Journal of Algebra 638 (2024) 238–254

Contents lists available at ScienceDirect

Journal of Algebra

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

On complete m-arcs ☆

Luca Bastioni, Giacomo Micheli *

Department of Mathematics and Statistics, University of South Florida, 4202 E Fowler Ave, Tampa, 33620, FL, USA

ARTICLE INFO

Article history:
Received 8 April 2023
Available online 10 October 2023
Communicated by William M. Kantor

MSC:
05B25
51E21
11R45
51E20
11T06

Keywords:
Complete arcs
Curves over finite fields
Density theorems
Polynomials over finite fields

ABSTRACT

Let m be a positive integer and q be a prime power. For large finite base fields $\mathbb{F}_q$, we show that any plane curve can be used to produce a complete m-arc as long as some generic explicit geometric conditions on the curve are verified. To show the effectiveness of our theory, we derive complete m-arcs from hyperelliptic curves and from Artin-Schreier curves.

1. Introduction

Let q be a prime power and $\mathbb{F}_q$ be the finite field of order q. Let $\mathbb{P}^2(\mathbb{F}_q) = \mathrm{PG}(2, q)$ be the set of $\mathbb{F}_q$-points $[X_0, X_1, X_2]$ of the projective plane. Let $\mathrm{AG}(2, q)$ be the set of $\mathbb{F}_q$ points of the affine plane, which we will identify with the projective points of $\mathbb{P}^2(\mathbb{F}_q)$

☆ This work was supported by the National Science Foundation under Grant No 2127742.
* Corresponding author.
E-mail addresses: lbastioni@usf.edu (L. Bastioni), gmicheli@usf.edu (G. Micheli).

https://doi.org/10.1016/j.jalgebra.2023.09.027
0021-8693/

with $X_2 \neq 0$. A (k, m)-*arc* $\mathcal{A}$ in $\mathbb{P}^2(\mathbb{F}_q)$ is a set of k points such that there are no $m+1$ points that are collinear and such that there exist m collinear points. For fixed m, q, we have that the set $\mathcal{A}_m(q)$ of all m-arcs in $\mathbb{P}^2(\mathbb{F}_q)$ is partially ordered by inclusion. A *complete* m-arc is a maximal element in $\mathcal{A}_m(q)$, i.e. it is an m-arc that is not contained in a strictly larger m-arc.

In the late 50's, Segre introduced the notion of arc for $m = 2$, which has been extensively studied in the literature (Segre was in fact interested to know how many points a complete arc in $\mathbb{P}^2(\mathbb{F}_q)$ can have, see [25]). In this simpler case $m = 2$, the theory is well developed and there are plenty for constructions (see for example [1–3,12,13,15,31,32]). For maximum size arcs in odd characteristic, Segre himself proved that the set of points of an arc is a conic.

Concerning minimal sizes, much less is known. Using a probabilistic method, the paper [17] shows that there exists a complete arc of size $O(\sqrt{q}\log^c q)$ in a projective plane of order $q > M$ (for some positive constants c, M independent on q). Another clever idea to construct arcs (due to Segre and Lombardo-Radice [21,26]) is to use a small set of $\mathbb{F}_q$-rational points of a curve of low degree over a finite field. A lot of research has been done in this direction [19,35,36,24,30,8] and the currently best known bound using this method gives $O(q^{3/4})$.

The case $m > 2$ is much more complex and the currently known constructions either use the theory of 2-character sets (see [13, Sects. 12.2 and 12.3] and [10]) or connections with certain special family of curves [9,16,34,5]. For $m = 3$ and $m = 4$ [4,7] construct small complete m-arcs of size $o(q)$ using subsets of the $\mathbb{F}_q$-rational points of a curve of degree $m + 1$. In [6] the authors construct a family of curves that gives rise to m-arcs of size smaller than q over certain subsequence of extension fields for all $m > 8$. In fact, the authors show that they can determine a curve and construct a sequence of positive integers n_k such that the set of $\mathbb{F}_{q^{n_k}}$-rational points of $\mathcal{C}$ gives rise to an m-arc of size roughly $q^{n_k} - C\sqrt{q^{n_k}}$ for an explicit C. Using a similar Galois theoretical approach as [6], in [18] the authors were able to construct complete m-arcs using the Hermitian curve of degree $q + 1$ and the BKS curve of degree $q + 1$.

The purpose of this paper is to provide a general theory to construct families of complete m-arcs arising from curves that satisfy explicit and easily verifiable generic conditions. As a proof of concept, we employ our methods in the case of hyperelliptic curves and Artin-Schreier curves, showing that they can be used to construct complete m-arcs.

Apart from their fundamental interest in combinatorics, complete m-arcs of size k have an important connection with coding theory, as they correspond to codes over $\mathbb{F}_q$ of length k, dimension 3 and distance $k - m$ (in the coding theoretical notation, $[k, 3, k - m]_q$-codes) that cannot be extended to a code with same dimension and larger minimum distance. In fact, given an m-arc A, one can place as columns of a $3 \times k$ matrix G representatives in $\mathbb{F}_q^3$ of the points of the m-arc. Let $\mathcal{C}$ be the code generated by G. Now, for every $x \in \mathbb{F}_q^3$, the codeword xG has weight at least $k - m$ or otherwise one could find $m + 1$ collinear points in A.

A general introduction to (k, m)-arcs can be found in the monograph [13, Chapter 12], as well as in the survey paper [15, Section 5].

1.1. Outline of the paper

We first provide an introduction to the basic techniques and notations that we use in the paper (Subsection 1.2 and Section 2). Firstly, we describe the auxiliary results that we will use to convert geometric properties into the arithmetic ones (Section 3). Then, we provide the main result (Section 4). Finally, to show the effectiveness of our results, we give two applications (Section 5) to hyperelliptic and Artin-Schreier curves.

