Journal of Combinatorial Theory, Series A 204 (2024) 105851

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

journal homepage: www.elsevier.com/locate/jcta

Algebraic approach to the completeness problem for (k, n)-arcs in planes over finite fields

Gábor Korchmáros [a], Gábor P. Nagy [b,c,*], Tamás Szőnyi [d,e]

[a] *Dipartimento di Matematica, Informatica ed Economia, Università degli Studi della Basilicata, viale dell'Ateneo Lucano 10, 85100 Potenza, Italy*
[b] *Bolyai Institute University of Szeged, Aradi vértanúk tere 1, H-6720 Szeged, Hungary*
[c] *Department of Algebra Budapest University of Technology and Economics, Műegyetem rkp. 3, H-1111 Budapest, Hungary*
[d] *Institute of Mathematics, ELTE Eötvös Loránd University and HUN-REN-ELTE Geometric and Algebraic Combinatorics Research Group, Pázmány Péter sétány 1/C, H-1117 Budapest, Hungary*
[e] *FAMNIT, University of Primorska, Glagoljaska 8, 6000 Koper, Slovenia*

ARTICLE INFO

Article history:
Received 26 February 2023
Received in revised form 29 November 2023
Accepted 4 December 2023
Available online xxxx

Keywords:
(k, n)-arcs in PG$(2, q)$
Algebraic curves
Galois theory

ABSTRACT

In a projective plane over a finite field, complete (k, n)-arcs with few characters are rare but interesting objects with several applications to finite geometry and coding theory. Since almost all known examples are large, the construction of small ones, with k close to the order of the plane, is considered a hard problem. A natural candidate to be a small (k, n)-arc with few characters is the set $\Omega(\mathcal{C})$ of the points of a plane curve $\mathcal{C}$ of degree n (containing no linear components) such that some line meets $\mathcal{C}$ transversally in the plane, i.e. in n pairwise distinct points. Let $\mathcal{C}$ be either the Hermitian curve of degree $q+1$ in PG$(2, q^{2r})$ with $r \geq 1$, or the rational BKS curve of degree $q+1$ in PG$(2, q^r)$ with q odd and $r \geq 1$. Then $\Omega(\mathcal{C})$ has four and seven characters, respectively. Furthermore, $\Omega(\mathcal{C})$ is small as both curves are either maximal or minimal. The completeness problem is investigated by an algebraic approach based on Galois theory and on the Hasse-Weil lower bound. Our main result for the Hermitian case is

* Corresponding author.
E-mail addresses: gabor.korchmaros@unibas.it (G. Korchmáros), nagyg@math.u-szeged.hu, nagy.gabor.peter@ttk.bme.hu (G.P. Nagy), tamas.szonyi@ttk.elte.hu, tamas.szonyi@famnit.upr.si (T. Szőnyi).

https://doi.org/10.1016/j.jcta.2023.105851

that $\Omega(\mathcal{C})$ is complete for $r \geq 4$. For the rational BKS curve, $\Omega(\mathcal{C})$ is complete if and only if r is even. If r is odd then the uncovered points by the $(q+1)$-secants to $\Omega(\mathcal{C})$ are exactly the points in $\mathrm{PG}(2,q)$ not lying in $\Omega(\mathcal{C})$. Adding those points to $\Omega(\mathcal{C})$ produces a complete $(k, q+1)$-arc in $\mathrm{PG}(2,q^r)$, with $k = q^r + q$. The above results do not hold true for $r = 2$ and there remain open the case $r = 3$ for the Hermitian curve, and the cases $r = 3, 4$ for the rational BKS curve. As a by product we also obtain two results of interest in the study of the Galois inverse problem for $\mathrm{PGL}(2,q)$.

1. Introduction

Let k, n with $2 \leq n < k$ be two positive integers. In the projective plane $\mathrm{PG}(2,q)$ over a finite field $\mathbb{F}_q$ of order q, a (k,n)-arc is point-set $\mathcal{K}$ of size k such that n is the maximum number of collinear points in $\mathcal{K}$. The concept of a (k,n)-arc has a useful interpretation in coding theory as the matrix whose columns are the projective coordinates of the points in the arc in $\mathrm{PG}(2,q)$ is the parity check matrix of a $[k, 3, k-n]_q$ almost MDS code which is non-extendible if and only if the corresponding (k,n)-arc is complete. Here, completeness means that the (k,n)-arc is maximal (not contained properly in a larger (k',n)-arc), in other words each point off the (k,n)-arc in $\mathrm{PG}(2,q)$ is incident to some n-secant i.e. lines meeting the (k,n)-arc in exactly n points. An (incidence) character n_i of a (k,n)-arc $\mathcal{K}$ is any integer $0 \leq n_i \leq n$ such that some line meets $\mathcal{K}$ in exactly n_i points. The foundation of the theory of (k,n)-arcs with special attention on their characters was laid down in the 1950s by B. Segre and A. Barlotti.

In the smallest case $n = 2$, plenty of results and constructions are known, especially for larger complete $(k,2)$-arcs; see [16]. In particular, the maximum size of a $(k,2)$-arc is $q+1$ or $q+2$ according as q odd or even. In the odd order case, the $(q+1,2)$-arcs are exactly the sets consisting of all points of an irreducible conic, whereas the classification of $(q+2,2)$-arcs is still open. The second and third largest $(k,2)$-arcs have also been studied intensively. On the other end, there is an elementary lower bound for the size of a complete arc, due to Lunelli and Sce, see [16, Theorem 9.12], and a slight improvement in Theorem 9.13. Probabilistic methods show the existence of complete $(k,2)$-arcs for $k = O(\sqrt{q}\log^c q)$ with a positive constant c. Several effective constructions for small $(k,2)$-arcs are available in the literature (see e.g. [25]), the best explicit example so far is for $k = O(q^{3/4})$.

Our current knowledge of (k,n)-arcs with $n \geq 3$ is much less although well known combinatorial structures embedded in $\mathrm{PG}(2,q)$, such as unitals, nets and other designs, provide inspiring examples of (k,n)-arcs with few characters. The upper bound on k for (k,n)-arcs is due to Barlotti (see [16], Corollary 12.5), and Ball, Blokhuis and Mazzocca [7] showed that it cannot be attained in $\mathrm{PG}(2,q)$, q odd. More details can be found in Chapter 12 of [16]. There is also a combinatorial lower bound, due to Alabdullah

and Hirschfeld [2], analogous to the Lunelli-Sce bound. In this case one can also apply probabilistic methods, and as well as effective constructions, in particular when n is enough large compared to q. Since (k,n)-arcs are truly combinatorial objects, counting arguments and incidence geometry are prevalent in their studies. Algebraic and geometric methods combined with combinatorics have also been successfully developed to construct and investigate new and interesting families of (k,n)-arcs, the principal tools being polarities, geometric transformations, groups of symmetries, and algebraic curves. Nevertheless, the study of (k,n)-arcs is still hard whenever it requires that the (k,n)-arc be complete with only few characters and small size $k \approx q$.

A natural candidate to be such a complete (k,n)-arc is the set of the points of a plane curve $\mathcal{C}$ of degree n (containing no linear components over $\mathbb{F}_q$) such that some line of $\mathrm{PG}(2,q)$ meets $\mathcal{C}$ transversally in $\mathrm{PG}(2,q)$, i.e. in n pairwise distinct points in $\mathrm{PG}(2,q)$. The most interesting families of complete (k,n)-arcs with very few characters are of this kind including Baer subplanes, ovals, classical unitals and Denniston type maximal arcs; see Section 3. In particular, the classical unital in $\mathrm{PG}(2,q^2)$ consists of all points of the Hermitian curve $\mathcal{H}_q$ which is also well known in number theory as being the most important $\mathbb{F}_{q^2}$-maximal curve. Further examples of (k,n)-arcs consisting of the points of (Frobenius non-classical) curves are found in [14] and [8,10,13]. The work by J.W.P. Hirschfeld and F.J. Voloch for cubic curves, and by M. Giulietti and F. Torres for $n \geq 4$, was the first important step towards a kind of sophisticated algebraic theory of (k,n)-arcs arising from plane algebraic curves. A main result in this theory concerns plane curves of degree n defined over a subfield $\mathbb{F}_{\bar{q}}$ of $\mathbb{F}_q$ and viewed as a curve of $\mathrm{PG}(2,q)$: If q is large enough compared to the parameters of $\mathcal{C}$, namely n and $\bar{q}$, then the set of the points of any absolutely irreducible curve $\mathcal{C}$ of degree n in $\mathrm{PG}(2,q)$ is a (k,n)-arc of small size $k \approx q$.

The algebraic theory approach is also adequate to deal with the completeness problem for such (k,n)-arcs even if it needs Galois theory in positive characteristic together with some Dirichlet or Čebotarev type density theorem; see the Bartoli-Micheli paper [6] that finds its origin in previous work by Guralnick, Tucker, Zieve [15] and others on permutation polynomials. The essential idea is to express the condition that a point $P \in \mathrm{PG}(2,q)$ is incident with a line intersecting transversally $\mathcal{C}$ in $\mathrm{PG}(2,q)$ in terms of the Galois closure of the algebraic extension $F|F_P$ where F is the function field of $\mathcal{C}$ and F_P is the rational subfield of F arising from the projection of $\mathcal{C}$ from P. The favorable situation occurs when the (geometric) Galois group $Gal(F|F_P)$ is the symmetric group Sym_n on the roots of the polynomial associated with $F|F_P$. In fact, for this case, a variant of the classical Čebotarev density theorem [21, Theorem 9.13B] works well and ensures the existence of a line ℓ through P meeting transversally $\mathcal{C}$ in $\mathrm{PG}(2,q)$ provided that q is large enough compared to the two parameters of $\mathcal{C}$, namely the degree of $\mathcal{C}$ and the order of the plane $\mathrm{PG}(2,\bar{q})$ where $\mathcal{C}$ is defined. For $Gal(F|F_P) \lneqq \mathrm{Sym}_n$, the (k,n)-arc may not be complete; nevertheless completeness can still be achieved by adding some (at most $O(n)$) points; see [6]. As a corollary, see [6, Theorem 5.3], for all but finitely many n's, if q is large enough, there are complete (k,n)-arcs of small size $k \approx q$.

The question arises whether complete (k,n)-arcs of small size $k \approx q$ can be obtained in this way for (almost) every q. As it appears plausible, at least intuitively, the choice of the curve is critical. We thoroughly work out two cases investigating the Hermitian curve $\mathcal{H}_q$ defined over $\mathbb{F}_{q^2}$ and the rational BKS curve Γ_q defined over $\mathbb{F}_q$, respectively. Our main result for the Hermitian case is that for every $r \geq 4$ the set Ω of points of $\mathcal{H}_q$ is a complete $(k, q+1)$-arc with only four characters $0, 1, 2, q+1$ where $k = q^{2r}+1\pm q^{r+1}(q-1)$ according as r is odd or even; see Theorem 7.2. For the rational BKS case, the set Ω of the points in $\mathrm{PG}(2,q^r)$ is a $(k, q+1)$-arc with $k = q^r + 1 - \frac{1}{2}q(q-1)$ and characters $0, 1, 2, \frac{1}{2}(q+1), \frac{1}{2}(q+3), q, q+1$. Furthermore, Ω is complete if and only if r is even. If r is odd, then the uncovered points by the $(q+1)$-secants to Ω are exactly the points in $\mathrm{PG}(2,q)$ not lying in Ω. Adding those points to Ω produces a complete $(k, q+1)$-arc in $\mathrm{PG}(2,q^r)$, with $k = q^r + q$; see Theorem 7.5.

The above results do not hold true for $r = 2$ and it remains open the case $r = 3$ for the Hermitian curve, and the cases $r = 3, 4$ for the rational BKS curve.

As a by product we also have the following two results of interest in the study of the Galois inverse problem.

Let $K = \bar{\mathbb{F}}_{q^{2r}}(m)$ and $L = K(u)$ where $u^{q+1} + u^q m^q + um - ((ma-b)^q + ma - b)$ and $a^{q+1} + b^q + b \neq 0$. Then the geometric monodromy group of $L|K$ is isomorphic to $\mathrm{PGL}(2,q)$, and the Galois closure M of $L|K$ is $M = \bar{\mathbb{F}}_{q^{2r}}(m,u,v,w)$ where

$$\begin{cases} u^{q+1} + u^q m^q + um - ((ma-b)^q + ma - b) = 0; \\ v^q + (u+m^q)v^{q-1} + u^q + m = 0; \\ v + u + m^q - (u+m^q)w^{q-1} = 0. \end{cases}$$

Let $K = \bar{\mathbb{F}}_{q^r}(t)$ and $L = K(u)$ where $u^{q+1} + um^q + um - (b-2)(t-1) - \frac{1}{2}q + 1$ and $b^{q+1} - (a^q + a) + (b^2 - 4a)^{(q+1)/2} \neq 0$. Then the geometric monodromy group of $L|K$ is isomorphic to $\mathrm{PGL}(2,q)$, and the Galois closure M of $L|K$ is $M = \bar{\mathbb{F}}_{q^r}(m,u,v,w)$ where

$$\begin{cases} u^{q+1} + mu^q + mu - (b-2)(m-1) - \frac{1}{2}a + 1 = 0, \\ v^q + (u+m)v^{q-1} + u^q + m = 0, \\ v + u + m - (u+m)w^{q-1} = 0. \end{cases}$$

2. Outline of the proofs for the Hermitian case

Some more notation is needed: $\mathcal{H}_q$ denotes the (absolutely irreducible) Hermitian curve of homogeneous equation $Y^qZ + YZ^q + X^{q+1} = 0$ defined over $\mathbb{F}_{q^2}$ and viewed as an (absolutely) irreducible curve in $\mathrm{PG}(2,q^{2r})$ for $r \geq 3$, and Ω stands for the set of all points of $\mathcal{H}_q$ in $\mathrm{PG}(2,q^{2r})$ where $k = |\Omega|$ with $k = q^{2r} + 1 \pm q^{r+1}(q-1)$ according as r is odd or even; see for instance [17, Chapter 10]. Then Ω is a $(k, q+1)$-arc in $\mathrm{PG}(2,q^{2r})$. For $r = 1$, Ω is the classical unital, and hence it is a complete $(q^3+1, q+1)$-arc in $\mathrm{PG}(2,q^2)$. This does not hold true for $r = 2$, as Ω in $\mathrm{PG}(2,q^4)$ is contained in $\mathrm{PG}(2,q^2)$

and hence no $(q+1)$-secant to Ω covers a point $P \in \mathrm{PG}(2,q^4) \setminus \mathrm{PG}(2,q^2)$ provided that P is chosen on a tangent line to $\mathcal{H}_q$.

To deal with the completeness problem in the general case, take any point $P \in \mathrm{PG}(2,q^{2r})$ not in $\mathrm{PG}(2,q^2)$. Since $PGU(3,q)$ leaves Ω invariant and preserves no line in $\mathrm{PG}(2,q^{2r})$, we may assume that P is not a point at infinity. Therefore we use affine coordinates with $Z=0$ taken to be the line at infinity. Let $P=(a,b)$. If ℓ_m denotes the (non-vertical) line through P with slope m, i.e. $Y=m(X-a)+b$, and

$$F(X) = X^{q+1} + X^q(a+m^q) + X(a^q+m) + b^q + b + a^{q+1} \in \mathbb{F}_{q^{2r}}[X]$$

then ℓ_m is a $(q+1)$-secant to Ω if and only if $F(X)$ has $q+1$ pairwise distinct roots in $\mathbb{F}_{q^{2r}}$. Now, take an algebraic closure $\bar{\mathbb{F}}$ of $\mathbb{F}_{q^2}$ containing $\mathbb{F}_{q^{2r}}$, and look at $F(X)$ as a polynomial with coefficients in the rational field $K=\bar{\mathbb{F}}(m)$. Two cases are distinguished according as P lies in Ω or does not.

