analysis of the points R_ξ for $k_i \geq t$, $i = 1, \ldots, M$. The following proposition will be used to study the point S_1.

Lemma 3.5. *Suppose $1 = k_1 < t < k_2 < \cdots < k_M$, with $k_M \geq t + 2$. Let $R_\xi = (0, \xi)$, $\xi \in \mathbb{F}_{q^t} \setminus \mathbb{F}_q$, be a singular point of $\widetilde{\mathcal{D}}_f$. Then there is a unique branch centered in it. Thus, the multiplicity of intersection of two putative components of $\mathcal{C}_f$ in the corresponding point is 0.*

Proof. Recall that since $\xi \notin \mathbb{F}_q$, $B_1 \neq 0$. The proof is the same as the one in Lemma 3.3, since $B_0 = 0$ does not affect the computations. □

The following lemma deals with the points S_ξ (and therefore with the points Q_ξ). Here we do not assume that $k_i > t$ for $i > 0$.

Lemma 3.6. *Let $S_1 = (0,1) \in \widetilde{\mathcal{D}}_f$ and $k_M \geq t$.*

- *If $t \mid k_M$ then there are q^t branches centered at S_1.*
- *If $k_M = tr + s$, with $s \in \{1, \ldots, t-1\}$ then there are $q^{(s,t)}$ branches centered at S_1.*

The maximum possible intersection multiplicity of two components of $\widetilde{\mathcal{D}}_f$ at S_1 is $\frac{q^{k_M + t}}{4}$.

Proof. Following the same notations as in Lemma 3.2,

$$H(X,Y) = Y^{q^t} - Y^{q^{k_M}} + Y^{q^t} \sum_{i=0}^{M-1} A_i X^{q^{k_M} - q^{k_i}} - \sum_{i=0}^{M-1} A_i X^{q^{k_M} - q^{k_i}} Y^{q^{k_i}}.$$

We distinguish two cases.

- $t \mid k_M$. We perform $(q^{k_M}-1)/(q^t-1)-1$ times θ and we get

$$\widetilde{H}(X,Y) = Y^{q^t} - A_0 Y X^{q^t-1} + \cdots .$$

Hence there are q^t branches at the q^t-singular point S_1. All the branches centered at the origin in $\mathcal{C} : H(X,Y) = 0$ are

$$Z_i = (t, \eta_i t^\alpha + \delta),$$

where $\alpha = (q^{k_M}-1)/(q^t-1)$, $\eta_i \in \mathbb{F}^*_{q^{k_M-t}}$, and $\deg_t(\delta) > \alpha$. Suppose now that the curve $\mathcal{C}$ splits into two components $\mathcal{X}$ and $\mathcal{Y}$ sharing no common irreducible component. It follows that $\mathcal{X}$ and $\mathcal{Y}$ have no branches in common. Let $U(X,Y)$ and $V(X,Y)$ be two polynomials defining the components $\mathcal{X}$ and $\mathcal{Y}$ such that U and V have no common factors. Then

$$U(X,Y) = Y^m + U_0(X,Y), \text{ and } V(X,Y) = Y^{q^t-m} + V_0(X,Y),$$

where $0 \le m \le q^t$, $\deg(U_0) > m$ and $\deg(V_0) > q^t - m$.
Our aim is to compute the intersection multiplicity of $\mathcal{X}$ and $\mathcal{Y}$ at the origin. For a branch Z_i contained in $\mathcal{X}$ it follows that the coefficient of the term degree $m\alpha$ (in t) in $U(Z_i)$ vanishes, that is,

$$\eta_i^m + \sum_{r=0}^{m} \gamma_r \eta_i^{m-r} = 0,$$

where the monomials $\gamma_r X^{r\alpha} Y^{m-r}$ belong to $U(X,Y)$. Analogously, if a branch Z_j belongs to $\mathcal{Y}$ then

$$\eta_i^{q^t-m} + \sum_{r=0}^{q^t-m} \bar{\gamma}_r \eta_i^{q^t-m-r} = 0,$$

where the monomials $\overline{\gamma}_r X^{r\alpha} Y^{q^t-m-r}$ belong to $V(X,Y)$, since the coefficient of the term degree $(q^t-m)\alpha$ (in t) in $V(Z_j)$ vanishes. Therefore, since $\eta_i, \eta_j \neq 0$, and there are exactly q^t-1 branches corresponding to distinct η_i, exactly m of them belong to $\mathcal{X}$ and q^t-m to $\mathcal{Y}$. Hence if Z_i belongs to $\mathcal{X}$, then Z_i does not belong to $\mathcal{Y}$. So the multiplicity of intersection at the origin of two putative components of $\mathcal{C}$ is given by

$$(q^t-m)m\beta \le \frac{q^{2t}}{4} q^{k_M-t} = \frac{q^{k_M+t}}{4}.$$

- $t \nmid k_M$. Let $k_M = tr + s$, with $s \in \{1, \dots, t-1\}$. We perform $q^s(q^{k_M - s} - 1)/(q^t - 1)$ times θ and we get

$$\widetilde{H}(X,Y) = Y^{q^t} - A_0 Y X^{q^s - 1} + X^{q^t} Y^{q^t} L(X,Y) \cdots,$$