1.2. Notation

Let x be a transcendental element over $\mathbb{F}_q$ and $\mathbb{F}_q(x)$ be the rational function field in the variable x. For a curve $\mathcal{C}$ we denote by $\mathcal{C}(\mathbb{F}_q)$ the set of $\mathbb{F}_q$-rational points of $\mathcal{C}$, and by $\mathbb{F}_q(\mathcal{C})$ its function field over $\mathbb{F}_q$. For a polynomial $F(X_0, \dots, X_n)$ we denote by $\deg(F)$ the total degree of F, whereas $\deg_{X_i}(F)$ denotes the maximal degree of X_i occurring in F. In the following we denote by $\mathbb{P}^2(\mathbb{F}_q)$ the set of $\mathbb{F}_q$-rational points of the projective plane $\mathbb{P}^2$ over $\mathbb{F}_q$, and with $\mathbb{A}^2(\mathbb{F}_q) = \mathbb{P}^2(\mathbb{F}_q) \setminus \ell_\infty$ the $\mathbb{F}_q$-rational points of the affine plane $\mathbb{A}^2$, where ℓ_∞ is the line at infinity $[X_0, X_1, 0]$.

Let $F = F(X_0, X_1, X_2) = 0$ be the homogeneous equation of an irreducible curve $\mathcal{C}$ of degree n in $\mathbb{P}^2$. For $i \in \{1, 2, 3\}$ let $F_i = \frac{\partial}{\partial X_i} F(X_0, X_1, X_2)$ be the partial derivative of F with respect the i-th variable. Then the dual curve $\mathcal{C}^*$ of $\mathcal{C}$ is defined as the closure of the image of the Gauss map

$$\begin{aligned} \mathcal{G} : \mathcal{C} &\to \mathbb{P}^2 \\ (X_0, X_1, X_2) &\mapsto (F_0(X_0, X_1, X_2), F_1(X_0, X_1, X_2), F_2(X_0, X_1, X_2)). \end{aligned}$$

For an irreducible plane curve $\mathcal{C}$, let $g(x, y) = 0$ be its affine equation. We say that $\mathbb{F}_q(\mathcal{C})$ is isomorphic to $\mathbb{F}_q(\mathcal{C}^*)$ via $\mathcal{G}$, and write $\mathbb{F}_q(\mathcal{C}) \cong_{\mathcal{G}} \mathbb{F}_q(\mathcal{C}^*)$, if

$$\mathbb{F}_q(x, y) = \mathbb{F}_q\left(\frac{\partial_x g(x, y)}{\partial_y g(x, y)}, x\frac{\partial_x g(x, y)}{\partial_y g(x, y)} + y\right). \tag{1}$$

Since $\mathcal{C}$ is an irreducible plane curve, we have that $\mathcal{C}^*$ is also plane and irreducible. Observe that $\mathcal{G}(\mathcal{C})$ is closed when $\mathcal{C}$ is non-singular.

2. Background

2.1. Arcs

A (k, m)-arc $\mathcal{A}$ in $\mathbb{P}^2(\mathbb{F}_q)$ is a set of k points no $m + 1$ of which are collinear and such that there exist m collinear points. The arc $\mathcal{A}$ is called a *complete* (k, m)-arc if it

is maximal with respect to the set theoretical inclusion among all m-arcs. In particular, every point in the complement of a complete m-arc $\mathcal{A}$ is collinear with m points in $\mathcal{A}$.

2.2. Rational maps between curves

We recall in this part some facts about rational maps and birational morphisms. For a complete exposition of the theory see for example [27–29].

Let $\mathbb{K}$ be an algebraically closed field and $\mathcal{V} \subset \mathbb{P}^n(\mathbb{K})$ a projective variety, i.e. an irreducible algebraic set of zeros in $\mathbb{K}$ of homogeneous polynomials with coefficients in $\mathbb{K}$. In the notation of this paper, an algebraic curve is simply a projective variety of dimension one. Let $\mathbb{K}(\mathcal{V})$ (resp. $\mathbb{K}[\mathcal{V}]$) denote the function field (resp. the homogeneous coordinate ring) of $\mathcal{V}$. A rational function $\varphi \in \mathbb{K}(\mathcal{V})$ is called *regular* at $x \in \mathcal{V}$ if it can be written as $\varphi = \frac{f}{g}$ where $f, g \in \mathbb{K}[\mathcal{V}]$ and $g(x) \neq 0$. The value of φ at the point x is $\frac{f(x)}{g(x)}$ and it is denoted by $\varphi(x)$. A rational function that is regular at every $x \in \mathcal{V}$ is called *regular function*.

Let $\mathcal{W} \subset \mathbb{P}^m(\mathbb{K})$ a projective variety. A *rational map* $\varphi : \mathcal{V} \dashrightarrow \mathcal{W}$ is a m-tuple of $\varphi_0, \dots, \varphi_m \in \mathbb{K}(\mathcal{V})$ such that $\varphi(x) = [\varphi_0(x), \dots, \varphi_m(x)] \in \mathcal{W}$ for all points $x \in \mathcal{V}$ at which all the φ_i are regular. The rational map φ is said to be *regular* at the points $x \in \mathcal{V}$ where it is defined. A rational map that is regular at every point $x \in \mathcal{V}$ is called a *morphism*.

The following result states that, for a non-singular curve $\mathcal{C}$ a rational map is defined at every point (see [28, Proposition 2.1]).

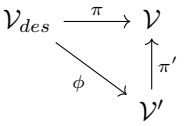
Proposition 2.1. *Let $\mathcal{C}$ be an algebraic curve and $\mathcal{W} \subset \mathbb{P}^m$ be a variety. Let $P \in \mathcal{C}$ be a non-singular point and let $\varphi : \mathcal{C} \dashrightarrow \mathcal{W}$ be a rational map. Then φ is regular at P. In particular, if $\mathcal{C}$ is non-singular, then φ is a morphism.*

A morphism $\varphi : \mathcal{V} \to \mathcal{W}$ is said to be an *isomorphism* if there exists a morphism $\psi : \mathcal{W} \to \mathcal{V}$ such that $\varphi \circ \psi$ and $\psi \circ \varphi$ are the identity maps on $\mathcal{W}$ and $\mathcal{V}$ respectively. Two varieties $\mathcal{V}$ and $\mathcal{W}$ are said to be *birationally equivalent* (or just *birational*) if there exist rational maps $\varphi : \mathcal{V} \dashrightarrow \mathcal{W}$ and $\psi : \mathcal{W} \dashrightarrow \mathcal{V}$ such that $\varphi \circ \psi$ and $\psi \circ \varphi$ are the identity maps on the points of $\mathcal{W}$ and $\mathcal{V}$ where they are defined. Each rational map φ and ψ is called a *birational equivalence*. If two varieties are isomorphic they are birationally equivalent, but the converse is generally not true.