Assume first $P \notin \Omega$. Then $F(X)$ is an irreducible separable polynomial over K. Take a root u of $F(X)$ in some overfield of K, and define $L=K(u)$ to be the algebraic extension of K by adjoining u. The field extension $L|K$ is not Galois. The Galois closure M of $L|K$ is the splitting field of $F(X)$ over K, and the associated Galois group $G=Gal(M|K)$ is the geometric monodromy group of $F(X)$ over K. We prove in our case that $M=K(u,v,w)$. Our proof is based on Abhyankar's work [1], especially on the concept of a twisted Abhyankar's derivative of a polynomial. More precisely, we show in Section 5 that if the first Abhyankar derivative f_1 of F is irreducible then the second Abhyankar derivative f_2 of F splits into linear factors. By [1, Section 2], G acts faithfully on the roots of F as a sharply 3-transitive permutation group whose 2-point stabilizer is cyclic. From Zassenhaus' classification of finite sharply 3-transitive permutation groups [28], $G=\mathrm{PGL}(2,q)$ follows. The missing piece in this argument, i.e. the irreducibility of f_1, is proven in Section 6 where we rely on a classical theorem of van der Waerden [27]. The result $G=\mathrm{PGL}(2,q)$ is quite a surprising since in most cases 2-transitive geometric monodromy groups are either the symmetric group or the alternating group.

The next step is to show that the ramified places in the Galois extension $M|K$ are as many as $(q+1)^2$. From this we deduce that G has $q+1$ short orbits on the set of places of M and that it acts on each short orbit as $\mathrm{PGL}(2,q)$ in its 3-transitive permutation representation.

It turns out that the point P is covered by at least one (non-vertical) line ℓ_m if and only if M has at least one $\mathbb{F}_{q^{2r}}$-rational place unramified in the Galois extension $M|K$. Using Serre's ramification theory [23], see also [17, Section 11.9] and [24, Section III.8], we are able to compute the genus $\mathfrak{g}(M)$ of M. Actually, $\mathfrak{g}(M)$ only depends on q, as $2\mathfrak{g}(M)-2=q^4-q^2-2q-2$ when no tangent to $\mathcal{H}_q$ at a point in $PG(2,q^2)$ passes through P. Results and arguments change a bit when P is covered by a tangent to $\mathcal{H}_q$ at a point in $PG(2,q^2)$. In this case, $2\mathfrak{g}(M)-2=q^4-3q^2$. Now, if

$$q^{2r}+1 > 2\mathfrak{g}q^r + (q+1)^2 > q^{r+4} - q^{r+2} - 2q^{r+1} + q^2 + 2q + 1,$$

then the Hasse-Weil lower bound ensures the existence of $m \in \mathbb{F}_{q^{2r}}$ such that the polynomial $F(X)$ has $q+1$ pairwise distinct roots over $\mathbb{F}_{q^2}$. Therefore, P is covered by a $(q+1)$-secant to Ω. Thus $r = 3$ remains the only open case. A Magma aided search shows that if $q = r = 3$ then Ω is complete.

The case $P \in \Omega$ is treated analogously. Let $P = P(a,b)$ with $b^q + b + a^{q+1} = 0$, and

$$F(X) = X^q + X^{q-1}(a + t^q) + (a^q + t) \in \mathbb{F}_{q^{2r}}[X].$$

Then G acts faithfully on the roots of $F(X)$ as a sharply 2-transitive permutation group, and $G \cong \mathrm{AGL}(1,q)$. Furthermore, G fixes a place of M and has a unique non-trivial short orbit of size q. From this, $\mathfrak{g}(M) = \frac{1}{2}q(q-1)^2$ follows. If

$$q^{2r} + 1 > 2\mathfrak{g}q^r + q + 1 > q^{r+3} - 2q^{r+2} + q^{r+1} + q + 1,$$

then the Hasse-Weil lower bound yields that P lies on a $(q+1)$-secant to Ω. This is indeed the case since as $r \geq 3$ has been assumed.

Polynomials of the form $X^{q+1} + \alpha X^q + \beta X + \gamma \in \mathbb{F}(t)$ and their Galois closures have been the subject of several papers; see [6,11,18–20]. Actually, we were not able to apply those results to our work. For instance, [11, Section 4] and [18, Section 5.1] provide a general sufficient condition in terms of α, β, γ for the existence of $t_0 \in \mathbb{F}_{q^k}$ such that the polynomial $X^{q+1} + \alpha(t_0)X^q + \beta(t_0)X + \gamma(t_0)$ splits into pairwise distinct linear factors defined over $\mathbb{F}_{q^k}$. Unfortunately, that condition in our particular case, $\alpha = m^q, \beta = m, \gamma = -((ma-b)^q + (ma-b))$, becomes too complicate to be applied to our case; see [11, Theorem 4.6], and [18, Theorem 8]. In the last few years, non-existence results for APN, PcN, APcN functions were obtained studying other type of polynomials and their Galois closures; see [3–5].

3. Preliminaries on absolutely irreducibility of polynomials and plane curves

Let

$$P(X) = X^{q+1} + eX^q + aX + b \in \mathbb{F}_{q^s}[X]. \tag{1}$$

As Bluher [11] pointed out if $ea \neq b$ and $a \neq e^q$ then the substitution of X by $(e^{q+1} - b)/(a - e^q)X - e$ brings $P(X)$ to the form $X^{q+1} - BX + B$ where $B = (a-e^q)^{q+1}/(b-ea)^q \in \mathbb{F}_{q^s}^*$. In particular, it has no multiple roots in $\mathbb{F}$. Also, she proved that if $X^{q+1} - BX + B$ has at least three (distinct roots) then all the $q+1$ roots are in $\mathbb{F}_{q^s}$; see [11, Theorem 4.3].

Result 3.1. Set either

$$P(X) = \begin{cases} X^{q+1} + m^q X^q + mX - ((ma-b)^q + ma - b) \in \mathbb{F}_{q^s}[X], \\ m^{q+1} + (ma-b)^q + (ma-b) \neq 0, \end{cases}$$

or

$$P(X) = \begin{cases} 2mX^{q+1} + (2m-1)X^q + (2m-1)X + m(2-a) + b - 2 \in \mathbb{F}_{q^s}[X], \\ 2am^2 - 2mb + 1 \neq 0. \end{cases}$$

Then $P(X)$ has no multiple roots. Furthermore, if $P(X)$ has at least three roots in $\mathbb{F}_{q^s}$ then all its $q+1$ roots are in $\mathbb{F}_{q^s}$.

Lemma 3.2. *Let $a, b \in \mathbb{F}$ such that $\mathbb{F}$ has no element t for which $a = 2(t+1)^{q+1}$ and $b = 2 + t^q + t$. Then the plane curve $\mathcal{C}$ with affine equation*

$$F(U,V) = V(2(U+1)^{q+1} - a) - U^q - U - 2 + b = 0$$

is irreducible.

Proof. The point at infinity V_∞ is an ordinary singular point of $\mathcal{C}$ with multiplicity $q+1$. The tangent lines ℓ_i to $\mathcal{C}$ at V_∞ have equations $U - u_i = 0$ where $(u_i+1)^{q+1} = \frac{1}{2}a$ and $i = 1, 2, \ldots, q+1$. None of them is a linear component of $\mathcal{C}$ as $b \neq 2 + u_i^q + u_i$. Moreover $I(V_\infty, \mathcal{C} \cap \ell_i) = q+2$. If $\mathcal{C}$ is reducible, Segre's criterium, [22, Lemma 8] applies to each ℓ_i. Therefore, $P(U) = \prod_{i=1}^{q+1}(U - u_i)$ divides $F(U,V)$. Since $P(U) = \prod_{i=1}^{q+1}(U+1-(u_i+1)) = (U+1)^{q+1} - \frac{1}{2}a$, this yields $F(U,V) = (2(U+1)^{q+1} - a)F_1(U,V)$ with $\deg(F_1(U,V)) = 1$. Thus $(2(U+1)^{q+1} - a)(V - F_1(U,V)) - (U^q + U + (b-2))$ would be the zero polynomial, a contradiction. Therefore, $\mathcal{C}$ is irreducible. □

Lemma 3.3. *Let $t \in \mathbb{F} \setminus \mathbb{F}_{q^2}$. Then the plane curve $\mathcal{C}$ with affine equation*

$$F(U,V) = V(U^{q-1} + 1) + U^q + tU^{q-1} + t^q = 0$$

is irreducible.

Proof. For $i = 1, \ldots, q-1$, let ℓ_i denote the line of equation $U - u_i = 0$ with $u_i^{q-1} + 1 = 0$. If ℓ_i is a component of $\mathcal{C}$ then $u_i^q + tu_i^{q-1} + t^q = 0$ and hence $t^q - t = u_i$. But then $(t^q - t)^{q-1} = -1$ whence $(t^q - t)^q = -(t^q - t)$ from which $t^{q^2} = t$, that is, $t \in \mathbb{F}_{q^2}$. Therefore, ℓ_i is not a component of $\mathcal{C}$. Therefore, the point at infinity V_∞ is an ordinary singular point of $\mathcal{C}$ with multiplicity $q-1$, and the tangent lines ℓ_i to $\mathcal{C}$ at V_∞ have equations $U - u_i = 0$ where $u_i^{q-1} = -1$ for $i = 1, 2, \ldots q-1$. Now, we argue as in the proof of Lemma 3.2. From Segre's criterium, $P(U) = \prod_{i=1}^{q-1}(U - u_i) = U^{q-1} + 1$ divides $F(U,V)$. Thus $F(U,V) = (U^{q-1} + 1)F_1(U,V)$ with $\deg(F_1(U,V)) = 1$ whence the claim follows. □

4. (k, n)-arcs arising from the Hermitian curve and the rational BKS curve

4.1. The Hermitian curve and its geometry

Let $\mathcal{H}_q$ denote the Hermitian curve given in its canonical form of affine equation

$$X^{q+1} + Y^q + Y = 0. \tag{2}$$

The properties of $\mathcal{H}_q$ pertinent to the present paper are: (i) $\mathcal{H}_q$ is non-singular of genus $\mathfrak{g} = \frac{1}{2}q(q-1)$, (ii) any line ℓ of $\mathrm{PG}(2, q^2)$ either meets $\mathcal{H}_q$ in $q+1$ pairwise distinct points all lying in $\mathrm{PG}(2, q^2)$, or is a tangent to $\mathcal{H}_q$ at a point $P \in \mathrm{PG}(2, q^2)$ and $I(P, \mathcal{H}_q \cap \ell) = q + 1$, in particular, each common point of ℓ with $\mathcal{H}_q$ lies in $\mathrm{PG}(2, q^2)$, (iii) Ω is a complete $(q^3 + 1, q + 1)$-arc with two characters namely 1 and $q + 1$, (iv) the subgroup of $\mathrm{PGL}(3, q^2)$ which leaves $\mathcal{H}_q$ invariant is the projective unitary group $\mathrm{PGU}(3, q)$, (v) $\mathcal{H}_q$ is an $\mathbb{F}_{q^2}$-maximal curve and the set of its points lying in $\mathrm{PG}(2, q^2)$ has size $q^3 + 1$.

From now on, we focus on the case $r \geq 3$. The set Ω consisting of all points of $\mathcal{H}_q$ lying in $\mathrm{PG}(2, q^{2r})$ has size equal to $q^{2r} + 1 \pm q^{n+1}(q - 1)$ according as r is odd or even [17, Chapter 10]. Fix a point $P \in \mathrm{PG}(2, q^{2r})$ not in $\mathrm{PG}(2, q^2)$. Since $\mathrm{PGL}(3, q)$ does not leave the infinite line $Z = 0$ invariant, we may assume $P \notin \ell_\infty$ and use affine coordinates. Then $P = P(a, b)$ with $a, b \in \mathbb{F}_{q^{2r}}$. For any line ℓ through P we determine its common points with $\mathcal{H}_q$. If the vertical line coincides with ℓ then $\mathcal{H}_q \cap \ell$ comprises Y_∞ together with the points $P(a, t)$ such that t is the root of the polynomial $F(Y) = Y^q + Y + a^{q+1} = 0$. If one of the roots belongs to $\mathbb{F}_{q^{2r}}$ then all do. Also, $F(Y)$ is separable and hence ℓ is not a tangent to $\mathcal{H}_q$. Now, let ℓ be a line through P of equation $Y = m(X - a) + b$. Then the common points of ℓ and $\mathcal{H}_q$ are the points $P(\xi, \eta)$ such that ξ is a root of the polynomial

$$F(X) = X^{q+1} + m^q X^q + mX - ((ma - b)^q + ma - b) \tag{3}$$

which can also be written as

$$F(X) = (X^q + m)(X + m^q) - (m^{q+1} + (ma - b)^q + (ma - b)). \tag{4}$$

Then ξ is a multiple root if and only if ξ is a root of the polynomial $dF/dX = X^q + m$ as well, that is, $\xi^q + m = 0$. From (4) this occurs if and only if $m^{q+1} + (ma - b)^q + ma - b = 0$. The polynomial $G(T) = T^{q+1} + (Ta - b)^q + Ta - b$ has a multiple root if and only if $b^q + b + a^{q+1} = 0$, that is, $P(a, b) \in \mathcal{H}_q$. Therefore two cases arise. If $P(a, b) \notin \mathcal{H}_q$ then there exist $q + 1$ lines ℓ_m which are tangent to $\mathcal{H}_q$ and the tangency point of ℓ_m is $P_m = (-\sqrt[q]{m}, m(\xi - a) + b)$ with $\xi^q = -m$. Furthermore, ℓ_m also meets $\mathcal{H}_q$ in the point $R_m = (-m^q, m(\xi - a) + b)$ with $\xi = -m^q$. It is possible that $P_m = R_m$ and this occurs when $\xi^{q^2} - \xi = 0$, that is, $\xi \in \mathbb{F}_{q^2}$. In this case $I(P_m, \mathcal{H}_q \cap \ell_m) = q + 1$. Otherwise, $P_m \neq R_m$ where $I(P_m, \mathcal{H}_q \cap \ell_m) = q$ and $I(R_m, \mathcal{H}_q \cap \ell_m) = 1$. If $P \in \mathcal{H}_q$ then $\mathcal{H}_q$ has a unique tangent ℓ at P where ℓ has equation $Y = -a^q(X - a) + b = -a^q X - b^q$.

Furthermore, $R = (a^{q^2}, b^{q^2})$ is another common point of $\mathcal{H}_q$. Since $P \neq R$ by our assumption, $I(P, \mathcal{H}_q \cap \ell) = q$ and $I(R, \mathcal{H}_q \cap \ell)$=1. Therefore, any tangent to $\mathcal{H}_q$ through P meets Ω in either one or two points, and in the former case the tangency point is in $\mathrm{PG}(2, q^2)$. Take a line ℓ be through P other than tangents ℓ_i. Then $\ell \cap \mathcal{H}_q$ consists of $q+1$ pairwise distinct points lying in some extension of $\mathrm{PG}(2, q^{2r})$. Furthermore, if three of them are in $\mathrm{PG}(2, q^{2r})$ then each of them is in $\mathrm{PG}(2, q^{2r})$. In fact, if three roots of the polynomial $F(T)$ given in (3) belong to $\mathbb{F}_{q^{2r}}$ then all do; see Result 3.1.

The above results show that the set Ω of all points of $\mathcal{H}_q$ in $\mathrm{PG}(2, q^{2r})$ with $r \geq 2$ is a $(k, q+1)$-arc with characters $0, 1, 2, q+1$ where $k = q^{2r} + 1 \pm q^{r+1}(q-1)$ according as r is odd or even.