for some $L(X,Y)$. Apart from the branch with tangent line $Y = 0$, the other branches centered at the origin correspond to the branches centered at the origin for

$$Y^{q^t - 1} - A_0 X^{q^s - 1} + X^{q^t} Y^{q^t - 1} L(X,Y) \cdots = 0.$$

By Proposition 2.6 there are other $q^{(s,t)} - 1$ branches. All the branches centered at the origin in $\mathcal{C} : H(X,Y) = 0$ are

$$Z_i = \left(t^\alpha, \eta_i t^\beta + \delta\right),$$

where $\alpha = (q^t - 1)/(q^{(t,s)} - 1)$, $\beta = (q^{k_M} - 1)/(q^{(t,s)} - 1)$, $\eta_i \in \mathbb{F}^*_{q^{(s,t)}}$, and $\deg_t(\delta) > \beta$. Suppose now that the curve $\mathcal{C}$ splits into two components $\mathcal{X}$ and $\mathcal{Y}$ sharing no common irreducible component. It follows that $\mathcal{X}$ and $\mathcal{Y}$ have no branches in common. Let $U(X,Y)$ and $V(X,Y)$ be two polynomials defining the components $\mathcal{X}$ and $\mathcal{Y}$ such that U and V have no common factors. Then

$$U(X,Y) = Y^m + U_0(X,Y), \text{ and } V(X,Y) = Y^{q^t - m} + V_0(X,Y),$$

where $0 \le m \le q^t$, $\deg(U_0) > m$ and $\deg(V_0) > q^t - m$.
Our aim is to compute the intersection multiplicity of $\mathcal{X}$ and $\mathcal{Y}$ at the origin. For a branch Z_i contained in $\mathcal{X}$ it follows that the coefficient of the term degree $m\beta$ (in t) in $U(Z_i)$ vanishes, that is,

$$\begin{aligned}\eta_i^m + \sum_{r=0}^{\lfloor m/\alpha \rfloor} \gamma_r \eta_i^{m - r\alpha} &= \eta_i^{m - r\lfloor m/\alpha \rfloor} \sum_{r=0}^{\lfloor m/\alpha \rfloor} \gamma_{\lfloor m/\alpha \rfloor - r} \eta_i^{r\alpha} \\ &= \eta_i^{m - r\lfloor m/\alpha \rfloor} \sum_{r=0}^{\lfloor m/\alpha \rfloor} \gamma_{\lfloor m/\alpha \rfloor - r} \left(\eta_i^\alpha\right)^r = 0,\end{aligned}$$

where the monomials $\gamma_r X^{r\beta} Y^{m - r\alpha}$ belong to $U(X,Y)$. Analogously, if a branch Z_j belongs to $\mathcal{Y}$ then

$$\eta_j^{q^t - m - r\lfloor (q^t - m)/\alpha \rfloor} \sum_{r=0}^{\lfloor (q^t - m)/\alpha \rfloor} \overline{\gamma}_{\lfloor (q^t - m)/\alpha \rfloor - r} \left(\eta_j^\alpha\right)^r = 0,$$

where the monomials $\overline{\gamma}_r X^{r\beta} Y^{q^t - m - r\alpha}$ belong to $V(X,Y)$, since the coefficient of the term degree $(q^t - m)\beta$ (in t) in $V(Z_j)$ vanishes. Therefore, since $\eta_i, \eta_j \neq 0$, and there

are exactly $q^{(s,t)-1}$ branches corresponding to distinct η_i, exactly $\lfloor m/\alpha \rfloor$ of them belong to $\mathcal{X}$ and $\lfloor (q^t-m)/\alpha \rfloor$ to $\mathcal{Y}$. In particular, noting that X^α is a permutation of $\mathbb{F}_{q^{(s,t)}}$, Z_i belongs to $\mathcal{X}$ if and only if

$$G(\eta_i) = \sum_{r=0}^{\lfloor m/\alpha \rfloor} \gamma_{\lfloor m/\alpha \rfloor - r} \eta_i^r = 0$$

and to $\mathcal{Y}$ if and only if

$$\overline{G}(\eta_i) = \sum_{r=0}^{\lfloor (q^t-m)/\alpha \rfloor} \overline{\gamma}_{\lfloor (q^t-m)/\alpha \rfloor - r} \eta_i^r = 0.$$

Suppose now that Z_i belongs to $\mathcal{X}$, then $\overline{G}(\eta_i) \neq 0$ and the coefficient of the term in t of degree $(q^t-m)\beta$ in $V(Z_i)$ does not vanish. So the multiplicity of intersection at the origin of two putative components of $\mathcal{C}$ is given by

$$(q^t-m)\left\lfloor \frac{m}{\alpha} \right\rfloor \beta \leq \frac{q^{2t}}{4} q^{k_M - t} = \frac{q^{k_M+t}}{4}. \quad \square$$

4. Proof of Theorem 1.4

Now we are in a position to prove our main result Theorem 1.4.