Remark 2.2. If $\varphi : \mathcal{V} \dashrightarrow \mathcal{W}$ is a birational equivalence, then φ is a 1-to-1 correspondence everywhere except at non-regular points of $\mathcal{V}$ and $\mathcal{W}$. Therefore, as a consequence of Proposition 2.1, if $\mathcal{C}$ is a non-singular curve, then $\varphi : \mathcal{C} \dashrightarrow \mathcal{W}$ is defined everywhere on $\mathcal{C}$, and 1-to-1 only at *regular* points of $\mathcal{W}$. This means that in the particular case when $\mathcal{W}$ is a curve too, we have that ϕ is defined everywhere on $\mathcal{C}$, and 1-to-1 only at *non-singular* points of $\mathcal{W}$.

2.3. Non-singular model of a curve

For the results in this subsection we refer to [29, Appendix B]. Let $\mathcal{V}$ be a projective curve. Then there exists a non-singular projective curve $\mathcal{V}_{des}$ and a birational morphism $\pi : \mathcal{V}_{des} \to \mathcal{V}$ that satisfies the following universal property: if $\mathcal{V}'$ is another non-singular projective curve, and $\pi' : \mathcal{V}' \to \mathcal{V}$ is a birational morphism, then there exists a unique isomorphism $\phi : \mathcal{V}_{des} \to \mathcal{V}'$ such that $\pi = \pi' \circ \phi$. This is to say that the following diagram commutes



The pair $(\mathcal{V}_{des}, \pi)$, or simpler just $\mathcal{V}_{des}$, is called the non-singular model of $\mathcal{V}$.

2.4. Galois theory over global fields

In this section we use the notation and terminology of [29]. For a field M we denote by $\mathrm{Aut}(M)$ the automorphism group of M. Let $L \supseteq K$ be a separable field extension and let M be the Galois closure. We denote by $\mathrm{Gal}(M : K)$ the Galois group of $M : K$, i.e. $\{g \in \mathrm{Aut}(M) : \ g(x) = x \ \forall x \in K\}$. The next result is a consequence of [37, Satz 1].

Lemma 2.3 *(Orbits' lemma). Let $L : K$ be a finite separable extension of function fields, let M be its Galois closure and $G := \mathrm{Gal}(M : K)$ be its Galois group. Let P be a place of K and $\mathcal{Q}$ be the set of places of L lying above P. Let R be a place of M lying above P. Then we have the following:*

1) *There is a natural bijection between $\mathcal{Q}$ and the set of orbits of $H := \mathrm{Hom}_K(L, M)$ under the action of the decomposition group $D(R|P) = \{g \in G \mid g(R) = R\}$.*
2) *Let $Q \in \mathcal{Q}$ and let H_Q be the orbit of $D(R|P)$ corresponding to Q. Then $|H_Q| = e(Q|P)f(Q|P)$ where $e(Q|P)$ and $f(Q|P)$ are the ramification index and relative degree, respectively.*
3) *The orbit H_Q partitions further under the action of the inertia group $I(R|P) = \{g \in D(R|P) \mid v_R(g(s) - s) \geq 1 \ \forall s \in \mathcal{O}_R\}$ into $f(Q|P)$ orbits of size $e(Q|P)$.*

The next result gives a characterization of the Galois group using the inertia groups. For a reference see for example [29].

Lemma 2.4. *Let $L : K$ be a finite separable extension of function fields, let M be its Galois closure and let $G := \mathrm{Gal}(\bar{\mathbb{F}}_q M : \bar{\mathbb{F}}_q K)$. Then G is generated by the inertia groups $I(R|P)$, i.e.*

$$G = \langle I(R|P) : P \text{ place of } K,\ R|P,\ R \text{ place of } M \rangle.$$

The following result follows from [11, Proposition 1 on p275].

Proposition 2.5. *Let G be a transitive subgroup of S_n generated by transpositions. Then $G = S_n$.*

3. From geometry to Galois theory

For this section, let $\mathbb{K}$ be an algebraically closed field, let $\mathbb{P}^2 = \mathbb{P}^2(\mathbb{K})$, and let r be a line in $\mathbb{P}^2$. Remark 3.9 combined with Chebotarev Density Theorem explains one way to transfer geometric information obtained over $\mathbb{P}^2(\overline{\mathbb{F}}_q)$ to arithmetic information in $\mathbb{P}^2(\mathbb{F}_q)$, which will be needed to construct m-arcs in $\mathbb{P}^2(\mathbb{F}_q)$ in Section 4.

Definition 3.1. The line $r \subseteq \mathbb{P}^2$ is said to be a *bitangent* to a curve $\mathcal{C}$ if it has at least two non-singular points of intersection with $\mathcal{C}$ where it is tangent to $\mathcal{C}$.

We start with a preliminary lemma.

Lemma 3.2. *Let $\mathcal{C} \subseteq \mathbb{P}^2$ be an irreducible plane projective curve of degree m over a finite field $\mathbb{F}_q$ with singular points contained in the line at infinity. Let $\mathcal{C}^*$ be the dual curve of $\mathcal{C}$ and suppose $\mathbb{F}_q(\mathcal{C}) \cong_{\mathcal{G}} \mathbb{F}_q(\mathcal{C}^*)$, that is $\mathbb{F}_q(\mathcal{C})$ and $\mathbb{F}_q(\mathcal{C}^*)$ are isomorphic through the Gauss map $\mathcal{G}$. Then there are at most $\mathcal{O}(m^4)$ affine bitangents to the curve.*

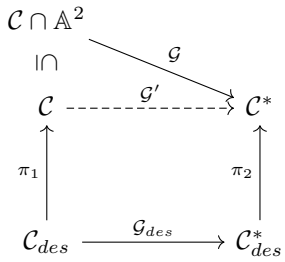
Proof. Let $F = F(X_0, X_1, X_2) = 0$ (resp. $G = G(X_0, X_1, X_2) = 0$) be the homogeneous equation of $\mathcal{C}$ (resp. $\mathcal{C}^*$). Since F has degree m, then G has at most degree $m(m-1)$ (see for example [23]).