4.2. The rational BKS curve and its geometry

For q odd, let $\mathcal{C}$ be the curve of affine equation

$$Y^{q+1} - (X^q + X) + (Y^2 - 2X)^{(q+1)/2} = 0. \tag{5}$$

For the known properties of $\mathcal{C}$; see [9, Proposition 4.24]: $\mathcal{C}$ has as many as $\frac{1}{2}q(q-1)$ singular points each of them being a node (ordinary doubly point) lying in $\mathrm{PG}(2, q)$ with both tangents defined over $\mathbb{F}_{q^2}$. The singular points of $\mathcal{C}$ are exactly the internal points to the conic $\mathcal{C}^2$ of affine equation $Y^2 - 2X = 0$. The intersection of $\mathcal{C}$ with a tangent line ℓ at a singular point P of $\mathcal{C}$ collapses into P. More precisely, if γ is a branch of $\mathcal{C}$ centered in P then the intersection multiplicity $I(P, \gamma \cap \ell) = q$ whereas $I(P, \delta \cap \ell) = 1$ for the other branch δ of $\mathcal{C}$ centered in P. The $q+1$ points of $\mathcal{C}^2$ in $\mathrm{PG}(2, q)$ are also points of $\mathcal{C}$. The intersection of $\mathcal{C}$ with the tangent line ℓ at a point $P \in \mathcal{C}^2$ of $\mathcal{C}$ also collapses into P, that is, $I(P, \mathcal{C} \cap \ell) = q+1$. The singular points of $\mathcal{C}$ together with the points of $\mathcal{C}^2$ lying in $\mathrm{PG}(2, q)$ form the set of size $\frac{1}{2}q(q-1) + q + 1$ consisting of all points of $\mathcal{C}$ lying in $\mathrm{PG}(2, q^2)$. The projective closure $\mathcal{D}$ of $\mathcal{C}$ is invariant under the action of a subgroup $G \cong \mathrm{PGL}(2, q)$ of $\mathrm{PGL}(3, q)$ which acts on $\mathcal{C} \cap \mathcal{C}^2$ as $\mathrm{PGL}(2, q)$ in its unique 3-transitive permutation representation. Since $\mathcal{C}$ has degree $q+1$ and possesses $\frac{1}{2}q(q-1)$ nodes, the genus of $\mathcal{C}$ equals zero and hence $\mathcal{C}$ is a rational curve. Thus $\mathcal{C}$ can be parametrized by a variable t over $\mathbb{F} = \bar{\mathbb{F}}_q$. More precisely, $\mathcal{C}$ consists of the points

$$P(t) = (2(t+1)^{q+1}, 2 + t + t^q), \ t \in \bar{\mathbb{F}}_q^* \cup \{\infty\} \tag{6}$$

where ∞ stands for the parameter of the point at infinity $P_\infty = (1 : 0 : 0)$. In this parametrization, $P(t) \in \mathrm{PG}(2, q)$ if and only if $t \in \mathbb{F}_{q^2} \cup \{\infty\}$ where either $t \in \mathbb{F}_q \cup \{\infty\}$ or $t \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ holds according as $P(t) \in \mathcal{C}^2 \cap \mathrm{PG}(2, q)$, or $P(t)$ is an internal point to $\mathcal{C}^2$ in $\mathrm{PG}(2, q)$. In the latter case, case $P(t) = P(t^q)$. For the other points, $P(t) = P(t')$ only occurs for $t = t'$, and $P(t) \in \mathrm{PG}(2, q^r)$ with $r \geq 3$ if and only $t \in \mathbb{F}_{q^r}$.

If a line ℓ is defined over $\mathbb{F}_q$ then the above properties of $\mathcal{C}$ completely determine $\ell \cap \mathcal{C}$: (i) If ℓ is an external line to $\mathcal{C}^2$ in $\mathrm{PG}(2, q)$ then $\ell \cap \mathcal{C}$ consists of $\frac{1}{2}(q+1)$ points each

being a double points of $\mathcal{C}$; (ii) if ℓ is a chord of $\mathcal{C}^2$ in $\mathrm{PG}(2,q)$ with $\ell \cap \mathcal{C}^2 = \{R_1, R_2\}$ then $\ell \cap \mathcal{C}$ comprises R_1, R_2 and $\frac{1}{2}(q-1)$ points each being a double points of $\mathcal{C}$; (iii) if ℓ is a tangent line to $\mathcal{C}^2$ in $\mathrm{PG}(2,q)$ with $\ell \cap \mathcal{C}^2 = \{R\}$ then the intersection collapses into the point R. This shows that the set Ω consisting of all points of $\mathcal{C}$ lying in $\mathrm{PG}(2,q)$ is a (k,n)-arc with $k = \frac{1}{2}q(q-1)+q+1 = \frac{1}{2}(q^2+q+2), n = \frac{1}{2}(q+3)$ and three characters $1, \frac{1}{2}(q+1), \frac{1}{2}(q+3)$. In particular, Ω is not a $(k, q+1)$-arc although it arises from a curve of degree $q+1$. Moreover, since no point of $\mathrm{PG}(2,q^2) \setminus \mathrm{PG}(2,q)$ belongs to $\mathcal{C}$, the set consisting of all points of $\mathcal{C}$ lying in $\mathrm{PG}(2,q)$ will have the same three characters $1, \frac{1}{2}(q+1), \frac{1}{2}(q+3)$.

In $\mathrm{PG}(2,q^r)$ with $r \geq 1$, fix a point P other than those of $\mathcal{C}$ lying in $\mathrm{PG}(2,q)$. We are going to study the possible intersection of $\mathcal{C}$ with a line ℓ through P.

If ℓ has equation $X = a$ then ℓ cuts out on $\mathcal{C}$ the points of parameters t that are the solutions of the equation $(t+1)^{q+1} + \frac{1}{2}a = 0$. If ℓ has equation $Y = b$ then the parameters of the points cut out by ℓ on $\mathcal{C}$ are ∞ together with the solutions of the equation $t^q + t + 2 = b$. If ℓ has equation $Y = \frac{1}{2}(X-a) + b$ then the points cut out by ℓ on $\mathcal{C}$ have parameters t satisfying the equation $t^{q+1} = 1 + \frac{1}{2}a - b$. In all three cases, the solutions of the equations are pairwise distinct and define distinct points of $\mathcal{C}$ unless one of the following cases occurs: either each of these points is counted twice and ℓ is a line of $\mathrm{PG}(2,q)$, or $a = 0$, or $b = \frac{1}{2}a + 1$ and $t = 0$ is the unique solution. In the latter two cases, ℓ is a line of $\mathrm{PG}(2,q)$, as well, since ℓ has equation $X = 0$ and $Y = \frac{1}{2}X + 1$, respectively.

From now on, the line ℓ through $P(a,b)$ is assumed to be distinct from the lines of $\mathrm{PG}(2,q)$.

To determine when ℓ is a tangent to $\mathcal{C}$, we assume that ℓ has slop m with $m \in \mathbb{F}$, and $m \neq 0, \frac{1}{2}$. Then the parameters t of the points of $\mathcal{C}$ cut out by ℓ_m are the roots of the polynomial $m(2(T+1)^{q+1} - a) - 2 - T^q - T + b$ that is of

$$F(T) = 2mT^{q+1} + (2m-1)T^q + (2m-1)T + m(2-a) + b - 2, \tag{7}$$

Then t is a multiple root of $f(T)$ if and only if t is also a root of the polynomial $dF(T)/dT = 2m(T+1)^q - 1$. This together with $F(t) = 0$ yield $(2m-1)t^q + m(2-a) + b - 2 = 0$. Eliminating t^q from the equations $2m(t+1)^q = 1$ and $(2m-1)t^q = -b - 2m - ma + 2$ gives $2am^2 - 2mb + 1 = 0$. Furthermore, if m satisfies $2am^2 - 2mb + 1 = 0$ then

$$F(T) = \frac{1}{2m}(2mT + (2m-1))(2mT^q + (2m-1)),$$

and the converse also holds. From this, if $b^2 - 2a \neq 0$ then through $P = P(a,b)$ there are exactly two tangents to $\mathcal{C}$: For $a \neq 0$, the lines ℓ_i of equation $Y = m_i(X-a) + b$ with $m_i = (b \pm \sqrt{b^2 - 2a})/(2a)$ while for $a = 0$ the line m_1 of equation $Y = \frac{1}{2}b^{-1}X + b$ and the line r_2 of equation $X = 0$. For $b^2 - 2a = 0$, that is, for $P \in \mathcal{C}^2 \setminus \mathcal{C}$, we have $m_1 = m_2$ and there is a unique tangent ℓ_1 to $\mathcal{C}$ where ℓ_1 has equation $Y = b/(2a)(X-a) + b$ and hence is the tangent to $\mathcal{C}^2$ at P. Also, for $i = 1, 2$, ℓ_i has exactly two common points with $\mathcal{C}$,

namely the points P_i, Q_i whose parameters are $(1-2m_i)/(2m_i)$ and $\sqrt[q]{(1-2m_i)/(2m_i)}$. Here, $I(P_i, \mathcal{C} \cap \ell_i) = 1$ and $I(Q_i, \mathcal{C} \cap \ell_i) = q$ unless $P_i = Q_i$ and $I(Q_i, \mathcal{C} \cap \ell_i) = q+1$. In the latter exceptional case, $m_i \in \mathbb{F}_q$. Furthermore, ℓ_i is the tangent to $\mathcal{C}$ at Q_i. This result holds true for r_2 which is the tangent to $\mathcal{C}$ at $O = (0,0)$ where $I(O, \mathcal{C} \cap r_2) = q+1$. From now on set $r_2 = m_2$. With this notation, m_1, m_2 are the tangents to $\mathcal{C}$ through $P(a,b)$ where $m_1 = m_2$ if and only if $P \in \mathcal{C}^2 \setminus \mathcal{C}$. In any case, $m_i \in \mathbb{F}_{q^{2r}}$ where $m_i \in \mathbb{F}_{q^r}$ occurs whenever $b^2 - 2a$ is a square in $\mathbb{F}_{q^r}$. Accordingly, both tangency points P_i, Q_i are in $\mathrm{PG}(2, q^{2r})$ or in $\mathrm{PG}(2, q^r)$. Here, $P_i = Q_i$ is only possible when $m_i \in \mathbb{F}_q$. In particular, both $P_1 = Q_1$ and $P_2 = Q_2$ hold if and only if P is an external point to $\mathcal{C}^2$ in $\mathrm{PG}(2,q)$ and the tangents through P to $\mathcal{C}$ and those to $\mathcal{C}^2$ coincide. Both tangents are lines of $\mathrm{PG}(2,q)$, and this case has already been discussed before.

Finally, let ℓ be a line through P other than the tangents ℓ_i and r_i. If ℓ passes through a (unique) singular point $R \in \mathrm{PG}(2,q)$ of $\mathcal{C}$ then $\ell \cap \mathcal{C}$ consists of R together with $q-1$ pairwise distinct points lying in $\mathrm{PG}(2,q^r)$ or in some extension of $\mathrm{PG}(2,q^r)$. Otherwise, $\ell \cap \mathcal{C}$ consists of $q+1$ pairwise distinct points lying in $\mathrm{PG}(2,q^r)$ or in some extension of $\mathrm{PG}(2,q^r)$. As in the Hermitian case, if three of them are in $\mathrm{PG}(2,q^r)$ then each of them is in $\mathrm{PG}(2,q^r)$; see Result 3.1. Also, since each internal point to $\mathcal{C}$ corresponds to two parameters, Ω has size $q^r + 1 - \frac{1}{2}q(q-1)$

From the above results, the set Ω of all points of $\mathcal{C}$ in $\mathrm{PG}(2,q^r)$ with $r \geq 2$ is a $(q^r + 1 - \frac{1}{2}q(q-1), q+1)$-arc of characters $0, 1, 2, \frac{1}{2}(q+1), \frac{1}{2}(q+3), q, q+1$.

5. Abhyankar's work

An important tool for the study of the action of the Galois group on the roots of its defining polynomial, whenever given by explicit equation, is Abhyankar's skew derivative introduced in [1]. Let

$$f = f(T) = T^m + a_1 T^{m-1} + \ldots + a_m \tag{8}$$

be a separable, monic polynomial in the indeterminate T with coefficients a_i in a field K. The splitting field M of $f(T)$ is generated by K together with the roots $\alpha_1, \alpha_2, \ldots, \alpha_m$ of $f(T)$, and the Galois group $Gal(M|K)$ consists of all K-automorphisms of M. Furthermore, $Gal(M|K)$ acts faithfully on the set $\Delta = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$, and it can be viewed as a permutation group on Δ named the Galois group $Gal(f,K)$ of f (over K). The group $Gal(f,K)$ is transitive on Δ if and only if $f(T)$ is irreducible (over K).

From now on assume that $F(T)$ is irreducible. Following [1, Section 4], we "throw away" a root of $f(T)$, say α_1, and get

$$f_1 = f_1(T) = \frac{f(T)}{T - \alpha_1} = T^{m-1} + b_1 T^{m-1} + \ldots + b_m \in K(\alpha_1)[T]. \tag{9}$$

Then $f_1(T)$ is irreducible over $K(\alpha_1)$ if and only if $Gal(f,K)$ is 2-transitive on Δ. As Abhyankar stressed in [1, Section 4], it does not matter which root of $f(T)$ we throw

away; for instance, the irreducibility of $f_1(T)$ over $K(\alpha_1)$ and, up to isomorphism, the Galois group $Gal(f_1, K(\alpha_1))$ are independent of which root we call α_1. Likewise, by throwing away s roots of f we get

$$f_s = f_s(T) = \frac{f(T)}{(T-\alpha_1)\cdots(T-\alpha_s)} = T^{m-s} + d_1 T^{m-s-1} + \ldots + d_{m-s} \in K(\alpha_1, \ldots, \alpha_s)[T], \tag{10}$$

and f_s is irreducible over $K(\alpha_1, \ldots, \alpha_s)$ for $1 \le s \le m$ if and only if $Gal(f, K)$ is $(s+1)$-transitive on Δ.

For any polynomial $\Theta = \Theta(T)$ in an indeterminate T with coefficients in a field L and for any element $\beta \in L$,

$$\frac{\Theta(T+\beta) - \Theta(\beta)}{T}$$

is the first Abhyankar's twisted T-derivative of T at β; see [1, Art.33]. With this definition, the following result is stated in [1, pg. 93]: If $f = f(T)$ is a nonconstant monic irreducible polynomial in an indeterminate T with coefficients in a field K such that f has no multiple root in any overfield of K, and if α is a root of f in some overfield of K, then by letting $f' = f'(T)$ to be the twisted derivative of f at α we have that the Galois group $Gal(f', K(\alpha))$ is the one-point stabilizer of the Galois group $Gal(f, K)$.

5.1. The Hermitian case

Let $K = \mathbb{F}(m)$ be the rational field over an algebraically closed field $\mathbb{F}$ of positive characteristic p. Fix a power q of p. Consider the polynomial

$$f = f(T) = T^{q+1} + m^q T^q + mT - ((ma-b)^q + ma - b) \in \mathbb{F}(m)[T]. \tag{11}$$

5.1.1. Case $a, b \in \mathbb{F}$ with $a^{q+1} + b^q + b \neq 0$

Lemma 5.1. *$f(T)$ is irreducible over K.*

Proof. In the Hermitian function field $H_q = \mathbb{F}(x, y)$ with $y^q + y - x^{q+1} = 0$, let φ be rational map defined by $\varphi(x) = x, \varphi(y) = (y-b)/(x-a)$. Clearly, φ is birational as $y = \varphi(y)(x-a)+b$. Set $m = \varphi(y)$. Let $g = g(X, Y)$ be a minimal polynomial of x and m. Then H_q coincides with the function field $U = U(x, m)$ where $g(x, m) = 0$. Now, regard (11) as a polynomial $f(X, Y)$ over K with $f(X, Y) = X^{q+1} + Y^q X^q + XY - ((Ya-b)^q + Ya - b)$. Choose an irreducible non-constant factor $h(X, Y) \in \mathbb{F}[X, Y]$ of $f(X, Y)$. Take $\xi, \mu \in \mathbb{F}$ such that $h(\xi, \mu) = 0$. Then $f(\xi, \mu) = 0$ whence $\eta^q + \eta - \xi^{q+1} = 0$ for $\eta = \mu(\xi - a) + b$. This yields $g(\xi, \mu) = 0$. From Study's theorem [17, Theorem 2.10], h divides g. Since g is irreducible, this yields $h = g$. Assume on the contrary that (11) reducible. Then $f(X, Y) = cg(X, Y)^i$ for $i \ge 2$ and a non-zero constant c. Since $\deg(f(X, Y)) = 2q$ this

yields $\deg(g(X,Y)) \le q$. On the other hand, $H_q = U$ implies that these function fields have the same genus $\frac{1}{2}q(q-1)$. But then $\deg(g(X,Y)) \ge q+1$, a contradiction. □

We point out that the curve $\mathcal{C}$ of affine equation $f(X,Y)=0$ introduced in the proof has two singular points, namely the points at infinity of the X and Y axes. Actually, each other point of $\mathcal{C}$ is non-singular. In fact, $f_X(\xi,\eta)=0$ and $f_Y(\xi,\eta)=0$ yield $\eta=-\xi^q$ and $\xi=a$, but $f(\xi,\eta)=U(a,-a^q)=-(a^{q+1}+b^q+b)\neq 0$.