Proposition 4.1. *Let $t \geq 2$ be a natural number, $f(X) = \sum_{i=0}^{M} A_i X^{q^{k_i}} \in \mathbb{F}_{q^r}[X]$ where $A_M = 1$, $k_0 = 0$, and either*

- *$k_1 = 1$, $k_i \geq t$ for $i \geq 2$ and $k_M \geq t+2$, or*
- *$k_1 > t$.*

Let $\mathcal{C}_f$ be the algebraic curve associated with f as in Lemma 2.1. If $t \mid k_M$ and $k_M \geq 3t$ or $t \nmid k_M$ and $k_M \geq 2t-1$ then $\mathcal{C}_f$ has an absolutely irreducible component defined over $\mathbb{F}_{q^r}$. In particular, $f(X)$ is not exceptional scattered.

Proof. Assume that $\tilde{F}(X,Y) = W_1(X,Y)\dots W_k(X,Y)$ is the decomposition of $\tilde{F}(X,Y)$ over $\mathbb{F}_{q^r}$ with $\deg(W_i) = d_i$ and $\sum_{i=1}^{k} d_i = q^{k_M} + q^t - q - 1 = \deg(\tilde{F}(X,Y))$ and suppose by contradiction that $\mathcal{C}_f$ has no absolutely irreducible components defined over $\mathbb{F}_{q^r}$. From [21, Lemma 10] (see also [26, Lemma 3.1]), there exist natural numbers s_i such that W_i splits into s_i absolutely irreducible factors over $\bar{\mathbb{F}}_{q^r}$ each of degree d_i/s_i. Since $\mathcal{C}_f$ has no absolutely irreducible factors defined over $\mathbb{F}_{q^r}$, $s_i > 0$ for $i = 1, \dots, k$. Consider the polynomials

$$A(X,Y) = \prod_{i=1}^{k} \prod_{j=1}^{\lfloor s_i/2 \rfloor} Z_i^j(X,Y), \quad B(X,Y) = \prod_{i=1}^{k} \prod_{j=\lfloor s_i/2 \rfloor + 1}^{s_i} Z_i^j(X,Y),$$

where $Z_i^1(X,Y),\dots,Z_i^{s_i}(X,Y)$ are absolutely irreducible components of $W_i(X,Y)$. Let $\mathcal{A}: A(X,Y)=0$ and $\mathcal{B}: B(X,Y)=0$. Since the number of singular points (in the algebraic closure) of $\mathcal{C}_f$ is finite, there is no repeated factors among $Z_i^j(X,Y)$, $i=1,\dots,k$, $j=1,\dots,s_i$, otherwise the number of singular points would be infinite. So $\mathcal{A}$ and $\mathcal{B}$ do not share (absolutely irreducible) components. Let α and $\alpha+\beta$ be the degrees of $A(X,Y)$ and $B(X,Y)$ respectively. Then $2\alpha+\beta=\deg(\mathcal{C}_f)=q^{k_M}+q^t-q-1$, $\beta\le\alpha$ and $\beta\le(q^{k_M}+q^t-q-1)/3$. Furthermore from $\alpha=(q^{k_M}+q^t-q-1-\beta)/2$,

$$\deg(A)\deg(B)=\alpha(\alpha+\beta)=\frac{(q^{k_M}+q^t-q-1)^2-\beta^2}{4}\ge\frac{2(q^{k_M}+q^t-q-1)^2}{9}.$$

By Bézout's Theorem 2.4,

$$\sum_{T\in\mathcal{A}\cap\mathcal{B}} I(T,\mathcal{A}\cap\mathcal{B})=\deg(A)\deg(B)\ge\frac{2(q^{k_M}+q^t-q-1)^2}{9}. \tag{4.1}$$

Clearly intersection points of $\mathcal{A}$ and $\mathcal{B}$ are singular points of $\mathcal{C}_f$. As previously observed, the origin is an ordinary singular point of $\mathcal{C}_f$ of multiplicity q^t-q-1 and from Lemmas 3.2, 3.3, 3.4, and 3.5, $I(R_\xi,\mathcal{X}\cap\mathcal{Y})=0$. Let $T\in\mathcal{I}:=\{P,S_\xi,Q_\xi\}$. From Lemma 3.6 $I(T,\mathcal{A}\cap\mathcal{B})\le q^{k_M+t}/4$. Note that $|\mathcal{I}|=1+q+(q^\ell-q)=q^\ell+1$, where $\ell=\gcd(t,k_1,\dots,k_M)$. Hence, if $t\mid k_M$ then

$$\sum_{T\in\mathcal{A}\cap\mathcal{B}} I(T,\mathcal{A}\cap\mathcal{B})\le\frac{(q^t-q-1)^2}{4}+(q^t+1)\frac{q^{k_M+t}}{4}; \tag{4.2}$$

while if $t\nmid k_M$ then

$$\sum_{T\in\mathcal{A}\cap\mathcal{B}} I(T,\mathcal{A}\cap\mathcal{B})\le\frac{(q^t-q-1)^2}{4}+(q^{t/2}+1)\frac{q^{k_M+t}}{4}. \tag{4.3}$$