Since $\mathbb{F}_q(\mathcal{C}) \cong_{\mathcal{G}} \mathbb{F}_q(\mathcal{C}^*)$, the Gauss map $\mathcal{G} : \mathcal{C} \cap \mathbb{A}^2 \to \mathcal{C}^*$ can be extended to a birational map $\mathcal{G}'$ between $\mathcal{C}$ and $\mathcal{C}^*$.

Let $\mathcal{C}_{des}$ and $\mathcal{C}^*_{des}$ be the non-singular models of $\mathcal{C}$ and $\mathcal{C}^*$ respectively. Let $\pi_1 : \mathcal{C}_{des} \to \mathcal{C}$ and $\pi_2 : \mathcal{C}^*_{des} \to \mathcal{C}^*$ the birational morphisms attached to the non-singular models (satisfying the universal property shown in Subsection 2.3, and defined everywhere as explained in Subsection 2.2, notice in particular Remark 2.2).

Notice that, thanks to Proposition 2.1 the birational map $\mathcal{G}' \circ \pi_1$ is a birational morphism because $\mathcal{C}_{des}$ is non-singular.

By using the universal property of π_2 for the birational morphism $\mathcal{G}' \circ \pi_1 : \mathcal{C}_{des} \dashrightarrow \mathcal{C}^*$ between $\mathcal{C}_{des}$ and $\mathcal{C}^*_{des}$ one obtains an isomorphism $\mathcal{G}_{des}$ that makes the diagram commutative.



The number of affine bitangents to $\mathcal{C} \cap \mathbb{A}^2$ equals the number of points of $\mathcal{C}^*$ that have multiple preimages through $\mathcal{G}$. Our strategy is to prove that the points of $\mathcal{C}^*$ that have multiple preimages via $\mathcal{G}$ are contained in the points of $\mathcal{C}^*$ that are singular. We will then bound the singular points with Bezout's Theorem. Suppose that P is a point of $\mathcal{C}^*$ that has a set $T \subseteq \mathcal{C} \cap \mathbb{A}^2$ of preimages via $\mathcal{G}$ of size larger than or equal to 2. Let now $T' = \pi_1^{-1}(T) \subseteq \mathcal{C}_{des}$. Since the diagram commutes, we have that $\pi_2 \circ \mathcal{G}_{des}(T') = \{P\}$, and therefore π_2 is mapping a set of points of size larger than 1 to a single point P, so P must be a singular point of $\mathcal{C}^*$.

We can now estimate the number of singular points of $\mathcal{C}^*$ using Bezout's Theorem: these points are contained in the set of solutions of the equations $G = 0$ and $G_0 = \frac{\partial}{\partial X_0} G = 0$, which are at most $\mathcal{O}(\deg(G)\deg(G_0)) = \mathcal{O}(m^4)$ because G_0 cannot divide G due to irreducibility. □

Lemma 3.3. *Let $\mathcal{C} \subseteq \mathbb{P}^2$ be a non-singular plane projective curve of degree m over a finite field $\mathbb{F}_q$ such that $\mathcal{C}$ is birationally equivalent to its dual curve $\mathcal{C}^*$ through the Gauss map. Then there are at most $\mathcal{O}(m^4)$ bitangents to the curve.*

Proof. It is a direct consequence of Lemma 3.2 because $\mathcal{C}$ is non-singular. □

Remark 3.4. Notice that for irreducible, non-singular plane projective curves, being birationally equivalent to the dual curve is a generic condition as long as the characteristic is different from 2 if the base field is large enough (see for example [14, Theorem 5.90] and specifically the rank condition on the matrix in [14, Equation 5.49]).

Definition 3.5. Let $\mathcal{C} \subseteq \mathbb{P}^2$ a plane curve. A line of $\mathbb{P}^2$ that is tangent to $\mathcal{C}$ with multiplicity at least 3 at a non-singular point $P \in \mathcal{C}$ is said to be an *inflection tangent* and the point of tangency P is said to be an *inflection point*.

Theorem 3.6. *Let $\mathcal{C}$ be an irreducible plane projective curve of degree $m \geq 3$ over a field K and $F = 0$ its homogeneous equation. Let H_F be the Hessian determinant associated to F. Let p be the characteristic of K, and assume that either $p = 0$ or $p > m$. Then $H_F \not\equiv 0 \mod (F)$, and the intersection of F with its Hessian curve consists of the singular points of $\mathcal{C}$ and the inflection points of $\mathcal{C}$.*

Proof. The claim follows using [20, Theorem 9.7 (b)] since $\mathcal{C}$ is irreducible. □

Lemma 3.7. *Let p be a prime number and q a power of p. Let $\mathcal{C} \subseteq \mathbb{P}^2$ be an irreducible plane projective curve of degree $m \geq 3$ over a finite field $\mathbb{F}_q$. Then, if $p > m$ the number of inflection tangents to $\mathcal{C}$ are at most $\mathcal{O}(m^2)$.*

Proof. Let $F = F(X_0, X_1, X_2) = 0$ be a homogeneous equation of $\mathcal{C}$. Let H_F be the Hessian determinant associated to F, therefore $\deg(H_F) \leq 3(m-2)$. Now, since $\mathcal{C}$ is irreducible we can use Theorem 3.6 obtaining that the intersection between $\mathcal{C}$ and the set of points that vanish at H_F consists only of singular points and inflection points of $\mathcal{C}$. Since by definition each inflection point has at most one inflection tangent, one can bound the number of inflection tangents with the number of inflection points and singular points of $\mathcal{C}$, that is $\mathcal{O}(\deg(F)\deg(H_F)) = \mathcal{O}(m^2)$ as a consequence of Bezout's Theorem. □

The following is a particular instance of a classical fact, we include its proof for completeness.