Let u be a root of $f(T)$ in some extension of K and put $L=K(u)$. A straightforward computation shows that the first Abhyankar's skew derivative of f at u is

$$f_1 = f_1(T) = \frac{f(T+u)-f(u)}{T} = T^q + (u+m^q)T^{q-1} + (m+u^q) \in L[X]. \tag{12}$$

Now we compute the second Abhyankar's twisted derivative of $f(T)$, i.e. the Abhyankar's twisted derivative of $f_1(T)$ at any v which is a root of $f(T)$ different from u.

$$\frac{f_1(T)-f_1(v)}{T} = T^{q-1} + (u+m^q)v^{q-1}\frac{(T/v+1)^{q-1}-1}{T}. \tag{13}$$

Let $\Psi(U)$ be the polynomial whose roots are those of $f(T)$ different from u and divided by v. This means replacing T with vU but preserving the splitting field M. Therefore,

$$\Psi(U) = v^{q-1}U^{q-1} + (u+m^q)v^{q-2}\frac{(U+1)^{q-1}-1}{U} =$$

whence $\Psi(U) = v^{q-2}(vU^{q-1} + (u+m^q)((U+1)^{q-2}+(U+1)^{q-3}+\ldots+1)$. We omit the factor v^{q-2}. Then

$$\begin{aligned}
&\Psi(U) = vU^{q-1} + (u+m^q)((U+1)^{q-2}+(U+1)^{q-3}+\ldots+1) = \\
&vU^{q-1} - (u+m^q)(U+1)^{q-1} + (u+m^q)((U+1)^{q-1}+(U+1)^{q-2}+\ldots+1) = \\
&vU^{q-1} - (u+m^q)(U+1)^{q-1} + (u+m^q)((U+1)^q-1)/U) = \\
&vU^{q-1} - (u+m^q)(U+1)^{q-1} + (u+m^q)U^{q-1} = \\
&(v+u+m^q)U^{q-1} - (u+m^q)(U+1)^{q-1}.
\end{aligned}$$

Let $\Gamma(V) = (v+u+m^q) - (u+m^q)(V+1)^{q-1}$ be the polynomial obtained by reciprocating the roots of $\Delta(U)$, i.e. replacing U with $V=U^{-1}$. This does not alter the splitting field M. Finally, let $\Phi(W)$ be the polynomial obtained by adding 1 to the roots of $\Gamma(V)$, i.e. replacing V by $W=V+1$. Again, M is left invariant. Then

$$\Phi(W) = (v+u+m^q) - (u+m^q)W^{q-1}. \tag{14}$$

Therefore the second Abhyankar's skew derivative of $f(T)$ at v is

$$f_2(T) = v^{q-2}((v+u+m^q)T^{q-1} - (u+m^q)(T+v)^{q-1}).$$

We show that if $f_1(T)$ is irreducible over $K(u)$ then $f_2(T)$ is irreducible over $K(u,v)$. Assume on the contrary that $\Phi(W)$ is reducible. Then there exist $\rho \in K(u,v)$ together with a divisor d of $(q-1)$ such that $\rho^d(u+m^q) = v+u+m^q$, otherwise $\Phi(W)$ defines a cyclic Kummer extension of $K(u,v)$ of degree $q-1$; see for instance [24, Appendix A.13]. Let $w = v^{(q-1)/d}$. Then $v^q + (u+m^q)v^{q-1} + m + u^q = (w\rho)^d(u+m^q) + m + u^q = 0$, where $(u+m^q)(m+u^q) \neq 0$. Since $w\rho \in K(u,v)$, and $[K(u,v) : K(u)] = q$ this yields that $w\rho \in K(u)$. From Kummer's theory, there exist $\tau \in K(u)$ together with a divisor r of d such that $-(m+u^q)/(m^q+u) = \tau^r$. Choose a root $m_0 \in \mathbb{F}$ of the polynomial $Y^{q+1} + (Ya-b)^q + Ya - b$ and then $u_0 \in \mathbb{F}$ such that $u_0^q = -m_0$. Then $P(m_0,u_0)$ is a point of the curve $\mathcal{U}$ with function field is $\mathbb{F}(m,u)$ where $\mathcal{U}$ is the curve $\mathcal{C}$ introduced in the proof of Lemma 5.1. As we have already shown after Lemma 5.1, $\mathcal{U}$ is non-singular, as an affine curve. Therefore, $P(m_0,u_0)$ is a non singular point and the tangent to $\mathcal{U}$ at $P(m_0,u_0)$ is the line of equation $U = m_0$. In particular, $m - m_0$ is a local parameter at $P(m_0,u_0)$. Therefore the valuation at $P(m_0,u_0)$ gives $v_{P(m_0,u_0)}(u^q+m) = 1$. Furthermore, $u_0 + m_0^q \neq 0$ otherwise $m \in \mathbb{F}_{q^2}$. Thus $v_{P(m_0,u_0)}(u+m^q) = 0$. Therefore

$$v_{P(m_0,u_0)}\Big(\frac{u^q+m}{u+m^q}\Big) = 1$$

which contradicts $-(m+u^q)/(m^q+u) = \tau^{q-1}$ with $\tau \in K(u) = \mathbb{F}(m,u)$.

Let w be a root of $F(t)$ other than u and v. The third Abhyankar's skew derivative $F_3(T)$ of $f(T)$ at w is obtained by means of the first Abhyankar's skew derivative $\Phi_1 = \Phi_1(W)$ of $\Phi(W)$ at w. From (14),

$$\Phi_1(W) = \frac{\Phi(W+w) - \Phi(w)}{W} = -(u+m^q)w^{q-2}\frac{(W/w+1)^{q-1}-1}{W/w}$$

whence

$$\Phi_1(W) = -\frac{u+m^q}{w}\prod_{i=1}^{q-1}(W + (1-\theta^i)w)$$

for a primitive $(q-1)$-root θ of unity in $\mathbb{F}$. This shows that $\Phi_1(W)$ and hence $f_2(T))$ is a completely reducible polynomial over $K(u,v,w) = \mathbb{F}(m,u,v,w)$. Moreover, $Gal(M|K)$ is a sharply 3-transitive group on Δ such that the 2-point stabilizer is cyclic. From Zassenhaus' theorem [28], $Gal(M/K) \cong \mathrm{PGL}(2,q)$, and $Gal(M/K)$ acts on Δ as $\mathrm{PGL}(2,q)$ on the projective line over $\mathbb{F}_q$.

Theorem 5.2. *Suppose that $f_1(T)$ is irreducible over $K = \mathbb{F}(m)$. Then $f_2(T)$ is irreducible over $K(u)$, and M coincides with $K(u,v,w) = \mathbb{F}(m,u,v,w)$ where the extension $K(u,v,w)|K(u,v)$ is cyclic of degree $q-1$, and $M = \mathbb{F}(m,u,v,w)$ with*

$$\begin{cases} u^{q+1} + m^q u^q + mu - ((ma-b)^q + (ma-b)) = 0, \\ v^q + (u+m^q)v^{q-1} + u^q + m = 0, \\ v + u + m^q - (u+m^q)w^{q-1} = 0. \end{cases} \tag{15}$$

$Gal(M|K) \cong \mathrm{PGL}(2,q)$ is generated by the following three automorphisms defined over $\mathbb{F}_q$ of order $2, p$ and $q-1$ respectively.

$$\begin{array}{llll} \varphi(m)=m, & \varphi(u)=v+u, & \varphi(v)=-v, & \varphi(w)=w^{-1}, \\ \varphi(m)=m, & \varphi(u)=u, & \varphi(v)=vw(w+1)^{-1}, & \varphi(w)=w+1, \\ \varphi(m)=m, & \varphi(u)=u, & \varphi(v)=v, & \varphi(w)=\lambda w, \lambda \in \mathbb{F}_q^*. \end{array}$$

In particular, $Gal(M|K)$ is defined over $\mathbb{F}_{q^2}$.

Proof. We make some computation to show that the above maps are automorphisms of M. We begin with the first one.

$$\begin{array}{l} (v+u)^{q+1} + m^q(v+u)^q + m(v+u) - ((ma-b)^q + (ma-b)) - (u^{q+1} + \\ m^q u^q + mu - ((ma-b)^q + (ma-b)) = v^{q+1} + v^q(u+m^q) + (u+m^q)v = 0. \\ (-v)^q + (u+v+m^q)(-v)^{q-1} + (v+u)^q + m = \\ -(v^q - (u+v+m^q)v^{q-1} - (v^q + u^q + m)) = 0. \\ -v + (v+u) + m^q - (v+u+m^q)w^{-(q+1)} = \\ (u+m^q) - (v+u+m^q)w^{-(q+1)} = 0 \end{array}$$

Now, the computation for the second map.

$$\begin{array}{l} (vw)^q(w+1)^{-q} + (u+m^q)(vw)^{(q-1)}(w+1)^{-(q-1)} + u^q + m = \\ (w+1)^{-q}((vw)^q + (u+m^q)(vw)^{q-1}(w+1) + (u^q+m)(w^q+1)) = \\ (w+1)^{-q}(v^{q-1}w^q(v+u+m^q) + (u+m^q)v^{q-1}w^{q-1} + (u^q+m)w^q + u^q + m) = \\ (w+1)^{-q})((w^q(v^q + (u+m^q)v^{q-1} + u^q + m) + (u+m^q)v^{q-1}w^{q-1} + u^q + m) = \\ (w+1)^{-q}(w^q(v^q + (u+m^q)v^{q-1} + u^q + m) + (u+m^q) + v^{q-1}w^{q-1} + u^q + m) = \\ (w+1)^{-q}((u+m^q)v^{q-1}w^{q-1} + u^q + m) = \\ (w+1)^{-q}(v^{q-1}(v+u+m^q) + u^q + m) = 0. \\ (vw)(w+1)^{-1} + u + m^q - (u+m^q)(1+w)^{q-1} = \\ (w+1)^{-1}(vw + (u+m^q)(w+1) - (u+m^q)(1+w)^q) = \\ (w+1)^{-1}(vw + (u+m^q)w - (u+m^q)w^q + u + m^q - (u+m^q) = \\ (w+1)^{-1}(w(v+u+m^q - (u+m^q)w^{q-1}) = 0. \end{array}$$

Finally, for the third map.

$$v + u + m^q - (u+m^q)(\lambda w)^{q-1} = v + u + m^q - (u+m^q)w^{q-1} = 0.$$

The group generated by the first and the third automorphisms is a dihedral group of order $2(q-1)$ which is a maximal subgroup of $\mathrm{PGL}(2,q)$. Thus, these together with the second automorphism generate the whole $Gal(M|K) = \mathrm{PGL}(2,q)$. □

Lemma 5.3. *Let $\mathcal{F}$ be the affine algebraic curve in* $\mathrm{AG}(3,\mathbb{F})$ *with coordinates* (X,Y,Z) *defined by*

$$\begin{cases} F_1 = X^{q+1} + Y^q X^q + YX - ((Ya-b)^q + (Ya-b)) = 0, \\ F_2 = Z^q + (X+Y^q)Z^{q-1} + X^q + Y = 0, \end{cases} \tag{16}$$

where $a^{q+1}+b^q+b \neq 0$. Let $S=(\xi,\eta,\zeta)$ be a point of $\mathcal{F}$ such that $\xi \notin \mathbb{F}_{q^2}$ and $\zeta \neq 0$. If either $\xi^q+\eta=0$ or $\xi+\eta^q=0$ then S is a non-singular point of $\mathcal{F}$.

Proof. The Jacobian matrix of $\mathcal{F}$ is

$$\begin{pmatrix} \partial F_1/\partial X & \partial F_1/\partial Y & \partial F_1/\partial Z \\ \partial F_2/\partial X & \partial F_2/\partial Y & \partial F_2/\partial Z \end{pmatrix} = \begin{pmatrix} X^q+Y & X-a & 0 \\ Z^{q-1} & 1 & -Z^{q-2}(X+Y^q) \end{pmatrix}$$

Therefore, if S is singular then J has rank 1, that is,

$$\begin{cases} \xi^q + \eta - (\xi-a)\zeta^{q-1} = 0 \\ (\xi^q+\eta)(\xi+\eta^q)\zeta^{q-2} = 0 \\ (\xi-a)(\xi+\eta^q)\zeta^{q-2} = 0. \end{cases} \tag{17}$$

We begin with the case $\xi^q+\eta=0$. By $\zeta\neq 0$ the first equation in (17) yields $\xi=a$ whence $\eta=-a^q$ follows. Therefore, from the first equation in (16), we get $a^{q+1}+b^q+b=0$, a contradiction. Now, $\xi+\eta^q=0$ is assumed. From the first equation in (16), $\zeta^q+\xi^q+\eta=0$. Since $\zeta\neq 0$, this together with the second equation in (17) yield $\zeta+\xi-a=0$ whence $\zeta^q+\xi^q-a^q=0$ follows. Thus, $\eta=-a^q$. Now, the first equation in (16) yields $a^{q+1}+b^q+b=0$, a contradiction. □

5.1.2. Case $a,b\in\mathbb{F}$ with $a^{q+1}+b^q+b=0$

For this choice of a,b, the polynomial $F(T)$ defined in (11) is reducible as $a^{q+1}+b^q+b=0$ yields $F(a)=0$. Replacing T by $T+a$, $F(T)$ becomes $T(T^q+(a+m^q)T^{q-1}+(m+a^q))$. Then dividing it by T,

$$g(T) = T^q + (a+m^q)T^{q-1} + (m+a^q) \in K[T].$$

Lemma 5.4. *$g(T)$ is irreducible over K.*

Proof. Since $g(T)$ and $h(T)=(m+a^q)T^q+(a+m^q)T+1\in K[T]$ are simultaneously irreducible, it is enough to show that the plane curve $\mathcal{U}$ of affine equation $U(X,Y)=(Y+a^q)X^q+(a+Y^q)X+1=0$ is non-singular. Since $\deg(\mathcal{U})=q+1$ and the line ℓ_∞ meets $\mathcal{U}$ in $q+1$ pairwise distinct points, these points are non-singular. Furthermore, $U_X=Y^q+a$ and $U_Y=X^q$. Since the system consisting of the equations $U(X,Y)=0, Y^q+a=0, X^q=0$ has no solution, the claim follows. □

Let u be a root of $g(T)$ in some overfield of K. Comparison of $g(T)$ with (12) shows that the computation in Section 5.1.1 carried out to obtain $f_2(T)$ from $f_1(T)$ can also be used to find the Abhyankar's derivatives $g_1(T)$ and $g_2(T)$ of $g(T)$. From (14),

$$\Phi(W) = (u + a + m^q) - (a + m^q)W^{q-1}.$$

Therefore, the first Abhyankar's derivative $g_1(T)$ of $g(T)$ is

$$g_1(T) = v^{q-2}((u + a + m^q)T^{q-1} - (a + m^q)(T + u)^{q-1}).$$

Moreover, the first Abhyankar's derivative $\Phi_1(T)$ of $\Phi(T)$ at v is,

$$\Phi_1(W) = -\frac{a + m^q}{v} \prod_{i=1}^{q-1} (W + (1 - \theta^i)v).$$

From this, $\Phi_1(W)$ (and hence $g_2(T)$) is a completely reducible polynomial over $K(u, v) = \mathbb{F}(m, u, v)$.

Theorem 5.5. *Let $a \in \mathbb{F}$. Suppose that $g_1(T)$ is irreducible over $K(u)$. Then M coincides with $K(u, v) = \mathbb{F}(m, u, v)$, and the extension $K(u, v)|K(u)$ is cyclic of degree $(q - 1)$. Therefore $M = \mathbb{F}(m, u, v)$ with*

$$\begin{cases} u^q + (a + m^q)u^{q-1} + a^q + m = 0, \\ u + a + m^q - (a + m^q)v^{q-1} = 0. \end{cases} \tag{18}$$

Moreover, $Gal(M|K)$ is a sharply 2-transitive group on Δ such that the 1-point stabilizer is cyclic. From Zassenhaus' theorem [28], $Gal(M/K) \cong \mathrm{AGL}(1, q)$, and $Gal(M/K)$ acts on Δ as $\mathrm{AGL}(1, q)$ on the affine line over $\mathbb{F}_q$.