Now we can combine (4.1) with (4.2) and (4.3). Assume first that $t\mid k_M$ so that $k_M=\gamma t$, $\gamma\ge1$. Then from (4.1) and (4.2) we get

$$\frac{(q^t-q-1)^2}{4}+(q^t+1)\frac{q^{k_M+t}}{4}\ge\frac{2(q^{\gamma t}+q^t-q-1)^2}{9}, \tag{4.4}$$

which is false whenever $\gamma\ge3$. If $t\nmid k_M$ then write $k_M=\gamma t+s$ with $s=1,\dots,t-1$. From (4.1) and (4.3)

$$\frac{(q^t-q-1)^2}{4}+(q^{t/2}+1)\frac{q^{(\gamma+1)t+s}}{4}\ge\frac{2(q^{\gamma t+s}+q^t-q-1)^2}{9},$$

which is false whenever $k_M\ge2t-1$. This shows that $\mathcal{C}_f$ has an absolutely irreducible component defined over $\mathbb{F}_{q^r}$. The claim follows from Theorem 2.3. □

Remark 4.2. We note that in the proof of Proposition the size of $\mathcal{I}$ can be strictly smaller that q^t+1 or $q^{q/2}+1$, for example when $\ell=1$. In these cases Bounds (4.2) and (4.3) can be significantly improved.

We note that for $t=2$ the hypothesis $k_i \geq 2$ for $i \geq 2$ is trivially satisfied. Hence the classification of exceptional scattered polynomials of index 2 follows as a corollary of Proposition 4.1.

Proof of Corollary 1.5. Without loss of generality a scattered polynomial of index 2 is $f(X)=X+\alpha X^q+\sum_{j\geq 3}\beta_j X^{q^j}$, for $\alpha,\beta_j \in \mathbb{F}_{q^r}$. Let $q^{k_M}=\deg(f(X))$. By Proposition 4.1 if $k_M \geq 6$ is even or $k_M \geq 3$ is odd then $f(X)$ is not scattered.

If $k_M=3$ since q is odd, $f(X)$ is not exceptional scattered from [18, Theorem 1.2].

Hence $k_M=4$. From Remark 4.2, if $\alpha\beta_3 \neq 0$, the size of $\mathcal{I}$ is equal to $q+1$ and a contradiction arises from (4.4).

We are left with the case $f(X)=X+\delta X^{q^4}$. The curve $\mathcal{C}_f$ reads

$$\frac{XY^{q^2}-X^{q^2}Y+\delta(X^{q^2}Y-XY^{q^2})^{q^2}}{X^qY-XY^q}=0.$$

If r is even, there exist points (x,y) with $x/y \in (\mathbb{F}_{q^2}\setminus\mathbb{F}_q) \subset \mathbb{F}_{q^r}$ and therefore $f(X)$ is not scattered over any extension of $\mathbb{F}_{q^r}$ (and thus not exceptional scattered).

Consider now r odd and then $\gcd(q^2-1,q^r-1)=q-1$. The affine equation of $\mathcal{C}_f$ can be rewritten as

$$(X^{q^2}Y-XY^{q^2})^{q^2-1}=1/\delta.$$

Note that no points (x,y) with $(x^{q^2}y-xy^{q^2})^{q^2-1}=1/\delta$ satisfy $x=\lambda y$ for some $\lambda \in \mathbb{F}_q$. We distinguish two cases.

- $Norm_{q^r/q}(\delta)=1$. Let $\eta,\theta \in \mathbb{F}_{q^r}$ be such that $\eta^{q-1}=1/\delta$ and $\theta^{q+1}=\eta$. Since the $\mathbb{F}_{q^r}$-rational curve $\mathcal{D}$ of the affine equation $X^{q^2}Y-XY^{q^2}=\theta$ is nonsingular, it is absolutely irreducible. Any $\mathbb{F}_{q^r}$-rational point $(x,y)\in\mathcal{D}$ satisfies

  $$(x^{q^2}y-xy^{q^2})^{q^2-1}=\theta^{q^2-1}=1/\delta$$

  and also belongs to $\mathcal{C}_f$. This shows that $f(X)$ is not scattered over any extension of $\mathbb{F}_{q^r}$ (and thus not exceptional scattered).
- $Norm_{q^r/q}(\delta)\neq 1$. Over $\overline{\mathbb{F}_{q^r}}$ The curve $\mathcal{C}_f$ decomposes as

  $$\prod_{\theta^{q^2-1}=1/\delta}(X^{q^2}Y-XY^{q^2}-\theta)=0,$$

  and each component $X^{q^2}Y-XY^{q^2}-\theta=0$ is absolutely irreducible. Since $Norm_{q^r/q}(\delta)\neq 1$, any $\theta \notin \mathbb{F}_{q^r}$ and therefore $\mathcal{C}_f$ does not contain any affine $\mathbb{F}_{q^r}$-

rational point. This means that $f(X)$ is scattered over $\mathbb{F}_{q^r}$ and any extension $\mathbb{F}_{q^{kr}}$ with k odd. □

5. The open cases for $t = 0$

In this subsection we prove that Theorem 1.3 (1) holds also for $q \leq 5$, that is for the open cases left in [1]. Since the open cases regards binomials and trinomials in the following we analyze two families of binomials and trinomials in a more general setting.