Lemma 3.8. *Let p be a prime number, q a power of p, and $K/\overline{\mathbb{F}}_q$ be a function field over $\overline{\mathbb{F}}_q$. Let $L : K$ be a proper finite separable extension of degree n of global function fields, and M be the Galois closure of $L : K$. Let P be a place of K, $\mathcal{Q}_P$ be the set of places of L lying above P, $e(Q|P)$ the ramification index of $Q \in \mathcal{Q}_P$ over P and $f(Q|P)$ the relative degree. Suppose that for every P and for every $Q \in \mathcal{Q}_P$ we have $e(Q|P) \leq 2$ and $e(\bar{Q}|P) = 2$ at most once for some $\bar{Q}|P$. If $G := \mathrm{Gal}(M : K)$ is transitive, then G is the symmetric group S_n.*

Proof. Using Proposition 2.5 it is enough to prove that G is generated by transpositions. By Lemma 2.4, since G is generated by the inertia groups $I(R|P)$ where R is a place of M lying above P, it is enough to prove that the inertia groups contain only transpositions. Since we are working over the algebraic closure, the decomposition group $D(R|P)$ equals the inertia group $I(R|P)$. In particular $f(R|P) = f(R|Q)f(Q|P) = 1$ and so $f(Q|P) = 1$. By the Orbits' Lemma 2.3 the action of $D(R|P)$ (i.e. $I(R|P)$) on $\mathrm{Hom}_K(L, M)$ gives orbits of order $e(Q|P)$, so each decomposition group acts either like the identity or a transposition. Since G acts faithfully on $\mathrm{Hom}_K(L, M)$ and $D(R|P) \leq G$, $D(R|P)$ cannot contain more than one element that acts like a transposition on the set $\mathrm{Hom}_K(L, M)$, so either $D(R|P) = \{1_G\}$ or $D(R|P) = \{1_G, g \mid g \text{ transposition }\}$. This shows that G is generated by transpositions, and therefore since G is transitive we have $G = S_n$. □

Remark 3.9. Notice that the lemma above can also be used to show that an *arithmetic* Galois group is symmetric. In fact, if $M : K$ is a Galois extension of a function field $K/\mathbb{F}_q$, then we have that $\mathrm{Gal}(k_M M : k_M K) = \mathrm{Gal}(\overline{\mathbb{F}}_q M : \overline{\mathbb{F}}_q K)$, where k_M is the field of constants of M (see for example [22, Lemma 2.6]). This implies that $\mathrm{Gal}(\overline{\mathbb{F}}_q M : \overline{\mathbb{F}}_q K)$ is canonically contained in $\mathrm{Gal}(M : K) \leq S_{[M:K]}$. Therefore, if one can prove $\mathrm{Gal}(\overline{\mathbb{F}}_q M : \overline{\mathbb{F}}_q K) = S_{[M:K]}$, one also has $\mathrm{Gal}(M : K) = S_{[M:K]}$ and most importantly $k_M = \mathbb{F}_q$.

4. Main result

Let us now state and prove the main theorem.

Theorem 4.1. *Let p be a prime number and q a power of p. Let $\mathcal{C} \subseteq \mathbb{P}^2$ be an irreducible plane projective curve of degree m over a finite field $\mathbb{F}_q$ such that $p > m$, the singular points of $\mathcal{C}$ are contained in the line at infinity, and that $\mathcal{C}$ is birationally equivalent to its dual $\mathcal{C}^*$ through the Gauss map. There exists an explicit constant c independent of q, for which if $q > c$ then there exists a set of points $S \subseteq \mathbb{P}^2(\mathbb{F}_q)$ of size at most $O(m^5)$ such that $\mathcal{C}(\mathbb{F}_q) \cup S$ is a complete m-arc of $\mathbb{P}^2(\mathbb{F}_q)$.*

Remark 4.2. Notice that the condition that $\mathcal{C}$ is birationally equivalent to its dual $\mathcal{C}^*$ is generic in characteristic different from 2 (see Remark 3.4). It is possible to calculate a sharp explicit constant c by estimating via Hurwitz formula the genus of the Galois closure of a certain covering of curves that appears in the proof (see Remark 4.3).

Proof of Theorem 4.1. Consider $\mathcal{R} = \{r_1, \dots, r_N\}$ with $N = \mathcal{O}(m^4)$ the set of all the bitangents and inflection tangents as in Lemma 3.2 and Lemma 3.7.

Firstly, we prove that through any affine point outside these lines and outside $\mathcal{C}(\mathbb{F}_q)$, there exists a line intersecting $\mathcal{C}(\mathbb{F}_q)$ in exactly m affine points. Afterwards, we outline how to choose a set S of points on the lines in $\mathcal{R}$ to construct a complete m-arc $\mathcal{C}(\mathbb{F}_q) \cup S$.

Therefore, consider a point $P = (a, b) \in \mathbb{A}^2(\mathbb{F}_q)$ such that $P \notin r_i$ for any $i \in \{1, \dots, N\}$. Let $f(x, y) = 0$ an affine equation for $\mathcal{C}$, i.e. $f(x, y) \in \mathbb{F}_q[x, y]$ irreducible of degree m. Let $\ell_{P,t} : y = t(x - a) + b$ be the (formal) line through P with slope t and