5.2. The rational BKS case

We use the same method as for the Hermitian case. For this purpose, it is useful to replace $(2m - 1)/2m$ by m. Then (7) becomes the monic polynomial

$$f = f(T) = T^{q+1} + mT^q + mT - (b - 2)(m - 1) - \tfrac{1}{2}a + 1 \in \mathbb{F}[T]. \tag{19}$$

5.2.1. Case $a, b \in \mathbb{F}$ with $b^{q+1} - (a^q + a) + (b^2 - 4a)^{(q+1)/2} \neq 0$

In this case $P(a, b) \notin \mathcal{C}$ and hence there exists no $t \in \mathbb{F}$ such that $a = 2(t+1)^{q+1}$ and $b = t^q + t + 2$. Therefore, Lemma 3.2 applies, and gives the following result.

Lemma 5.6. *$f(T)$ is irreducible over K.*

Let u be a root of $f(T)$ in some extension of K and put $L = K(u)$. A straightforward computation shows that the first Abhyankar's skew derivative of f at u is

$$f_1 = f_1(T) = \frac{f(T+u) - f(u)}{T} = T^q + (u+m)T^{q-1} + u^q + m \in L[X]. \tag{20}$$

Computation to obtain the second Abhyankar's skew derivative of $f(T)$ can be carried out as in Section 5.1.1 determining first $\Phi(W)$.

$$\Phi(W) = (v+u+m) - (u+m)W^{q-1}. \tag{21}$$

Therefore the second Abhyankar's skew derivative of $f(T)$ at v

$$f_2(T) = v^{q-2}((v+u+m)T^{q-1} - (u+m)(T+v)^{q-1}).$$

Furthermore, if $f_1(T)$ is irreducible then the arguments on the third Abhyankar's skew derivative used in Section 5.1.1 remain valid in the present case whenever m^q is replaced by m. In particular, $f_3(T)$ is completely reducible over $K(u,v) = \mathbb{F}(m,u,v)$. Therefore, the following result holds.

Theorem 5.7. *Suppose that $f_1(T)$ is irreducible over $K = \mathbb{F}(m)$. Then $f_2(T)$ is irreducible over $K(u)$, M coincides with $K(u,v,w) = \mathbb{F}(m,u,v,w)$ where the extension $K(u,v,w)|K(u,v)$ is cyclic of degree $q-1$, and $M = \mathbb{F}(m,u,v,w)$ with*

$$\begin{cases} u^{q+1} + mu^q + mu - (b-2)(m-1) - \frac{1}{2}a + 1 = 0, \\ v^q + (u+m)v^{q-1} + u^q + m = 0, \\ v + u + m - (u+m)w^{q-1} = 0. \end{cases} \tag{22}$$

As in the hermitian case, $Gal(M|K)$ is a sharply 3-transitive group on Δ such that the 2-point stabilizer is cyclic. $Gal(M/K) \cong \mathrm{PGL}(2,q)$ and $Gal(M/K)$ acts on Δ as $\mathrm{PGL}(2,q)$ on the projective line over $\mathbb{F}_q$.

5.2.2. Case $a, b \in \mathbb{F}$ with $b^{q+1} - (a^q + a) + (b^2 - 4a)^{(q+1)/2} = 0$

In this case, $P(a,b) \in \mathcal{C}$ and hence there exists $t \in \mathbb{F}$ such that $a = 2(t+1)^{q+1}$ and $b = t^q + t + 2$. Replace T by $T + t$ in (19). Then $f(T) = Tg(T)$ where

$$g(T) = T^q + (m+t)T^{q-1} + m + t^q. \tag{23}$$

From now on we assume $P(a,b) \notin \mathrm{PG}(2,q)$, i.e. $t \notin \mathbb{F}_{q^2}$. From Lemma 3.3 the following claim follows.

Lemma 5.8. *$g(T)$ is irreducible over K.*

Now, the arguments in Section 5.1.2 remain valid if a is replaced by t. Therefore, the following result is obtained.

Theorem 5.9. *Let $t \in \mathbb{F} \setminus \mathbb{F}_{q^2}$. Suppose that $g_1(T)$ is irreducible over $K(u)$. Then M coincides with $K(u,v) = \mathbb{F}(m,u,v)$, and the extension $K(u,v)|K(u)$ is cyclic of degree $(q-1)$. Therefore $M = \mathbb{F}(m,u,v)$ with*

$$\begin{cases} u^q + (t+m)u^{q-1} + t^q + m = 0, \\ u + t + m - (t+m)v^{q-1} = 0. \end{cases} \tag{24}$$

As in the hermitian case, $Gal(M|K)$ is a sharply 2-transitive group on Δ such that the 1-point stabilizer is cyclic. $Gal(M/K) \cong \mathrm{AGL}(1,q)$, and $Gal(M/K)$ acts on Δ as $\mathrm{AGL}(1,q)$ on the affine line over $\mathbb{F}_q$.

In the theorems of this section, Theorems 5.2, 5.5, 5.7 and 5.9, it is assumed that the first Abhyankar's derivative is irreducible. Actually, this hypothesis can be dropped. Our proof requires a further tool, namely a classical theorem due to van der Waerden, and it is detailed in the following section.

6. van der Waerden's theorem

In this section, $L|K$ stands for a finite separable extension of function fields, M for its splitting field (equivalently, for its Galois closure), and $G = \mathrm{Gal}(M|K)$ for the Galois group. Also, $A = \mathrm{Gal}(M|L)$ denotes the Galois group of the Galois extension $M|L$. Furthermore, if P is a place of K and $\mathcal{S}$ is a set of all places of L over P, then $e(S|P)$ and $f(S|P)$ denote the ramification index and the relative degree for $S \in \mathcal{S}$, and W is a place of M lying above P. Moreover, $D(W|P)$ is the decomposition group and $I(W|P)$ is the inertia group. Finally, $f(x)$ denotes an irreducible polynomial over K such that $L = K(\alpha_1)$ for $f(\alpha_1) = 0$.

Artin and later on van der Waerden investigated the action of $D(W|P)$ and $I(W|P)$ on the set of all roots of $f(x)$ and, in particular, how their orbits are linked to the ramification picture of $\mathcal{S}$. The following result is due to van der Waerden.

Result 6.1. ([27, Satz I]) Under the action of $D(W|P)$, the set of all roots of $f(x)$ splits into as many as $|\mathcal{S}|$ orbits. Each $D(W|P)$-orbit consists of $e(S|P)f(S|P)$ roots of $f(x)$ while each $I(W|P)$-orbit does of $e(S|P)$.

In particular, if $L|K$ is ramified at W then $D(W|P)$ is non-trivial.

We reproduce the proof of Result 6.1 using notation and terminology from [17,24].

Let $S \in \mathcal{S}$, and take a place U of M lying over S, Since S lies over P, we have that U is in the G-orbit of W. Therefore, there exists a $g_S \in G$ (not uniquely determined) such that $g_S(P) = U$. Clearly, the cosets Ag_S with S running over $\mathcal{S}$ give a partition of the G-orbit of W. Now, consider the sets $Ag_SD(W|P)$ with S ranging over $\mathcal{S}$.

We show that if $g \in Ag_S D(W|P)$ for some $S \in \mathcal{S}$ then $g^{-1}(\alpha_1)$ and $g_S^{-1}(\alpha_1)$ fall in the same $D(W|P)$-orbit on $\{\alpha_1, \ldots, \alpha_n\}$. Write $g = ag_S d$ with $a \in A$ and $d \in D(W|P)$. Then $g^{-1} = d^{-1} g_S^{-1} a^{-1}$, and hence $g^{-1}(\alpha_1) = d^{-1}(g_S^{-1}(a^{-1}(\alpha_1))) = d^{-1}(g_S^{-1}(\alpha_1))$. Therefore, $g^{-1}(\alpha_1)$ can be viewed as the image of $g_S^{-1}(\alpha_1)$ by d^{-1}. The converse also holds. In fact, let $g^{-1}(\alpha_1) = d^{-1}(g_S^{-1}(\alpha_1))$. Then $(gd^{-1}g_S^{-1})(\alpha_1) = \alpha_1$. Therefore, $gd^{-1}g_S^{-1}$ fixes L element-wise as $L = K(\alpha_1)$. Thus $gd^{-1}g_S^{-1} \in A$ whence $g = ag_S d \in Ag_S D(W|P)$.

Since G is transitive on $\{\alpha_1, \ldots, \alpha_n\}$, each $\alpha_i = g(\alpha_1)$ for some $g \in G$. Therefore there exists a bijective correspondence between the places $S \in \mathcal{Q}$ and the $D(W|P)$-orbits on $\{\alpha_1, \ldots, \alpha_n\}$. Since $D(W|P)$ is not transitive in general on $\{\alpha_1, \ldots, \alpha_n\}$ one can ask to compute the size of such a $D(W|P)$-orbit on $\{\alpha_1, \ldots, \alpha_n\}$.

We show that $e(S|P)f(S|P)$ is the size of the corresponding $D(W|P)$-orbit on $\{\alpha_1, \ldots, \alpha_n\}$. Take $\alpha \in \{\alpha_1, \ldots, \alpha_n\}$. Let $D(W|P)_\alpha$ be the stabilizer of α in $D(W|P)$. Then the size of the $D(W|P)$-orbit of α is given by $|D(W|P)|/|D(W|P)_\alpha|$. We may think about $D(W|P)_\alpha$ as the intersection of $D(W|P)$ with G_α. Take $g \in G$ such that $g^{-1}(\alpha_1) = \alpha$. Then $g^{-1}Ag(\alpha) = \alpha$ and hence $g^{-1}Ag$ fixes $K(\alpha)$ element-wise. Therefore, $G_\alpha = g^{-1}Ag$. This yields

$$\frac{|D(W|P)|}{|D(W|P)_\alpha|} = \frac{|D(W|P)|}{|D(W|P) \cap g^{-1}Ag|}$$

Let $g(W) = U$. When $D(W|P) = g^{-1}D(U|P)g$, and hence $D(W|P) \cap g^{-1}Ag = g^{-1}(D(U|P) \cap A)g$. Since $|D(W|P|) = D(U|P)$, we have

$$\frac{|D(W|P)|}{|D(W|P)_\alpha|} = \frac{|D(U|P)|}{|D(U|P) \cap A|}.$$

Since $M|K$ is a Galois extension, $|D(U|P)| = e(U|P)f(U|P)$. Moreover, $D(U|P) \cap A$ is the stabilizer of A at U. Since $M|L$ is a Galois extension, we also have $D(U|P) \cap A = e(U|S)f(U|S)$. Therefore, the $D(W|P)$ orbit of α has size $e(W|P)f(W|P)/e(W|Q)f(W|Q) = e(S|P)f(S|P)$ whence the first claim follows.

Each $D(S|P)$-orbits on $\{\alpha_1, \ldots, \alpha_n\}$ splits further into $I(S|P)$-orbits. The above argument applied to $I(W|P)$ gives that the size of α under the action of $I(D|P)$-orbit is

$$\frac{|I(W|P)|}{|I(W|P)_\alpha|} = \frac{|I(U|P)|}{|I(U|P) \cap A|} = \frac{e(U|P)}{e(U|Q)} = e(Q|P).$$

This ends the proof of Result 6.1.

Now we look inside the case where $K = \bar{\mathbb{F}}_q(t)$. Then the decomposition and inertia groups coincide. Let $f(x) = x^n + \ldots + a_{n-1}(t)x + a_n(t)$ with $a_i(t) \in \mathbb{F}_q[t]$ and $\deg a_i(t) \le i$. Let $\mathcal{C}$ be the irreducible (possible singular) plane curve of equation $f(X,T) = X^n + \ldots + a_{n-1}(T)X + a_n(T) = 0$. Observe that $X_\infty \notin \mathcal{C}$.

The places of K are the points of the projective line $\mathrm{PG}(1, \bar{\mathbb{F}}_q)$. Let $x_1, \ldots, x_{u(\tau)}$ be the roots of the polynomial $f(X, \tau)$ in the indeterminate X. Geometrically speaking, let

$Q(\tau, x_1), \dots Q(\tau, x_v(\tau))$ be the centers of the branches $\gamma_1, \dots, \gamma_{u(\tau)}$ of $\mathcal{C}$ whose centers lie over τ. Note that $v(\tau) \geq u(\tau)$. Let ℓ_τ be the vertical line through τ. From Bézout's theorem,

$$\sum_{i=1}^{v(\tau)} I(\gamma_i \cap \ell_\tau, Q_i(\tau)) = \deg(\mathcal{C}).$$

Therefore, $\sum_{i=1}^{v(\tau)} e(\gamma_i|\tau) = \deg(f(X,T))$ since $I(\gamma_i \cap \ell_\tau, Q_i(\tau))$ is the ramification index of $e(\gamma_i|\tau)$. Result 6.1 shows that the $D(R|\tau)$ orbits on the set $\{\alpha_1, \dots, \alpha_n\}$ are as many as the $v(\tau)$ orbits and that their sizes are $ord(\gamma_1), \dots, ord(\gamma_v(\tau))$. In particular, if γ_i is linear then $D(P|\tau)$ has a fixed point. This occurs in particular when $Q_i(\tau, \alpha_i)$ is a non-singular point and the tangent to $\mathcal{C}$ at that point is not the vertical line. It turns out that if each of the common points of $\mathcal{C}$ and ℓ is non-singular and ℓ is tangent to $\mathcal{C}$ at exactly one point then $D(R|P)$ is a transposition on $\{\alpha_1, \dots, \alpha_n\}$.

If we drop the hypothesis $\deg a_i(t) \leq i$, some changes are needed. Assume that X_∞ is a point of $\mathcal{C}$. Let γ be a branch of $\mathcal{C}$ centered at Y_∞ with a primitive representation $(x = x(t), y = y(t))$, Two cases arise according as γ is a pole or not of x. In the latter case $x(t) = c_i t^i + c_j t^j + \dots$ with $i \geq 0$ (and $ord(y(t)) < 0$). If $i = 0$ then $x = c_0$ is the tangent of γ, and γ lies over the place c_0 of K, and we have $e(\gamma|c_0) = j$. If $i \geq 1$ then $x = 0$ is the tangent of γ, and γ lies over the place 0 of K and $e(\gamma|0) = i$. Otherwise, $i < 0$ and the tangent line of γ is the line at infinity and γ lies over the place ∞ of K, and we have $e(\gamma|\infty) = -i$.

We illustrate van der Waerden's theorem on three polynomials related to the Hermitian curve and hence to the present work, namely $f_1(x) = x^{q+1} + t^{q+1} + 1$, $f_2(x) = x^q - x - \omega t^{q+1} = 0$ with $\omega^{q-1} = -1$, and $f_3(x) = x^q + t^q X + t = 0$ defined over $\bar{F}_q(t)$. It is worth mentioning that the splitting field of $f_3(x)$ gives rise a function field $\bar{F}_q(x,t)$ with $x^q + t^q x + t = 0$ which is maximal over $\mathbb{F}_{q^6}$.

6.1. Example, Hermitian curve I

Let $\mathcal{C}$ be the Hermitian curve with affine equation $X^{q+1} + T^{q+1} + 1 = 0$. Let $K = \bar{\mathbb{F}}_q(t)$ and $L = K(x)$ with $x^{q+1} + t^{q+1} + 1 = 0$. Then L is a Galois extension of K (i.e. $M = L$) as $Gal(L|K)$ consists of all automorphisms α of $\mathcal{C}$ with $\alpha(t) = t, \alpha(x) = \lambda x$ and $\lambda^{q+1} = 1$. In particular, $Gal(L|K)$ acts on the set of all roots of the polynomial $f(X) = X^{q+1} + t^{q+1} + 1 \in K[X]$ as a sharply transitive permutation group. Let $t_0 \in \bar{\mathbb{F}}_q(t) \cup \{\infty\}$. Then vertical line ℓ through the point $U = (1 : 0 : 0)$ meets $\mathcal{C}$ in pairwise distinct points except for $t_0^{q+1} = 0$ in which case ℓ is the tangent to $\mathcal{C}$ and $I(\mathcal{C} \cap \ell, U) = q + 1$ so that $\mathcal{C} \cap \ell = \{U\}$. From this van der Waerden's theorem follows, since the stabilizer of any place of M in $Gal(L|K)$ is trivial.