In this last section, we use a quite different terminology following [42]. A place P of the function field $\mathbb{F}/K$ is the maximal ideal of some valuation ring $\mathcal{O}$ of $\mathbb{F}/K$ and every element $t \in P$ such that $P = t\mathcal{O}$ is called a local parameter for P; see [42, Definition 1.1.8]. Every $0 \neq z \in \mathbb{F}/K$ has a unique representation $z = t^n u$, with $u \in \mathcal{O}$ invertible and $n \in \mathbb{Z}$. We define the valuation $v_P(z)$ of z at P as $v_P(z) := n$ and $v_P(0) := \infty$.

Denote by $\mathbb{K}$ the algebraic closure of the finite field $\mathbb{F}_q$. A curve $\mathcal{C}$ in some affine or projective space over $\mathbb{K}$ is said to be defined over $\mathbb{F}_q$ if the ideal of $\mathcal{C}$ is generated by polynomials with coefficients in $\mathbb{F}_q$. Let $\mathbb{K}(\mathcal{C})$ denote the function field of $\mathcal{C}$. The subfield $\mathbb{F}_q(\mathcal{C})$ of $\mathbb{K}(\mathcal{C})$ consists of the rational functions on $\mathcal{C}$ defined over $\mathbb{F}_q$. The extension $\mathbb{K}(\mathcal{C}) : \mathbb{F}_q(\mathcal{C})$ is a constant field extension; see [42, Section 3.6]. In particular, ($\mathbb{F}_q$-)rational places of $\mathbb{F}_q(\mathcal{C})$ can be viewed as the restrictions to $\mathbb{F}_q(\mathcal{C})$ of places of $\mathbb{K}(\mathcal{C})$ that are fixed by the Frobenius map on $\mathbb{K}(\mathcal{C})$. The center of an $\mathbb{F}_q$-rational place is an $\mathbb{F}_q$-rational point of $\mathcal{C}$; conversely, if P is a simple $\mathbb{F}_q$-rational point of $\mathcal{C}$, then the only place centered at P is $\mathbb{F}_q$-rational. Hasse-Weil bound in this context is the following.

Theorem 5.1. *[42, Theorem 5.2.3] The number N_q of $\mathbb{F}_q$-rational places of a function field $\mathbb{F}$ with constant field $\mathbb{F}_q$ and genus g satisfies*

$$|N_q - (q+1)| \leq 2g\sqrt{q}.$$

In what follows we will make use a number of times of a particular case of [42, Corollary 3.7.4].

Proposition 5.2. *Consider an algebraic function field $\mathbb{F}$ with constant field $\mathbb{L}$ containing a primitive n-th root of unity ($n > 1$ and n relatively prime to the characteristic of $\mathbb{L}$). Let $u \in \mathbb{F}$ be such that there is a place Q of $\mathbb{F}$ with $gcd(v_Q(u), n) = 1$. Let $\mathbb{F}' = \mathbb{F}(y)$ with $y^n = u$. Then $T^n - u$ is the minimal polynomial of u over $\mathbb{F}$ and $\mathbb{L}$ is the constant field of $\mathbb{F}'$.*

5.1. General binomials

Consider a curve of type $\mathcal{X}_f : F(X, Y) = 0$, where

$$F(X,Y) = \frac{(X^{q^n} + bX^{q^m})Y^{q^t} - (Y^{q^n} + bY^{q^m})X^{q^t}}{X^qY - XY^q} \in \mathbb{F}_{q^k}(X,Y),$$

where $n < m$ and $b \in \mathbb{F}_{q^k}$. Now,

$$F(X, XY) = \frac{(X^{q^n} + bX^{q^m})X^{q^t}Y^{q^t} - (X^{q^n}Y^{q^n} + bX^{q^m}Y^{q^m})X^{q^t}}{X^{q+1}(Y - Y^q)}$$
$$= X^{q^n+q^t-q-1}\frac{(1 + bX^{q^m-q^n})Y^{q^t} - (Y^{q^n} + bX^{q^m-q^n}Y^{q^m})}{(Y - Y^q)}.$$

We have that $G(X, Y) = F(X, XY) = 0$ if and only if (apart from $X = 0$)

$$bX^{q^m-q^n}\frac{Y^{q^t} - Y^{q^m}}{Y^q - Y} + \frac{Y^{q^t} - Y^{q^n}}{Y^q - Y},$$

that is

$$bX^{q^m-q^n} = \frac{Y^{q^n} - Y^{q^t}}{Y^{q^t} - Y^{q^m}}.$$

Consider $U = X^{q^n}$, $V = Y^{q^{\min(t,n)}}$, therefore

$$bU^{q^{m-n}-1} = \frac{V^{q^{n-\min(t,n)}} - V^{q^{t-\min(t,n)}}}{V^{q^{t-\min(t,n)}} - V^{q^{m-\min(t,n)}}}.$$

- Suppose $t < n < m$. Then

$$bU^{q^{m-n}-1} = \frac{V^{q^{n-t}} - V}{V - V^{q^{m-t}}}.$$

- Suppose $n < t \leq m$. Then

$$bU^{q^{m-n}-1} = \frac{V - V^{q^{t-n}}}{V^{q^{t-n}} - V^{q^{m-n}}} = \frac{V - V^{q^{t-n}}}{(V - V^{q^{m-t}})^{q^{t-n}}}.$$