$$F_P(t, x) = f(x, t(x - a) + b) \in \mathbb{F}_q[t, x]$$

be the polynomial obtained by $f(x, y)$, which results from substituting y with $t(x-a)+b$. We want to prove that there exists a specialization t_0 for t such that $F_P(t_0, x)$ totally splits, giving m points of intersection between the curve $f(x, y) = 0$ and the line ℓ_{P,t_0}. To this end, consider $G = \mathrm{Gal}(F_P(t, x) \mid \overline{\mathbb{F}}_q(t))$. Now notice that since $f(x, y)$ is irreducible, we have that $F_P(t, x)$ is an irreducible polynomial. Set $K = \mathbb{F}_q(t)$ and let L be the fraction field of $\mathbb{F}_q[x, t]/\langle F_P(t, x)\rangle$. Let M be the Galois closure of $L : K$ and observe that $\overline{\mathbb{F}}_q M$ is the Galois closure of $\overline{\mathbb{F}}_q L : \overline{\mathbb{F}}_q K$. Now let P be a place of $\overline{\mathbb{F}}_q K$ and $\mathcal{Q}_P$ the set of places of $\overline{\mathbb{F}}_q L$ lying above P. Because we are neither on a bitangent nor on an inflection tangent, $e(Q|P) \leq 2$ and $e(\bar{Q}|P) = 2$ at most once for some $\bar{Q}|P$. Therefore, by Lemma 3.8 and Remark 3.9.

$$\mathrm{Gal}(\overline{\mathbb{F}}_q M : \overline{\mathbb{F}}_q(t)) = \mathrm{Gal}(M : K) = S_m.$$

By [6, Theorem 3.3], there exists an explicit constant c depending only on the genus of M and the degree of $[L : K]$ for which if $q > c$ then $L : K$ has a totally split place, that

means a t_0 exists such that ℓ_{P,t_0} intersects $\mathcal{C}$ in m distinct affine points, i.e. the point P is collinear with other m distinct points of $\mathcal{C}$.

For a set of points $T \subseteq \mathbb{P}^2(\mathbb{F}_q)$, we say that a point $Q \in \mathbb{P}^2(\mathbb{F}_q) \setminus T$ is *covered by* T if there are m distinct points of T collinear with Q.

We now show how to construct the set S recursively so that $\mathcal{C}(\mathbb{F}_q) \cup S$ is a complete m-arc of $\mathbb{P}^2(\mathbb{F}_q)$. First, set $A_0 = \mathcal{C}(\mathbb{F}_q)$. Now for $i \in \{1, \dots, N\}$ set $A_i = A_{i-1} \cup H_i$ where H_i satisfies the following

1) $H_i \subset r_i$ and $|H_i| \leq m$;
2) $\nexists\, m+1$ points in $A_i = A_{i-1} \cup H_i$ that are collinear
3) each point of r_i is covered by A_i.

Such H_i always exists: running over the points in $r_i \in \mathcal{R}$ we consider them one by one and add them to the arc until we get all points on r_i covered. This procedure adds at most m points, which constitute the set H_i. In other words, for every $i \in \{1, \dots, N\}$, one must consider the tangent r_i, take a point and add it to the set if it is not covered by the set of points added until then. We observe now that H_i cannot contain more than m points because r_i is a line (and therefore any m points on r_i cover all points in r_i). Once all points on the line r_i are covered, one can move to r_{i+1} continuing the same procedure.

Finally, consider ℓ_∞ the line at infinity in $\mathbb{P}^2(\mathbb{F}_q)$. With the same procedure, we can find at most m points $P_1, \dots, P_m \in \ell_\infty$ in such a way that

$$A = A_N \cup \{P_1, \dots, P_m\}$$

is also an m-arc. Set now

$$S := A \setminus \mathcal{C}(\mathbb{F}_q).$$

Note that since we have added at most m points for each tangent in $\mathcal{R}$ and for ℓ_∞, the size of S is at most $\mathcal{O}(m^5)$. Obviously the set $A = C(\mathbb{F}_q) \cup S$ is a complete m-arc of $\mathbb{P}^2(\mathbb{F}_q)$ by construction. □

Remark 4.3. Following [6, Corollary 3.4], since $p > m$, the explicit constant c can be chosen to be

$$c = 9(g_K + g_L + m)^2(m!)^2 = 9m^2(m!)^2,$$

where g_K and g_L are the genera of K and L appearing in the proof of Theorem 4.1.

Since a non-singular projective curve obviously verifies the hypothesis of Theorem 4.1, we have proven the following, which we state for conveniency of future reference.

Theorem 4.4. *Let p be a prime number and q a power of p. Let $\mathcal{C} \subseteq \mathbb{P}^2$ be a nonsingular plane projective curve of degree m over a finite field $\mathbb{F}_q$ such that $p > m$, and $\mathcal{C}$ is birationally equivalent to its dual $\mathcal{C}^*$ through the Gauss map. There exists an explicit constant c independent of q, for which if $q > c$ then there exists a set of points $S \subseteq \mathbb{P}^2(\mathbb{F}_q)$ of size at most $O(m^5)$ such that $\mathcal{C}(\mathbb{F}_q) \cup S$ is a complete m-arc of $\mathbb{P}^2(\mathbb{F}_q)$.*

We now observe that our theory goes well beyond the restrictions given by Theorem 4.1. In fact, if one does not require the characteristic to be greater than the degree of the curve one has the following result.

Theorem 4.5. *Let p be a prime number and q a power of p. Let $\mathcal{C} \subseteq \mathbb{P}^2$ be an irreducible plane projective curve of degree m over a finite field $\mathbb{F}_q$, the singular points of $\mathcal{C}$ are contained in the line at infinity, and $\mathcal{C}$ is birationally equivalent to its dual $\mathcal{C}^*$ through the Gauss map. There exists an explicit constant c independent of q, for which if $q > c$ then there exists a set of points $S \subseteq \mathbb{P}^2(\mathbb{F}_q)$ of size at most $mT + O(m^5)$ such that $\mathcal{C}(\mathbb{F}_q) \cup S$ is a complete m-arc of $\mathbb{P}^2(\mathbb{F}_q)$, where T is the number of inflection tangents to the curve $\mathcal{C}$.*

Proof. The proof of this is completely identical with the wrinkle that one has to add separately m points for every inflection tangent to the curve, where now the number of inflection tangents is not absolutely bounded. More precisely, this refined count is necessary because we are not anymore ensured that the number of inflection tangents is $O(m^2)$, as Lemma 3.6 would prescribe in the case $p > m$. Notice also that the genus of M (on which the constant c depends in the proof of Theorem 4.1) can be bounded independently of q simply using recursively Castelnuovo Inequality [29, Theorem 3.11.3]. □

We will show an application of Theorem 3.6 in the case of Artin-Schreier curves.