6.2. Example, Hermitian curve II

Let $\mathcal{C}$ be the Hermitian curve with affine equation $X^q - X - \omega T^{q+1} = 0$ with $\omega^{q-1} = -1$. Let $K = \bar{\mathbb{F}}_q(t)$ and $L = K(x)$ with $x^q - x - \omega t^{q+1} = 0$. Then L is a Galois extension of K (i.e. $M = L$) as $Gal(L|K)$ consists of all automorphisms α of $\mathcal{C}$ with $\alpha(t) = t, \alpha(x) = x + a$ and $a \in \mathbb{F}_q$. In particular, $Gal(L|K)$ acts on the set of all roots of the polynomial $f(X) = X^q - X - t^{q+1} \in K[X]$ as a sharply transitive permutation group. Let $t_0 \in \bar{\mathbb{F}}_q(t)$. Then vertical line ℓ through the point $U = (t_0, 0)$ meets $\mathcal{C}$ in q pairwise distinct points. $\mathcal{C}$ has a just one point at infinity, namely X_∞. The unique branch γ_∞ of $\mathcal{C}$ centered at X_∞ has a primitive representation $(t = s^{-q}, s^{-1} + \ldots)$ and hence $e(\gamma_\infty|\infty) = q$. This yields van der Waerden's theorem, as the stabilizer of any place of M in $Gal(L|K)$ is trivial.

6.3. Example, Hermitian curve III

Let $\mathcal{C}$ be the curve with affine equation $X^q + T^q X + T = 0$. It is known that $\mathcal{C}$ is (linearly) isomorphic to the Hermitian curve over $\mathbb{F}_{q^6}$. Let $K = \bar{\mathbb{F}}_q(t)$ and $L = K(x)$ with $x^q + t^q x + t = 0$. Then the automorphism group of $\mathcal{C}$ fixing the points $(t_0, 0)$ of $\mathcal{C}$ is trivial. Therefore, $L|K$ is not a Galois extension. Moreover, $\mathcal{C}$ has exactly two points at infinity, namely X_∞ and T_∞. The unique branch γ_∞ of $\mathcal{C}$ centered at T_∞ has a primitive representation $(t = s^{-1}, x = -s^{(q-1)}(1 + \ldots))$ while the unique branch δ_∞ of $\mathcal{C}$ centered at X_∞ has a primitive representation $(t = s^{-(q-1)}(1 + \ldots), x = s^{-q}(1 + \ldots))$. Therefore, L has exactly two places (branches) lying over ∞ and $e(\gamma_\infty|\infty) = 1$, $e(\delta_\infty|\infty) = q - 1$. Van der Waerden's theorem shows that $Gal(M|K)$ has a subgroup that has two orbits on the set $\{\alpha_1, \ldots, \alpha_q\}$ of all roots of $f(X) = X^q + t^q X + t = 0 \in K[x,]$ of size 1 and $q-1$ respectively. Since $Gal(M|K)$ is transitive on $\{\alpha_1, \ldots, \alpha_q\}$ this yields that $Gal(M|K)$ is doubly transitive on $\{\alpha_1, \ldots, \alpha_q\}$. We show that $Gal(M|K)$ is sharply 2-transitive on $\{\alpha_1, \ldots, \alpha_q\}$, and hence $Gal(M|K)$ is the semidirect product of an elementary abelian group of order q by a cyclic complement of order $q - 1$ i.e. $Gal(M/K) \cong \mathrm{AGL}(1, q)$. First we give an explicit equation for M. Let N be an extension of L of degree $q - 1$ defined by $\mathbb{K}(N) = \mathbb{K}(x, t, y)$ with $x^q + xt^q + t = 0$, and $y^{q-1} = t^q$. Clearly, the map $\varphi_\lambda : (x, t, y) \mapsto (x, t, \lambda y)$ with $\lambda \in {\mathbb{F}_q}^*$ is an automorphism of N which fixes L element-wise, and $\Lambda = \{\varphi_\lambda | \lambda \in {\mathbb{F}_q}^*\}$ is (cyclic) group of order $q - 1$. Since $[N : L] = q - 1$, this shows that $N|L$ is a Galois extension with $Gal(M|L) = \Lambda$. Furthermore, for a fixed $\alpha \in \mathbb{F}_{q^2}$ with $\alpha^{q-1} = -1$, the map $\sigma_\alpha : (x, t, y) \mapsto (x + \alpha y, t, y)$ is an automorphism of N which fixes t, and hence K element-wise. In fact, $(x + \alpha y)^q + (x + \alpha y)t^q + t = x^q + xt^q + t + \alpha y(\alpha^{q-1} y^{q-1} + t^q) = 0$. Therefore, $\Sigma = \{\sigma_\alpha | \alpha^{q-1} = -1\} \cup \{id\}$ is an elementary abelian group of order q. Moreover, Σ together with Λ generate a group H of order $q(q-1)$ which is the semidirect product of Σ with complement Λ. Clearly, H fixes t, and hence K element-wise. Let R be the fixed field of H, Then $q(q-1) = |H| = [N : R]$. Since $[N : K] = q(q - 1)$, this yields $K = R$, that is, K is the fixed field of H. As $K \leq L \leq N$, this shows that $M \leq N$ up to a birational isomorphism. On the other

hand, $|Gal(M|K)| \geq q(q-1)$, as $Gal(M|K)$ is a 2-transitive permutation group of degree q, Therefore $N = M$, up to a birational isomorphism. Eliminating t from the equations defining N shows that $N = \mathbb{K}(x, y)$ with $y^{q-1} + x^{q^2} + x^q y^{q(q-1)} = 0$. Replacing xy^{-1} by ξ and y^{-1} by η shows that M is birationally isomorphic to $\mathbb{K}(\xi, \eta)$ with $\eta^{q^2-q+1} + \xi^{q^2} + \xi^q$, and hence $M \cong \mathbb{K}(\xi, \eta); \eta^{q^2-q+1} + \xi^q + \xi = 0$. By a result of Tafazolian and Torres [26], M is $\mathbb{F}_{q^6}$-covered by the Hermitian function field $\mathbb{F}_{q^6}(\mathcal{H}_{q^3})$. In particular, M is $\mathbb{F}_{q^6}$ maximal of genus $g = \frac{1}{2}q(q-1)^2$ and is Galois subcover of $\mathbb{F}_{q^6}(\mathcal{H}_{q^3})$.

7. Case $P \notin \Omega$

We keep up our notation from Sections 5 and 6.

7.1. Hermitian case

We show that the irreducibility condition in Theorem 5.2 is fulfilled. We first prove that $Gal(f, K)$ is 2-transitive on Δ. From Lemma 5.1, $Gal(f, K)$ is transitive on Δ. Therefore, it is sufficient to prove that the 1-point stabilizer of $Gal(f, K)$ on Δ is transitive on the remaining q points.

Consider the function field $L = \mathbb{F}(m, u)$ with $u^{q+1} + m^q u^q + mu - (ma-b)^q + (ma-b)) = (u^q + m)(u + m^q) - (m^{q+1} + (ma-b)^q + ma - b) = 0$, as the algebraic extension $L|K$ of degree $q+1$. Let $m_i \in \mathbb{F}$ with $i = 1, 2, \ldots, q+1$ be the roots of the polynomial $Y^{q+1} + (Ya - b)^q + Ya - b \in \mathbb{F}[Y]$. The results stated in Section 4.1 show that the tangents to $\mathcal{H}_q$ passing through the point $P(a, b)$ are exactly the lines ℓ_i of equation $Y = m_i(x-a)+b$. Furthermore, the tangency point on ℓ_i is $P_i = P_i(-\sqrt[q]{m_i}, m_i(\xi-a)+b)$ with $I(P_i, \mathcal{H}_q \cap \ell_i) = q$, and the remaining intersection of ℓ_i with $\mathcal{H}_q$ is the point $R_i = (-m_i^q, m_i(-m_i^q - a)+b)$ with $I(R_i, \mathcal{H}_q \cap \ell_i) = 1$. Let $\mathcal{S}_i$ be the set of places of $K(u)$ lying over m_i in the covering $K(u)|K$. Then $\mathcal{S}_i = \{P_i, R_i\}$ and $e(P_i|m_i) = q$ and $e(R_i|m_i) = 1$. Let W_i be a place of M lying over m_i in the covering $M|K$. From Result 6.1, the inertia group $I(W_i|m_i)$ has two orbits on the set Δ of the roots of the polynomial (11), one of size q and another of size 1. Therefore, $I(W_i|m_i)$ as a subgroup of $Gal(f, K)$ acting on Δ fixes a point and transitive on the remaining points.

By the results recalled in Section 5.1.1, the 2-transitivity of $Gal(f, K)$ has the following implication.

Proposition 7.1. *The first Abhyankar's skew derivative $f_1(T)$ of $f(T)$ given in (11) is an irreducible polynomial over $K(u)$, and the irreducibility condition in Theorem 5.2 can be dropped.*

Therefore, Theorem 5.2 applies and it determines the structure of $Gal(M|K)$. In fact, $Gal(M|K)$ turns out be a sharply 3-transitive group on Δ such that the 2-point stabilizer is cyclic. From Zassenhaus' theorem [28], $Gal(M/K) \cong \mathrm{PGL}(2, q)$, and $Gal(M/K)$ acts

on Δ as $\mathrm{PGL}(2,q)$ on the projective line over $\mathbb{F}_q$, in its unique 3-transitive permutation representation.

We go on by describing the set $\mathcal{W}_i$ of places of M lying over the place m_i of $K=\mathbb{F}(m)$. As we have observed, the set $\mathcal{S}_i$ of the places of $K(u)$ lying over (m_i) consists of two points P_i and R_i unless $m_i \in \mathbb{F}_{q^2}$ in which case $P_i = R_i$ and hence S_i is reduced in a unique place. We treat these two cases separately using the equations in (15).

7.1.1. Case $m_i \notin \mathbb{F}_{q^2}$

We begin with P_i. The second equation in (15) together with Lemma 5.3 shows that there exist exactly two places in $K(u,v)$ lying over P_i, namely those with center at $P_{i,1}=(m_i,u_i,0)$ and $P_{i,2}$ by $(m_i,u_i,-u_i-m^q)$ respectively. Here $e(P_{i,1}|P_i)=q-1$ and $e(P_{i,2}|P_i)=1$. From the third equation in (15), there exist exactly $q-1$ pairwise distinct places of M lying over $P_{i,1}$, they are centered at $P_{1,i,j}=(m_i,u_i,0,w_i^j)$ where $w_i \in \mathbb{F}_q$ is a fixed primitive $(q-1)$-st root of unity. Here $e(P_{i,1,j}|P_{i,1})=1$. Let κ be the number of places of M lying over $P_{i,2}$. Then $1 \le \kappa \le q-1$, and all these places are centered at $(m_i,u_i,-u_i-m_i^q,0)$. We repeat the same argument for R_i which is the place of $K(u)$ centered at (m_i,u_i) with $u_i+m_i^q=0$. From the second equation in (15), there exists a unique place of $K(u,v)$ lying over R_i, identified by $R_{i,1}=(m_i,u_i,-\sqrt[q]{u_i^q+m_i})$ where $e(R_{i,1}|R_i)=q$. Let ρ be the number of places of M lying over $R_{i,1}$. Then $1 \le \rho \le q-1$, and all these places are centered at the same point. Therefore, there are as many as $q-1+\kappa+\rho$ places of M lying over (m_i). They form $\mathcal{W}_i$ which is an orbit under the action of $Gal(M|K)$. Since $Gal(M|K) \cong \mathrm{PGL}(2,q)$ and the 1-point stabilizer of $Gal(M|K)$ contains a subgroup of order q, the Dickson classification of subgroups [17, Theorem A.8] of $\mathrm{PGL}(2,q)$ yields that 1-point stabilizer has order $q(q-1)/r$ with $r \mid (q-1)$. Therefore $|\mathcal{W}_i|=(q+1)r$ whence $(q+1)r=q-1+\kappa+\rho$ follows. From this $r \le 2$. For $r=2$, the 1-point stabilizer of any subgroup of order $q-1$ has order $\frac{1}{2}(q-1)$. On the other hand, case $r=2$ may only occur when $\kappa+\rho=q+3$ and hence one of κ and ρ is equal to $q-1$ and the other is 4. Therefore, if $r=2$ then the subgroup of $Gal(M|K)$ of order $q-1$, namely $Gal(M|K(u,v))$, has an orbit of size 4 and hence its subgroup of order $\frac{1}{2}(q-1)$ cannot fix a place in $\mathcal{W}_i$. Thus $r=1$ and $|\mathcal{W}_i|=q+1$. In particular, $\kappa=\rho=1$.

7.1.2. Case $m_i \in \mathbb{F}_{q^2}$

This time, there exists just one place in $K(u,v)$ lying over $P_i=R_i$. Let T be a place of M lying over P_i in the covering $M|K$. From Result 6.1, the stabilizer of T in $Gal(M|K) \cong \mathrm{PGL}(2,q)$ is transitive on the set Δ of the $q+1$ roots of the polynomial (4), and hence its order is a multiple $r(q+1)$ of $q+1$. From the Dickson classification of subgroups of $\mathrm{PGL}(2,q)$, either $r=1$, or the stabilizer of T contains $PSL(2,q)$. The latter case cannot actually occur, since the p-subgroup of an automorphism group of any function field fixing a place is a normal subgroup. Thus the stabilizer of T in $Gal(M|K)$ is a cyclic group of order $q+1$, and hence $|\mathcal{W}_i|=q(q-1)$.

We are in a position to compute the genus $\mathfrak{g}(M)$. For $T \in \mathcal{W} = \cup_{i=1}^{q+1}\mathcal{W}_i$, let $G_T^{(k)}$ be the k-th ramification group of G at T; see [17, Section 11.9] and [24, Section III.8]. Since G_T is isomorphic to the 1-point stabilizer of $\mathrm{PGL}(2,q)$ in its action on the projective line, we have that G_T is a semidirect product of an elementary abelian normal subgroup S_q of order q by a cyclic complement of order $q-1$. Since the non-trivial elements in S_q form a unique conjugacy class in G_T, the non-trivial ramification groups with $k \geq 1$ coincide with S_q. Thus, for some positive integer $s = s_i$, $i = 1, 2, \ldots q+1$ depending only on $\mathcal{W}_i$, $S_q = G_T^{(1)} = \cdots = G_T^{(s_i)}$ and $G_T^{(k)} = \{1\}$ with $k > s_i$. Two cases are treated separately according as there is a tangent to $\mathcal{H}_q$ at a point in $\mathrm{PG}(2,q^2)$ which passes through $P(a,b)$, or is not.

7.1.3. $m_i \in \mathbb{F} \setminus \mathbb{F}_{q^2}$ for $i = 1, 2, \ldots, q+1$

From the Hurwitz genus formula [17, Theorem 11.72] applied to the Galois covering $M|K$,

$$2\mathfrak{g}(M) - 2 = -2|\mathrm{PGL}(2,q)| + \sum_{T\in\mathcal{W}}\sum_{k\geq 0}(|G_T^{(k)}| - 1) \tag{25a}$$

$$= -2(q^3-q) + \underbrace{(q+1)^2(q(q-1)-1)}_{\text{summation for } k=0} + \underbrace{(q+1)\sum_{i=1}^{q+1} s_i(q-1)}_{\text{summation for } k\geq 1} \tag{25b}$$

$$= q^4 - q^3 - 2q^2 - q - 1 + (q+1)(q-1)\sum_{i=1}^{q+1} s_i. \tag{25c}$$

Notice that if $m_0 \in \mathbb{F}$ is not a root of $Y^{q+1} + (Ya-b)^q + (Ya-b)$, and T is a place of M over (m_0), then the stabilizer G_T is trivial.