- Suppose $n < m < t$. Then

$$bU^{q^{m-n}-1} = \frac{V - V^{q^{t-n}}}{V^{q^{t-n}} - V^{q^{m-n}}} = \frac{V - V^{q^{t-n}}}{(V^{q^{t-m}} - V)^{q^{m-n}}}.$$

First note that only a finite number of points of the curves defined by the above equations are contained in lines $U = \alpha V$ with $\alpha \in \mathbb{F}_q$. Suppose that $m - t \neq t - n$, that is the three integers are not in arithmetical progression. Therefore the function field $\overline{\mathbb{F}_{q^k}}(U, V)$ defined by $U^r = \phi(U)$, for some r, in the equations above is a Kummer extension of the rational function field $\overline{\mathbb{F}_{q^k}}(V)$. If r is coprime with $p = char(\mathbb{F}_{q^k})$ and there exists a place Q in $\overline{\mathbb{F}_{q^k}}(V)$ with $gcd(v_Q(\phi(V)), r) = 1$, by Proposition 5.2 $T^r - \phi(V)$ is irreducible over $\overline{\mathbb{F}_{q^k}}(V)$. By [4, Lemma 2.4] applied to $F = \mathbb{F}_{q^k}(V)$, $f = T^n - \phi(V)$,

$z = U$, the constant field of $\mathbb{F}_{q^k}(U,V)$ is $\mathbb{F}_{q^k}$. By Hasse-Weil Theorem, the number of $\mathbb{F}_{q^k}$-rational places N_{q^k} of $\mathbb{F}_{q^k}(U,V)$ grows as k grows.

This means that, for k large enough, the curve $U^r = \phi(V)$ contains $\mathbb{F}_{q^k}$-rational points (u_0, v_0) (the centers of the $\mathbb{F}_{q^k}$-rational places above) such that $v_0/u_0 \notin \mathbb{F}_q$ and then $X^{q^n} + bX^{q^m}$ is not exceptional scattered.

5.2. Particular trinomial in characteristic 2

Now we consider the following trinomial

$$f_k(X) = X^{2^{k-2}} + aX^{2^{k-1}} + bX^{2^k},$$

where $a, b \in \mathbb{F}_{2^n}^*$.

Proposition 5.3. *The polynomial f_k, $k > 2$, $a, b \in \mathbb{F}_{2^n}^*$, is not exceptional scattered of index $t = 0$.*

Proof. Consider the curve $\mathcal{C}_k$ associated with f_k.

$$\mathcal{C}_k : \frac{(X^{2^{k-2}} + aX^{2^{k-1}} + bX^{2^k})Y + (Y^{2^{k-2}} + aY^{2^{k-1}} + bY^{2^k})X}{XY(X+Y)} = 0.$$

Let us consider the isomorphism $(X, Y) \mapsto (X, XY)$. The equation of the new curve is

$$\frac{(X^{2^{k-2}} + aX^{2^{k-1}} + bX^{2^k})XY + (X^{2^{k-2}}Y^{2^{k-2}} + aX^{2^{k-1}}Y^{2^{k-1}} + bX^{2^k}Y^{2^k})X}{X^3Y(1+Y)} = 0,$$

that is (dividing also by $X^{2^{k-2}-2}$)

$$\frac{Y^{2^{k-2}-1}+1}{Y+1} + aX^{2^{k-1}-2^{k-2}}\frac{Y^{2^{k-1}-1}+1}{Y+1} + bX^{2^k-2^{k-2}}\frac{Y^{2^k-1}+1}{Y+1} = 0.$$

Let $U = X^{2^{k-2}}$, then the above equation reads

$$bU^3 + aU\frac{Y^{2^{k-1}-1}+1}{Y^{2^k-1}+1} + \frac{Y^{2^{k-2}-1}+1}{Y^{2^k-1}+1} = 0. \tag{5.1}$$

The curve defined above is irreducible if and only if $U - \alpha(Y)$ is not a factor of $bU^3 + aU\frac{Y^{2^{k-1}-1}+1}{Y^{2^k-1}+1} + \frac{Y^{2^{k-2}-1}+1}{Y^{2^k-1}+1}$ for any $\alpha(Y) \in \overline{\mathbb{F}_q}(Y)$. This is equivalent to say that there is no solution $\overline{U} = \frac{F(Y)}{G(Y)} \in \overline{\mathbb{F}_q}(Y)$ of Equation (5.1), that is no element in the rational function field $\overline{\mathbb{F}_q}(Y)$ is a root of the polynomial

$$\psi(T) = bT^3 + aT\frac{Y^{2^{k-1}-1}+1}{Y^{2^k-1}+1} + \frac{Y^{2^{k-2}-1}+1}{Y^{2^k-1}+1}.$$

Suppose that there exists $\overline{U} \in \overline{\mathbb{F}_q}(Y)$ root of $\psi(T)$.