5. Applications

To show the effectiveness of our construction, in this section we want to illustrate how a complete m-arc can be constructed using hyperelliptic curves, and Artin-Schreier curves of degree $m > p$.

Proposition 5.1. *Let p be an odd prime number, q be a power of p, and $m \geq 3$ be a positive integer smaller than p. Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of degree m with m distinct roots. Let $\mathcal{C}$ be the projective closure of the affine curve defined by the equation $y^2 - f(x) = 0$. Then $\mathbb{F}_q(\mathcal{C})$ is isomorphic to $\mathbb{F}_q(\mathcal{C}^*)$ via the Gauss map $\mathcal{G}$.*

Proof. It is enough to show the equality in (1) using $g(x, y) = y^2 - f(x)$. First, let us observe that

$$\mathbb{F}_q(\mathcal{C}^*) \cong \mathbb{F}_q\left(-\frac{f'(x)}{2y}, -\frac{xf'(x)}{2y} + y\right) \subseteq \mathbb{F}_q(\mathcal{C}) = \mathbb{F}_q(x)[y]/\langle y^2 - f(x)\rangle.$$

From now on, we will omit the dependence on x when it does not create confusion, and write f and f' instead of $f(x)$ and $f'(x)$. In the rest of the proof we show that $\mathbb{F}_q(x) \subseteq \mathbb{F}_q\left(\frac{f'}{2y}, -\frac{xf'}{2y} + y\right)$ which directly implies that

$$\mathbb{F}_q\left(\frac{f'}{2y}, -\frac{xf'}{2y} + y\right) = \mathbb{F}_q(\mathcal{C}).$$

Notice that

$$\left(\frac{f'}{2y}\right)^2 = \frac{(f')^2}{4f} =: k,$$
$$\frac{f'}{2y}\left(-\frac{xf'}{2y} + y\right) = -\frac{x(f')^2}{4f} + \frac{f'}{2} = \frac{-x(f')^2 + 2ff'}{4f} =: h$$

and that

$$\left(-\frac{xf'}{2y} + y\right)^2 = \frac{(xf' - 2f)^2}{4f} =: u.$$

Let $a \in \mathbb{F}_q$ be the leading coefficient of f. Observe that the leading coefficient of $-x(f')^2 + 2ff'$ is $-(a\deg(f))^2 + 2a^2\deg(f) = \deg(f)a^2(-\deg(f) + 2) \neq 0$ because f has degree larger than 2 and the characteristic is larger than $\deg(f)$. Let us now treat two separate cases.

Case (1): $x \nmid f$. In this case $\deg(h) = 2\deg(f) - 1$, because numerator and denominator are coprime, and k has degree $2\deg(f) - 2$. By Luroth Theorem this shows that $\mathbb{F}_q(h,k) = \mathbb{F}_q(x)$, as we now explain. In fact, let $s = s_1/s_2 \in \mathbb{F}_q(x)$ (with $s_1, s_2 \in \mathbb{F}_q[x]$ and coprime) be such that $\mathbb{F}_q(h,k) = \mathbb{F}_q(s)$ and let $n = \deg(s) = \max\{\deg(s_1), \deg(s_2)\} = [\mathbb{F}_q(x) : \mathbb{F}_q(s)]$. Then by the Tower Law we also have that every function in $\mathbb{F}_q(s)$ has degree divisible by n, but since $\gcd(\deg(h), \deg(k)) = 1$, then $n = 1$, and therefore $\mathbb{F}_q(x) = \mathbb{F}_q(s)$, concluding the proof for this case.

Case (2): $x \mid f$. Rewrite u as

$$u = \frac{x(f' - 2(f/x))^2}{4(f/x)}$$

and therefore observe that $\deg(u) = 2\deg(f) - 1$ because the leading coefficient of $f' - 2(f/x)$ is $a\deg(f) - 2a \neq 0$, f is squarefree, and the numerator and denominator are coprime because f and f' are coprime. But $\deg(k) = 2\deg(f) - 2$ which concludes the proof using Luroth's theorem with the same argument as Case (1). □

The following is immediate to see using Theorem 4.1.

Corollary 5.2. *Let $m \geq 3$ be a positive integer and p an odd prime greater than m. There exists an absolute constant c, depending only on m, such that for any $q = p^\ell > c$ power of*

p, any hyperelliptic curve $\mathcal{H} : y^2 - f(x) = 0$ over $\mathbb{F}_q$ of degree m gives rise to a complete m-arc of size $|\mathcal{H}(\mathbb{F}_q)| + \mathcal{O}(m^5)$ in the sense of Theorem 4.1.

Proof. It is enough to check that the hypotheses of Theorem 4.1 are verified. □

The next example allows us to construct a complete m-arc on $\mathbb{F}_{q^2}$ with $q^2 - 2gq + c$ points, where c is a constant that does not depend on q, and g is the genus of the hyperelliptic curve:

$$g = \begin{cases} (m-1)/2 & \text{if } m \equiv 1 \mod 2, \\ (m-2)/2 & \text{if } m \equiv 0 \mod 2. \end{cases}$$

Example 5.3. We illustrate now how our method works by producing a complete m-arc of small size for a very well known family of hyperelliptic curves. Let q be an odd prime power and m a positive integer that divides $q+1$. Then, by [33, Theorem 1], the hyperelliptic curve $\mathcal{C}$ given by $y^2 = x^m + 1$ is maximal over $\mathbb{F}_{q^2}$, i.e. the number of places of degree 1 (i.e. defined over $\mathbb{F}_{q^2}$) of $\mathbb{F}_{q^2}(\mathcal{C}) = \mathbb{F}_{q^2}(x, y)$ (with $y^2 = x^m + 1$) is $\#\mathcal{C}(\mathbb{F}_{q^2}) = q^2 + 1 + 2gq$ where g indicates the genus of $\mathcal{C}$. Notice that the affine places of degree 1 of $\mathbb{F}_{q^2}(\mathcal{C})$ are in natural bijective correspondence with the $\mathbb{F}_{q^2}$-rational points of the affine points of $\mathcal{C}$, as the only singular point is at infinity.