The subfield $K(u)$ is isomorphic to the hermitian function field H_q, and the extension $M|K(u)$ is Galois with Galois group $Gal(M|K(u))$ isomorphic to $\mathrm{AGL}(1,q)$. Since $\mathfrak{g}(H_q) = \frac{1}{2}q(q-1)$, the Hurwitz genus formula [17, Theorem 11.72] applied to the Galois cover $M|K(u)$ gives

$$2\mathfrak{g}(M) - 2 = |\mathrm{AGL}(1,q)|(q(q-1)-2) + \sum_{T\in\mathcal{W}}\sum_{k\geq 0}(|G_T^{(k)}| - 1) \tag{26a}$$

$$= q(q-1)(q(q-1)-2) \quad + \quad (q+1)(q(q-1)-1) \tag{26b}$$

$$+ \quad \sum_{i=1}^{q+1} s_i(q-1) \tag{26c}$$

$$+ \quad (q+1)q(q-2). \tag{26d}$$

$$= q^4 - 2q^2 - 2q - 1 \quad + \quad (q-1)\sum_{i=1}^{q+1} s_i \tag{26e}$$

In the second term of (26b), we sum for the (unique) place T over R_i with $k = 0$, $i = 1, \ldots, q+1$. In (26c), for the same place T with $k \geq 1$. In (26d), the summation is for the places T over P_i. There are q choices for T, G_T has order $q-1$, and $G_T^{(k)}$ is trivial for $k \geq 1$. If Q is a place of $K(u)$ different from P_i, R_i, and T is a place of M over Q, then G_T is trivial. This proves that the formula (26e) is correct.

Comparison of (25c) with (26e) yields $\sum_{i=1}^{q+1} s_i = q+1$. Since $s_i \geq 1$, this yields $s_1 = \ldots = s_{q+1} = 1$. Therefore,

$$2\mathfrak{g}(M) - 2 = (q+1)(q^3 - q - 2) = q^4 - q^2 - 2q - 2. \tag{27}$$

7.1.4. $m_i \in \mathbb{F} \setminus \mathbb{F}_{q^2}$ for $i = 1, 2, \ldots, q$ and $m_{q+1} \in \mathbb{F}_{q^2}$

The contribution of $\mathcal{W}_{q+1}$ in the Hurwitz genus formula equals $q^2(q-1)$. The above computation gives $\sum_{i=1}^{q} s_i = q$ and hence $s_i = 1$ for $i = 1, \ldots q$. Therefore,

$$\begin{cases} 2\mathfrak{g}(M) - 2 & = -2|PGL(2,q)| + \sum_{T \in \mathcal{W}} \sum_{k \geq 0} (|G_T^{(k)}| - 1) \\ & = -2(q^3 - q) + (q+1)q(q(q-1) - 1) + \sum_{i=1}^{q+1} s_i(q-1)) + q^2(q-1) \\ & = q^4 - 3q^2. \end{cases} \tag{28}$$

Theorem 7.2. *Let $k = q^{2r} + 1 \pm q^{r+1}(q-1)$ where $\pm$ is taken according as r is even or odd. In $\mathrm{PG}(2, q^{2r})$ with $r \geq 3$, let Ω be the $(k, q+1)$-arc consisting of all points of the Hermitian curve. If $r > 3$ then Ω is complete.*

Proof. We show that some long orbit of $Gal(M|K)$ consists of places defined over $\mathbb{F}_{q^{2r}}$. Since $Gal(M|K)$ has exactly $(q+1)$ short orbits, each of size $q+1$, M has as many as $(q+1)^2$ ramified places. By (27) and (28), the Hasse-Weil lower bound ensures at least $q^{2r} + 1 - q^r(q^4 - q^2 - 2q) = q^{2r} - q^{r+4} + q^{r+2} + 2q^{r+1}$ places of M defined over $\mathbb{F}_{q^{2r}}$. For $r > 3$, this number is larger than $(q+1)^2$. Therefore, as long as $r > 3$, M has a unramified place P_0 over $\mathbb{F}_{2r}$. Since $Gal(M|K)$ is defined over $\mathbb{F}_{q^{2r}}$ (Theorem 5.2 and Proposition 7.1), the long orbit of P_0 under the action of $Gal(M|K)$ is entirely consists of places defined over $\mathbb{F}_{q^{2r}}$. Therefore, the place m_0 of K lying under P_0 has the required property, that is, the roots of the polynomial $F(T) = T^{q+1} + m_0^q T^q + m_0 T - ((m_0 a - b)^q + m_0 a - b)$ are pairwise distinct and belong to $\mathbb{F}_{q^{2r}}$. □

7.2. The rational BKS case

Our goal is to show that Proposition 7.1 holds true for the rational BKS curve unless $P \in \mathrm{PG}(2, q)$. For this purpose, we proceed as in Section 7.1. First we prove the transitivity of the 1-point stabilizer of $Gal(f, K)$ on the remaining q points of Δ.

This time, the function field L to be investigated is

$$L = \mathbb{F}(m, u);\ 2mu^{q+1} + (2m-1)u^q + (2m-1)u + m(2-a) + b - 2.$$

The algebraic extension $L|K$ of degree $q+1$. For $a \neq 0$, let $m_i \in \mathbb{F}$ with $i = 1, 2$ be the roots of the polynomial $2aY^2 - 2bY + 1 \in \mathbb{F}[Y]$, i.e. $m_i = (b \pm \sqrt{b^2 - 2a})/(2a)$, and let ℓ_i be the line of equation $Y = m_i(X - a) + b$. For $a = 0$, let ℓ_1 be the line of equation $Y = \frac{1}{2}b^{-1}X + b$ and ℓ_2 be the line of equation $X = 0$. The results stated in Section 4.1 show that the tangents to $\mathcal{C}$ passing through the point $P(a, b)$ are exactly the lines ℓ_i. Furthermore, ℓ_i has exactly two common points with $\mathcal{C}$, namely the points P_i, Q_i where $I(P_i, \mathcal{C} \cap \ell_i) = 1$ and $I(Q_i, \mathcal{C} \cap \ell_i) = q$, unless $P_i = Q_i$ and $I(Q_i, \mathcal{C} \cap \ell_i) = q + 1$. In the latter exceptional case, $m_i \in \mathbb{F}_q$. If this occurs for $i = 1, 2$ then $P(a, b) \in \mathrm{PG}(2, q) \setminus \mathcal{C}$, i.e. $P(a, b)$ is an external point to $\mathcal{C}^2$ in $\mathrm{PG}(2, q)$. Dismissing this case allows us to assume that $I(P_1, \mathcal{C} \cap \ell_1) = 1$ and $I(Q_1, \mathcal{C} \cap \ell_1) = q$. Therefore we may argue as in Section 7.1 and prove that the 1-point stabilizer of $Gal(f, K)$ is transitive on the remaining q points of Δ. From this, $Gal(f, K)$ is a 2-transitive permutation group on Δ. More precisely, $Gal(f, K) \cong \mathrm{PGL}(2, q)$ and it acts on Δ as $\mathrm{PGL}(2, q)$ in its unique 3-transitive permutation representation on the projective line over $\mathbb{F}_q$.

Therefore, the following result is obtained.

Proposition 7.3. *Assume that $P(a, b) \notin \mathrm{PG}(2, q)$. Then the first Abhyankar's skew derivative $f_1(T)$ of $f(T)$ given in (20) is an irreducible polynomial over $K(u)$, and the irreducibility condition in Theorem 5.2 can be dropped.*

For $q = 11, r = 3$, Magma computation shows that the dismissed case, $P(a, b) \in \mathrm{PGL}(2, q)$ is a real exception for Proposition 7.3, as $Gal(f, K)$ has order $2(q+1)$ in that case.

From now on we assume $P(a, b) \notin \mathrm{PG}(2, q)$. For $i = 1, 2$, let $\mathcal{W}_i$ be the set of places of M lying over the place m_i of $K = \mathbb{F}(m) \cup \{\infty\}$. We distinguish two cases, called general and special, according as P_i and Q_i are distinct or coinciding.

For the general case, we may proceed as in Section 7.1.

Assume first that $m_1 \neq m_2$. In this case, $Gal(M|K)$ has exactly two short orbits on M, namely $\mathcal{W}_1$ and $\mathcal{W}_2$, both of size $q+1$, and the action of $Gal(M|K) \cong \mathrm{PGL}(2, q)$ on $\mathcal{W}_i$ is the same as on Δ. From the Hurwitz genus formula [17, Theorem 11.72] applied to the Galois covering $M|K$,

$$\begin{cases} 2\mathfrak{g}(M) - 2 &= -2|\mathrm{PGL}(2, q)| + \sum_{T \in \mathcal{W}} \sum_{i \geq 0} (|G_T^{(i)}| - 1) \\ &= -2(q^3 - q) + 2(q + 1)(q(q - 1) - 1 + s(q - 1)). \end{cases} \tag{29}$$

The subfield $K(u)$ of M is a Galois cover of M with Galois group $Gal(M|K(u)$ isomorphic to $\mathrm{AGL}(1, q)$. Since $K(u)$ is the function field of $\mathcal{C}$ which is a rational curve, we have $\mathfrak{g}(K(u)) = 0$, the Hurwitz genus formula [17, Theorem 11.72] applied to the Galois covering $M|K(u)$ gives

$$\begin{cases} 2\mathfrak{g}(M) - 2 &= -2|\mathrm{AGL}(1, q)| + \sum_{T \in \mathcal{W}} \sum_{i \geq 0} (|G_T^{(i)}| - 1) \\ &= -2q(q - 1) + 2[(q(q - 1) - 1 + s(q - 1) + q(q - 2)]. \end{cases} \tag{30}$$

Comparison of (29) with (30) yields $s = 1$ whence $2\mathfrak{g}(M) - 2 = 2q^2 - 2q - 4$ follows.

Assume now that $m_1 = m_2$. Then $\mathcal{W}_1 = \mathcal{W}_2$, and $\mathcal{W}_1$ is the only short orbit of $Gal(M|K)$ on M. The above computation gives

$$\begin{cases} 2\mathfrak{g}(M) - 2 &= -2|\mathrm{PGL}(2,q)| + \sum_{T\in\mathcal{W}} \sum_{i\geq 0} (|G_T^{(i)}| - 1) \\ &= -2(q^3 - q) + (q+1)(q(q-1) - 1 + s(q-1)). \end{cases} \tag{31}$$

and

$$\begin{cases} 2\mathfrak{g}(M) - 2 &= -2|\mathrm{AGL}(1,q)| + \sum_{T\in\mathcal{W}} \sum_{i\geq 0} (|G_T^{(i)}| - 1) \\ &= -2q(q-1) + (q(q-1) - 1 + s(q-1) + q(q-2). \end{cases} \tag{32}$$

From this, $s = q + 1$ follows. Therefore $2\mathfrak{g}(M) - 2 = q^2 - q - 2$.

In the special case, $m_1 \neq m_2$ with $m_1 \notin \mathbb{F}_q$, $m_2 \in \mathbb{F}_q$ and $P_1 \neq Q_1, P_2 = Q_2$. Let $\mathcal{W}_2$ be the set of the places of M lying over P_2. Since there exists a unique place of $K(u,v)$ lying over P_2, $[M : K] = |\mathrm{PGL}(2,q)| = q(q+1)(q-1)$ together with $K(u,v) : K] = q+1$ yield $|\mathcal{W}_2| \leq q(q-1)$. Therefore 1-point stabilizer G_1 of $Gal(M : K) \cong \mathrm{PGL}(2,q)$ in $\mathcal{W}_2$ has order at least $q+1$, say $\lambda(q+1)$ with a divisor λ of $q(q-1)$. Actually, $\lambda = 1$. In fact, G_1 is always solvable and its subgroups of order prime to p are cyclic, see [17, Lemma 11.44], hence the claim follows from [17, Theorem A.8] which is a corollary to the Dickson's classification of subgroups of $PSL(2,q)$. Therefore G_1 is a cyclic group of order $q+1$, and $|\mathcal{W}_2| = q(q-1)$. Thus $Gal(M|K)$ has two short orbits, namely $\mathcal{W}_1$ and $\mathcal{W}_2$ where $|\mathcal{W}_1| = q+1$ and $Gal(M|K)$ acts on $\mathcal{W}_1$ as its 3-transitive permutation representation on $\mathrm{PG}(1,q)$ whereas $\mathcal{W}_2| = q(q-1)$ and $Gal(M|K)$ acts on $\mathcal{W}_2$ as on the sets consisting of its cyclic subgroups of order $q+1$, and the action is by conjugacy. From the Hurwitz genus formula [17, Theorem 11.72] applied to the Galois cover $M|K$,

$$\begin{cases} 2\mathfrak{g}(M) - 2 &= -2|\mathrm{PGL}(2,q)| + \sum_{T\in\mathcal{W}} \sum_{i\geq 0} (|G_T^{(i)}| - 1) \\ &= -2(q^3 - q) + (q+1)(q(q-1) - 1 + s(q-1)) + q^2(q-1). \end{cases} \tag{33}$$

and

$$\begin{cases} 2\mathfrak{g}(M) - 2 &= -2|\mathrm{AGL}(1,q)| + \sum_{T\in\mathcal{W}} \sum_{i\geq 0} (|G_T^{(i)}| - 1) \\ &= -2q(q-1) + (q(q-1) - 1 + s(q-1) + q(q-2). \end{cases} \tag{34}$$

This is only possible for $s = 1$. Therefore $2\mathfrak{g}(M) - 2 = 0$, and hence $\mathfrak{g}(M) = 0$.

Thus the following claim is proven.

Lemma 7.4. *In the general case, either* $\mathfrak{g}(M) = q^2 - q - 1$, *or* $\mathfrak{g}(M) = \frac{1}{2}(q^2 - q)$ *according as* $m_1 \neq m_2$, *or* $m_1 = m_2$. *In the special case,* M *is a rational function field.*

We are in a position to prove the following theorem.

Theorem 7.5. *Let $k = q^3+1-\frac{1}{2}q(q-1)$. In $\mathrm{PG}(2,q^r)$ with $r \geq 5$, let Ω be the $(k,q+1)$-arc consisting of all points of the rational BKS curve. For even r, Ω is complete. If r is odd then the points which are uncovered by the $(q+1)$-secants to Ω are exactly the points in $\mathrm{PG}(2,q)$ not lying in Ω. Adding those points to Ω produces a complete $(k,q+1)$-arc in $\mathrm{PG}(2,q^r)$, r odd, with $k = q^3+q+1$.*

Proof. The Čebotarev type argument in the proof of Theorem 7.2 in Section 7.1 can be used to deal with both the general and special cases.

In the general case, if $m_1 \neq m_2$, the Hasse-Weil lower bound [17, Theorem 9.18] ensures at least $q^r + 1 - 2q^{r/2}(q^2-q-1) = q^r - 2q^{r/2+2} + 2q^{r/2+1} + 2q^{r/2}$ places of M defined over $\mathbb{F}_{q^r}$. For $r > 3$, this number is larger than $(q+1)+q(q-1) = q^2+1$ which is the number of ramified places of M under the action of $Gal(M|K)$. Therefore, as long as $r \geq 5$, M has a unramified place P_0 over $\mathbb{F}_{2r}$. From this, as in the proof of Theorem 7.2, the claim follows. If $m_1 = m_2$, the same computation with the Hasse-Weil lower bound proves the existence of a unramified place of M defined over $\mathbb{F}_{q^r}$ as far as $q^r + 1 - q^{r/2+2} - q^{r/2+1} - (q+1) > 0$, i.e. $q \geq 5$.

In the special case, M is rational and hence it has exactly q^r+1 places. Furthermore, $(q+1)+q^2-q = q^2+1$ is the number of the places of M which are ramified under the action of $Gal(G|K)$. Therefore, for $r \geq 3$, M has a unramified place over $\mathbb{F}_r$ and the claim can be proven as in the general cases.