- Suppose k even and let η be such that $\mathbb{F}_4^* = \langle \eta \rangle$. Consider P_η the place in $\overline{\mathbb{F}_q}(Y)$ corresponding to η. Then

$$v_{P_\eta}\left(\frac{Y^{2^{k-1}-1}+1}{Y^{2^{k-1}}+1}\right) = -1, \qquad v_{P_\eta}\left(\frac{Y^{2^{k-2}-1}+1}{Y^{2^{k-1}}+1}\right) = 0.$$

  Since $v_{P_\eta}(\overline{U})$ is an integer,

$$3v_{P_\eta}(\overline{U}) \neq v_{P_\eta}\left(\frac{Y^{2^{k-1}-1}+1}{Y^{2^{k-1}}+1}\overline{U}\right) = v_{P_\eta}(\overline{U}) - 1.$$

  Recall that for any place P, $v_P(u_1+u_2) = \min\{v_P(u_1), v_P(u_2)\}$ if $v_P(u_1) \neq v_P(u_2)$. So,

$$\infty = v_{P_\eta}(0) = v_{P_\eta}(\psi(\overline{U})) = \begin{cases} -1, & \text{if } v_{P_\eta}(\overline{U}) \geq 0 \\ 3v_{P_\eta}(\overline{U}), & \text{if } v_{P_\eta}(\overline{U}) < 0 \end{cases},$$

  a contradiction.
- Suppose k odd. Then all the places of $\overline{\mathbb{F}_q}(Y)$ corresponding to roots of $Y^{2^{k-1}}+1$ are not poles of $\overline{U}$ (same argument as above). All the other places of $\overline{\mathbb{F}_q}(Y)$ are not poles of $\frac{Y^{2^{k-1}-1}+1}{Y^{2^{k-1}}+1}$ nor of $\frac{Y^{2^{k-2}-1}+1}{Y^{2^{k-1}}+1}$ and therefore they are not poles of $\overline{U}$. This means that the unique pole of a root $\overline{U}$ of $\psi(T)$ is P_∞. Arguing as above, the unique possibility is that $v_{P_\infty}(\overline{U}) = 2^{k-2}$, that is $G(Y)$ is a constant and $F(Y)$ has degree 2^{k-2}. Thus

$$b(Y^{2^{k-1}}+1)F(Y)^3 + aF(Y)(Y^{2^{k-1}-1}+1) + Y^{2^{k-2}-1} + 1 = a_0 Y^{3\cdot 2^{k-2}+2^{k-1}} + \cdots$$

  should vanish. Since $a_0 \neq 0$, a contradiction arises.

So Equation (5.1) has no solution in $\overline{\mathbb{F}_q}(Y)$ and so it defines an absolutely irreducible $\mathbb{F}_{2^n}$-rational curve. Since $\mathcal{C}_k$ is $\mathbb{F}_2$-isomorphic to it, $\mathcal{C}_k$ is absolutely irreducible too of degree $2^k - 2$.

The claim now follows from Theorem 2.3. □

Acknowledgments

The first author was partially supported by the Italian Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) and by the Gruppo Nazionale per le Strutture Algebriche, Geometriche e le loro Applicazioni (GNSAGA-INdAM). The authors would like to thank the anonymous referees who provided useful and detailed comments on a previous version of the manuscript.

References

[1] D. Bartoli, Y. Zhou, Exceptional scattered polynomials, J. Algebra 509 (2018) 507–534.
[2] S. Ball, A. Blokhuis, M. Lavrauw, Linear $(q+1)$-fold blocking sets in $\mathrm{PG}(2, q^4)$, Finite Fields Appl. 6 (4) (2000) 294–301.
[3] D. Bartoli, K.-U. Schmidt, Low-degree planar polynomials over finite fields of characteristic two, J. Algebra 535 (2019) 541–555.
[4] D. Bartoli, P. Speziali, G. Zini, Complete $(k, 4)$-arcs from quintic curves, J. Geom. 108 (3) (2017) 985–1011.
[5] D. Bartoli, M. Giulietti, G. Marino, O. Polverino, Maximum scattered linear sets and complete caps in Galois spaces, Combinatorica 38 (2) (2018) 255–278.
[6] A. Blokhuis, M. Lavrauw, Scattered spaces with respect to a spread in $\mathrm{PG}(n, q)$, Geom. Dedic. 81 (1) (2000) 231–243.
[7] A. Blokhuis, M. Lavrauw, On two-intersection sets with respect to hyperplanes in projective spaces, J. Comb. Theory, Ser. A 99 (2) (2002) 377–382.
[8] I. Cardinali, O. Polverino, R. Trombetti, Semifield planes of order q^4 with kernel F_{q^2} and center F_q, Eur. J. Comb. 27 (6) (2006) 940–961.
[9] F. Caullery, A new large class of functions not APN infinitely often, Des. Codes Cryptogr. 73 (2) (2014) 601–614.
[10] F. Caullery, K.-U. Schmidt, On the classification of hyperovals, Adv. Math. 283 (2015) 195–203.
[11] F. Caullery, K.-U. Schmidt, Y. Zhou, Exceptional planar polynomials, Des. Codes Cryptogr. 78 (3) (2016) 605–613.
[12] B. Csajbók, G. Marino, O. Polverino, Classes and equivalence of linear sets in $\mathrm{PG}(1, q^n)$, J. Comb. Theory, Ser. A 157 (2018) 402–426.
[13] B. Csajbók, G. Marino, O. Polverino, C. Zanella, A new family of MRD-codes, Linear Algebra Appl. 548 (2018) 203–220.
[14] B. Csajbók, G. Marino, O. Polverino, F. Zullo, Maximum scattered linear sets and MRD-codes, J. Algebraic Comb. 46 (3–4) (2017) 517–531.
[15] B. Csajbók, C. Zanella, On the equivalence of linear sets, Des. Codes Cryptogr. 81 (2) (2016) 269–281.
[16] N. Durante, R. Trombetti, Y. Zhou, Hyperovals in Knuth's binary semifield planes, Eur. J. Comb. 62 (2017) 77–91.
[17] G.L. Ebert, G. Marino, O. Polverino, R. Trombetti, Infinite families of new semifields, Combinatorica 29 (6) (2009) 637–663.
[18] A. Ferraguti, G. Micheli, Exceptional scatteredness in prime degree, J. Algebra 565 (2021) 691–701.
[19] M.D. Fried, M. Jarden, Field Arithmetic, 3rd ed., Springer-Verlag, Berlin, 2008.
[20] W. Fulton, Algebraic Curves. An Introduction to Algebraic Geometry, Advanced Book Classics, Addison–Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989, notes written with the collaboration of Richard Weiss, reprint of 1969 original.
[21] F. Hernando, G. McGuire, Proof of a conjecture on the sequence of exceptional numbers classifying cyclic codes and APN functions, J. Algebra 343 (1) (2011) 78–92.
[22] F. Hernando, G. McGuire, Proof of a conjecture of Segre and Bartocci on monomial hyperovals in projective planes, Des. Codes Cryptogr. 65 (3) (2012) 275–289.
[23] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic Curves over a Finite Field, Princeton Series in Applied Mathematics, Princeton University Press, Princeton, 2008.
[24] H. Janwa, G. Mcguire, R. Wilson, Double-error-correcting cyclic codes and absolutely irreducible polynomials over $GF(2)$, J. Algebra 178 (2) (1995) 665–676.
[25] D. Jedlicka, APN monomials over $GF(2^n)$ for infinitely many n, Finite Fields Appl. 13 (4) (2007) 1006–1028.
[26] S. Kopparty, S. Yekhanin, Detecting rational points on hypersurfaces over finite fields, in: Computational Complexity, 23rd Annual IEEE Conference, 2008, CCC '08, 2008, pp. 311–320.
[27] M. Lavrauw, Scattered spaces in Galois geometry, in: Contemporary Developments in Finite Fields and Applications, World Scientific, 2016, pp. 195–216.
[28] M. Lavrauw, G. Van de Voorde, Field reduction and linear sets in finite geometry, in: G. Kyureghyan, G. Mullen, A. Pott (Eds.), Contemporary Mathematics, vol. 632, American Mathematical Society, 2015, pp. 271–293.
[29] E. Leducq, Functions which are PN on infinitely many extensions of $\mathbb{F}_p$, p odd, Des. Codes Cryptogr. 75 (2) (2015) 281–299.

[30] G. Lunardon, Linear k-blocking sets, Combinatorica 21 (4) (2001) 571–581.
[31] G. Lunardon, G. Marino, O. Polverino, R. Trombetti, Maximum scattered linear sets of pseudoregulus type and the Segre variety $\mathcal{S}_{n,n}$, J. Algebraic Comb. 39 (4) (2014) 807–831.
[32] G. Lunardon, O. Polverino, Blocking sets of size $q^t+q^{t-1}+1$, J. Comb. Theory, Ser. A 90 (1) (2000) 148–158.
[33] G. Lunardon, O. Polverino, Blocking sets and derivable partial spreads, J. Algebraic Comb. 14 (1) (2001) 49–56.
[34] G. Lunardon, R. Trombetti, Y. Zhou, Generalized twisted Gabidulin codes, J. Comb. Theory, Ser. A 159 (2018) 79–106.
[35] G. Lunardon, R. Trombetti, Y. Zhou, On kernels and nuclei of rank metric codes, J. Algebraic Comb. 46 (2) (2017) 313–340.
[36] G. Marino, O. Polverino, R. Trombetti, Towards the classification of rank 2 semifields 6-dimensional over their center, Des. Codes Cryptogr. 61 (1) (2011) 11–29.
[37] K. Morrison, Equivalence for rank-metric and matrix codes and automorphism groups of Gabidulin codes, IEEE Trans. Inf. Theory 60 (11) (2014) 7035–7046.
[38] O. Polverino, Linear sets in finite projective spaces, Discrete Math. 22 (2010) 3096–3107.
[39] F. Rodier, Functions of degree $4e$ that are not APN infinitely often, Cryptogr. Commun. 3 (4) (2011) 227–240.
[40] K.-U. Schmidt, Y. Zhou, Planar functions over fields of characteristic two, J. Algebraic Comb. 40 (2) (2014) 503–526.
[41] J. Sheekey, A new family of linear maximum rank distance codes, Adv. Math. Commun. 10 (3) (2016) 475–488.
[42] H. Stichtenoth, Algebraic Function Fields and Codes, 2nd edn., Graduate Texts in Mathematics, vol. 254, Springer, Berlin, 2009.
[43] M.E. Zieve, Planar functions and perfect nonlinear monomials over finite fields, Des. Codes Cryptogr. 75 (1) (2015) 71–80.