We are left with the case where $m_1, m_2 \in \mathbb{F}_q$ and $P(a,b) \in \mathrm{PG}(2,q) \setminus \Omega$. As mentioned in Section 4.2, a linear automorphism group $G \cong \mathrm{PGL}(2,q)$ of $\mathrm{PG}(2,q)$ leaves $\mathcal{C}$ invariant and acts transitively on the external points to $\mathcal{C}$ in $\mathrm{PG}(2,q)$. Moreover, the line at infinity meets $\mathcal{C}$ only in $X_\infty = (1:0:0)$. Therefore, we may assume that P is the point at infinity $Y_\infty = (0:1:0)$ so that the line at infinity is not a $(q+1)$-secant to Ω. We show that Y_∞ is covered by a $(q+1)$-secant to Ω in $\mathrm{PG}(2,q^r)$ if and only if r is even. Let $P \in \mathrm{PG}(2,q^r)$ be a point of $\mathcal{C}$ with parameter $t_1 \in \mathbb{F}_{q^r}$. Then the vertical line through P meets $\mathcal{C}$ in the points P_i with parameters t_i such that $(t_i+1)^{q+1} = (\tau+1)^{q+1}$. Then $t+1 = \lambda(\tau+1)$ with $\lambda^{q+1} = 1$. Therefore, $P_i \in \mathrm{PG}(2,q^r)$ for $i = 1,2,\ldots,q+1$ if and only if $q+1$ divides q^r-1 whence the claim follows. □

8. Case $P \in \Omega$

We keep our notation from Sections 5.2 and 5.2.2. As in Section 7, our first step is to show if the irreducibility condition in Theorems 5.5 and 5.9 is fulfilled. For this purpose, it is sufficient the 2-transitivity of $Gal(g,K)$ one the set $\Delta = \{\alpha_1,\ldots,\alpha_q\}$ of the roots of the polynomial $g(T)$. Since $Gal(g,K)$ is transitive by Lemmas 5.4 and 5.8, we may limit ourselves to investigate whether the 1-point stabilizer of $Gal(g,K)$ is transitive.

8.1. Hermitian case

We may assume that $P \notin \mathrm{PG}(2,q^2)$. From Section 4.1, P is incident with two tangent lines to $\mathcal{H}_q$, say ℓ_{m_1} and ℓ_{m_2} where P is the tangency point of ℓ_{m_1} while ℓ_{m_2} is tangent to $\mathcal{H}_q$ at the point R whose Frobenius image is P, i.e. $R = R(\alpha,\beta)$ with $\alpha^{q^2} = a, \beta^{q^2} = b$. Moreover, ℓ_1 meets $\mathcal{H}_q$ in another point P' which is the Frobenius image of P. Since $P = P(a,b)$, we have $a^q + m_1 = 0$ and $a + m_2^q = 0$.

Therefore, exactly two places of $K(u)$ lie over m_1. They are identified by $P_1 = (m_1, 0)$ and $P_2 = (m_1, -(a+m_1^q))$ where $e(P_1|m_1) = q-1$ and $e(P_2|m_1) = 1$. Instead, there exists just one place of $K(u)$ lying over m_2 identified by $R_1 = (m_2, -\sqrt[q]{a^q + m_2})$ where $e(R_1|m_2) = q$. Furthermore, there are $(q-1)$ places of M over P_1 identified by $T_{1,i} = (m_1, 0, v_1^i)$ where v_1 is a primitive $(q-1)$-st root of unity. Also, there exists a unique place of M lying over P_2 identified by $T_2 = (m_1, -(a+m_1^q), 0)$, and unique place over R identified by $T_3 = (m_2, -\sqrt[q]{a^q + m_2}, \infty)$.

From Result 6.1, the inertia group $I(T_2|m_1)$ has two orbits on the set Δ of the roots of $g(T)$, one of size $q-1$ and another of size 1. Therefore, $I(T_1|m_1)$ as a subgroup of $Gal(g,K)$ acting on Δ fixes a point and transitive on the remaining points. Thus $Gal(g,K)$ is 2-transitive on Δ. Therefore $g_1(T)$ is irreducible over K and $Gal(M|K)$ acts on Δ as a sharply 2-transitive permutation group (of order $q(q-1)$).

Let $\mathcal{W}_1 = \{T_{1,i}, T_2 | i = 0, 1 \ldots, q-2\}$ and $\mathcal{W}_2 = \{T_3\}$. Then $\mathcal{W}_1$ and $\mathcal{W}_2$ are the only short orbits of $Gal(M|K)$. Since $Gal(M|K) \cong \mathrm{AGL}(1,q)$, $Gal(M|K)$ has a cyclic subgroup Λ of order $q-1$ that fixes a root of $g(T)$. We may assume that u is that root. Then the fixed field of Λ is $K(u) = \mathbb{F}(m,u)$. As we have shown, $\mathbb{F}(m,u)$ has a non-singular plane model of degree q, and hence $\mathfrak{g}(K(u)) = \frac{1}{2}q(q-1)$. Furthermore, Λ has exactly two fixed places, namely T_2 and T_3. From the Hurwitz genus formula [17, Theorem 11.72] applied to the Galois covering $M|K(u)$,

$$2\mathfrak{g}(M) - 2 = (q-1)(q(q-1-2) + 2(q-2) = q(q-1)^2 - 2. \tag{35}$$

Now, if

$$q^{2r} + 1 > 2\mathfrak{g}q^r + q + 1 > q^{r+3} - 2q^{r+2} + q^{r+1} + q + 1,$$

then the Hasse-Weil lower bound yields that P lies on a $(q+1)$-secant to Ω. In fact, the arguments in the proof of Theorem 7.2 also work for this case and provide a proof for the following result.

Theorem 8.1. *Let $k = q^{2r} + 1 \pm q^{r+1}(q-1)$ where $\pm$ is taken according as r is even or odd. In $\mathrm{PG}(2,q^{2r})$ with $r \geq 3$, let Ω be the $(k, q+1)$-arc consisting of all points of the Hermitian curve. If $r > 3$ then each point of Ω is covered by some $(q+1)$-secant to Ω.*

For $r = 3$, the results stated in Section 6.3 are sufficient to determine the number n_P of $(q+1)$-secants to $\mathcal{H}_q$ through any point $P \in PG(2,q^6) \setminus \mathrm{PG}(2,q^2)$ lying in $\mathcal{H}_q$. We may

assume $\mathcal{H}_q$ in its canonical form $X^q + T^q X + T = 0$ over $\mathbb{F}_{q^6}$. Since the automorphism group of $\mathcal{H}_q$ has two orbits in $PG(2, q^6)$, one consisting of its points in $PG(2, q^2)$, we may also assume $P = X_\infty$. As the Galois closure M is a maximal curve of genus $\frac{1}{2}q(q-1)^2$, it has as many as $q^6 + 1 + q(q-1)^2 q^3$ points in $PG(2, q^6)$. Moreover, the Galois extension $M|L(u)$ has degree $q(q-1)$ where $L(u)$ is the function field of $\mathcal{H}_q$. Therefore, $n_P q(q-1) = q^6 + 1 + q(q-1)^2 q^3 - (q+1)^2$ whence $n_P = 2q^4 + q^2 + q + 1$ follows. A direct proof based on norms and traces in finite fields is also possible. This was pointed out by B. Csajbók [12].

8.2. The rational BKS case

We begin with case $P \notin \mathrm{PG}(2, q)$. From Section 4.2, P is incident with two tangent lines to $\mathcal{C}$, say ℓ_{m_1} and ℓ_{m_2} where P is the tangency point of ℓ_{m_1} while ℓ_{m_2} is tangent to $\mathcal{C}$ at the point R whose Frobenius image is P. As in Section 5.2, we replace $2m/(1-2m)$ by m so that we may use equation (19). Then, if P has parameter $t \in \mathbb{F}$, then the tangent line ℓ_1 at P has slope $-t^q$ and meets $\mathcal{C}$ in another point, namely that with parameter t^q.

Thus, exactly two places of $K(u)$ lie over t. They are identified by $P_1 = (-t^q, 0)$ and $P_2 = (-t^q, t^q - t)$. Moreover, there exists just one place over $-t$ identified by $R_1 = (-t, \sqrt[q]{t - t^q})$. Furthermore, there are $(q-1)$ places of M over P_1 identified by $T_{1,i} = (-t^q, 0, -v_1^i)$ where v_1 is a primitive $(q-1)$-st root of unity. Also, there exists a unique place of M lying over P_2 identified by $T_2 = (-t^q, t^q - t, 0)$, and unique place over R identified by $T_3 = (-t, -\sqrt[q]{t - t^q}, \infty)$. This ramification picture is analog of that in Section 8. In particular, Result 6.1 yields that the inertia group $I(T_2|-t)$ has two orbits on the set Δ of the roots of $g(T)$, one of size $q-1$ and another of size 1. Therefore, $I(T_1|-t)$ as a subgroup of $Gal(g, K)$ acting on Δ fixes a point and transitive on the remaining points. Thus $Gal(M|K)$ is 2-transitive and $g_1(T)$ is irreducible over K. More precisely, $Gal(g, K)$ acts on Δ as a sharply 2-transitive permutation group (of order $q(q-1)$). As in Section 8, we introduce $\mathcal{W}_1, \mathcal{W}_2, \Lambda$ and u. This time the fixed field of Λ, that is, $\mathbb{F}(m, u)$ given in (23) which a rational curve. From the Hurwitz genus formula [17, Theorem 11.72] applied to the Galois covering $M|K(u)$,

$$2\mathfrak{g}(M) - 2 = -2(q+1) + 2(q-2) = -2. \tag{36}$$

Thus M is a rational function field, and hence it has exactly $q^r + 1$ places over $\mathbb{F}_q$. Therefore, the number of long orbits of $Gal(M|K)$ defined over $\mathbb{F}_{q^r}$ is equal to $(q^r + 1 - (q+1))/(q(q-1)) = 1 + q + \ldots + q^{r-2}$.

Now, suppose that $P \in \mathrm{PG}(2, q)$. If P is an internal point to $\mathcal{C}^2$ then P is a singular point. Clearly, no singular point of $\mathcal{C}$ is covered by a $(q+1)$-secant to $\mathcal{C}$ as $\deg(\mathcal{C}) = q+1$. Therefore, we are left with the case where $P \in \mathcal{C}^2$. As mentioned in Section 4.2, a linear automorphism group $G \cong \mathrm{PGL}(2, q)$ of $\mathrm{PG}(2, q)$ leaves $\mathcal{C}$ invariant and acts transitively on the points of $\mathcal{C}^2$ in $\mathrm{PG}(2, q)$ Therefore, we may assume $P = X_\infty(1:0:0)$. Take point $R \in \mathcal{C}$ with parameter $t_0 \in \mathbb{F}_{q^r} \setminus \mathbb{F}_{q^2}$. The horizontal line ℓ through R meets $\mathcal{C}$ in the

points with parameters t such that $t^q+t+2 = t_0^q+t_0 = 2$, that is, $(t-t_0)^q+(t-t_0) = 0$. Then $t = t_0+\tau$ with $\tau \in \mathbb{F}_q$. Hence $t \in \mathbb{F}_{q^r} \setminus \mathbb{F}_{q^2}$. Thus the common points of ℓ and $\mathcal{C}$ are pairwise distinct and each lies in $\mathrm{PG}(2,q^r)$.

Therefore the following result is obtained.

Theorem 8.2. *Let $k = q^3+1-\frac{1}{2}q(q-1)$. In $\mathrm{PG}(2,q^r)$ with $r \geq 3$, let Ω be the $(k,q+1)$-arc consisting of all points of the rational BKS curve. Then the points of Ω uncovered by the $(q+1)$-secants to Ω are exactly the points of $\mathrm{PG}(2,q)$ lying in Ω.*

CRediT authorship contribution statement

All authors have participated in (a) conception and design, or analysis and interpretation of the data; (b) drafting the article or revising it critically for important intellectual content; and (c) approval of the final version.

Declaration of competing interest

This manuscript has not been submitted to, nor is under review at, another journal or other publishing venue.

The authors have no affiliation with any organization with a direct or indirect financial interest in the subject matter discussed in the manuscript

Data availability

No data was used for the research described in the article.

Acknowledgment

The research was supported by the Hungarian Academy of Sciences "MTA Vendégkutatói Program 2022", the NKFIH-OTKA Grants SNN 132625, K 124950, and the Program of Excellence TKP2021-NVA-02 at the Budapest University of Technology and Economics. The third author was partially supported by the Slovenian Research Agency, research project J1-9110.

The authors thank the anonymous referee whose advices enhanced the clarity and accuracy of the paper.

References

[1] S.S. Abhyankar, Galois theory on the line in nonzero characteristic, Bull. Am. Math. Soc. 27 (1992) 68–133.
[2] S. Alabdullah, J.W.P. Hirschfeld, A new lower bound for the smallest complete (k,n)-arc in $\mathrm{PG}(2,q)$, Des. Codes Cryptogr. 87 (2019) 679–683.
[3] Y. Aubry, A. Issa, F. Herbaut, Polynomials with maximal differential uniformity and the exceptional APN conjecture, J. Algebra 635 (2023) 822–837.

[4] Y. Aubry, F. Herbaut, J.F. Voloch, Maximal differential uniformity polynomials, Acta Arith. 188 (2019) 345–366.
[5] Y. Aubry, F. Herbaut, Differential uniformity and second order derivatives for generic polynomials, J. Pure Appl. Algebra 222 (2018) 1095–1110.
[6] D. Bartoli, G. Micheli, Algebraic constructions of complete m-arcs, Combinatorica 42 (2022) 673–700.
[7] S. Ball, A. Blokhuis, F. Mazzocca, Maximal arcs in Desarguesian planes of odd order do not exist, Combinatorica 17 (1997) 31–41.
[8] H. Borges, On complete (N, d)-arcs derived from plane curves, Finite Fields Appl. 15 (2009) 82–96.
[9] H. Borges, G. Korchmáros, P. Speziali, Plane curves with a large linear automorphism group in characteristic p, arXiv:2202.05765 [math.AG].
[10] H. Borges, B. Motta Beatriz, F. Torres, Complete arcs arising from a generalization of the Hermitian curve, Acta Arith. 164 (2014) 101–118.
[11] A.W. Bluher, On $x^{q+1} + ax + b$, Finite Fields Appl. 10 (2004) 285–305.
[12] B. Csajbók, Private communication, 2022.
[13] M. Giulietti, On plane arcs contained in cubic curves, Finite Fields Appl. 8 (2002) 69–90.
[14] M. Giulietti, F. Pambianco, F. Torres, E. Ughi, On complete arcs arising from plane curves, Des. Codes Cryptogr. 25 (2002) 237–246.
[15] R.M. Guralnick, T.J. Tucker, M.E. Zieve, Exceptional covers and bijections on rational points, Int. Math. Res. Not. 2007 (2007) rnm004.
[16] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, second edition, Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1998.
[17] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic Curves over a Finite Field, Princeton University Press, Princeton, N.J., 2008, xviii+696 pp., Int. J. Algebra 1 (2007) 563–585.
[18] K.H. Kim, J. Choe, Sihem Mesnager, Solving $X^{q+1} + X + a = 0$ over finite fields, Finite Fields Appl. 70 (2021) 101797.
[19] K.H. Kim, J. Choe, Sihem Mesnager, Complete solution over $\mathbb{F}_{p^n}$ of the equation $X^{p^k+1}+X+a = 0$, Finite Fields Appl. 76 (2021) 101902.
[20] K.H. Kim, Sihem Mesnager, Solving $x^{2^k+1} + x + a = 0$ in $\mathbb{F}_{2^n}$ with $gcd(n, k) = 1$, Finite Fields Appl. 63 (2020) 101630.
[21] M. Rosen, Number Theory in Function Fields, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002, xii+358 pp.
[22] B. Segre, U. Bartocci, Ovali ed altre curve nei piani di Galois di caratteristica due, Acta Arith. 18 (1971) 423–449.
[23] J.-P. Serre, Local Fields, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979.
[24] H. Stichtenoth, Algebraic Function Fields and Codes, Springer, Berlin, 1993, x+260 pp.
[25] T. Szőnyi, Small complete arcs in Galois planes, Geom. Dedic. 18 (1985) 161–172.
[26] S. Tafazolian, F. Torres, The curve $y^n = x^\ell(x^m + 1)$ over finite fields II, Adv. Geom. 21 (2021) 385–390.
[27] B.L. van der Waerden, Die Zerlegungs- und Trägheitsgruppe als Permutationsgruppen, Math. Ann. 111 (1935) 731–733.
[28] H. Zassenhaus, Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen, Abh. Math. Semin. Univ. Hamb. 11 (1936) 17–40.