We note that, as x varies in $\mathbb{F}_{q^2}$, $x^m + 1$ essentially covers the maximal number of squares. Conversely, for every non-square $\xi \in \mathbb{F}_{q^2}$, the curve $\mathcal{C}'$ defined by $y^2 = \xi(x^m + 1)$ covers fewer squares and can be used to construct a m-arc with less points. We now give an estimate of the number of points of $\mathcal{C}'$.

First of all, notice that if a point $(x, 0)$ belongs to $\mathcal{C}$, it also belongs to $\mathcal{C}'$. Moreover, since $m | q+1$ and $q-1$ is even, $2m | q^2 - 1$. Thus the polynomial $x^{2m} - 1$ splits completely over $\mathbb{F}_{q^2}$ and so $x^m + 1$ does. This means that the number of points of the form $(x, 0)$ is exactly m.

The $\mathbb{F}_{q^2}$ affine rational points (x_0, y_0) of $\mathcal{C}$ such that $y_0 \neq 0$ are at least

$$q^2 + 1 + 2gq - \#\mathcal{P}_\infty - m,$$

where $\#\mathcal{P}_\infty$ refers to the number of places at the infinity of $\mathbb{F}_q(\mathcal{C})$. Therefore, the x_0's such that $x_0^m + 1$ is a square different from zero are at least

$$\frac{q^2 + 1 + 2gq - \#\mathcal{P}_\infty - m}{2}.$$

We can now count the $\mathbb{F}_{q^2}$ affine rational points of $\mathcal{C}'$, which are

$$m + 2\Big(q^2 - \frac{q^2 + 1 + 2gq - \#\mathcal{P}_\infty - m}{2}\Big) = q^2 - (1 + 2gq - \#\mathcal{P}_\infty) + 2m.$$

Therefore, the complete m-arc obtained from $\mathcal{C}'$ is made of $q^2 - 2gq + \mathcal{O}(m^5)$ points. Of course, if one works out exactly the constants and the number of bitangents it follows that the implied constants and the $O(m^5)$ are loose bounds and one can do better. Nevertheless, this shows that the size of the complete m-arc $\mathcal{A}_{q^2}$ constructed from these hyperelliptic curves satisfies $\#\mathcal{A}_{q^2} - q^2 \to -\infty$ for $q \to \infty$. As a byproduct, this also removes the restriction on the existence of the prime r in [6, Proposition 6.4].

Remark 5.4. So far in the literature, it has been shown how complete m-arcs can be constructed for $m = 2, 3, 4$ and $m \geq 8$ using certain curves, see [6]. This example, and more generally the theory developed in this work, can be used to construct m-arcs for arbitrary values of $m \geq 3$ and arbitrary curve verifying generic conditions. As a byproduct, we have covered the cases when $m = 5, 6, 7$ that were missing in the literature.

Using Theorem 4.5, we now show that Artin-Schreier curves of degree $m > p$ can be used to construct an m-arc.

Theorem 5.5. *Let $\mathbb{F}_q$ be a finite field of odd characteristic p and m be a positive integer larger than p. Let $f \in \mathbb{F}_q[x]$ be such that $f \neq z^p - z$ for any $z \in \mathbb{F}_q[x]$, and f squarefree of degree m such that $f' \notin \mathbb{F}_q[x^p]$. Let $\mathcal{C}$ be the projective closure of the affine curve defined by $g(x, y) := y^p - y - f(x) = 0$. Then there exists an absolute constant c, depending only on m, such that if $q > c$, then there exists a complete m-arc with $|\mathcal{C}(\mathbb{F}_q)| + O(m^5)$ points.*

Proof. First, we will prove that

$$\mathbb{F}_q(x, y) = \mathbb{F}_q\left(\frac{\partial_x g(x,y)}{\partial_y g(x,y)}, x\frac{\partial_x g(x,y)}{\partial_y g(x,y)} + y\right),$$

verifying the hypothesis of Lemma 3.2. Therefore, we need to show that

$$\mathbb{F}_q(f', xf' + y) = \mathbb{F}_q(x, y),$$

where $g(x, y) = 0$. By computing

$$(xf' + y)^p - (xf' + y) = x^p (f')^p - xf' + f =: h.$$

We realize that if we prove that $\mathbb{F}_q(f', h) = \mathbb{F}_q(x)$, then $\mathbb{F}_q(x) \subseteq \mathbb{F}_q(f', xf' + y)$ which implies $\mathbb{F}_q(f', xf' + y) \supseteq \mathbb{F}_q(x, y)$ and therefore the claim.

Since $\mathbb{F}_q(f', h) \subseteq \mathbb{F}_q(x)$, by Luroth's Theorem there exists $s \in \mathbb{F}_q(x)$ such that $\mathbb{F}_q(f', h) = \mathbb{F}_q(s)$. In particular, this implies that, for some $u, v \in \mathbb{F}_q(x)$, we have that $u(s) = f'$ and $v(s) = h$, which forces

$$x^p u(s)^p - xu(s) + f = v(s).$$

By deriving both sides we get

$$-u(s) - xu'(s)s' + u(s) = v'(s)s'$$

and therefore

$$(xu'(s) + v'(s))s' = 0$$

so either $x = -v'(s)/u'(s)$, in which case we are done, or $s' = 0$, but then $s = \ell(x^p) \in \mathbb{F}_q(x^p)$ and therefore $f' = u(\ell(x^p))$, contradicting the hypothesis $f' \notin \mathbb{F}_q[x^p]$.

We now count the number of inflection tangents. Notice that for every inflection point there exists exactly one inflection tangent. Therefore, one can bound the number of inflection tangents by the number of inflection points.

We are now going to characterize the inflection points. Suppose $P_0 = (x_0, y_0)$ is an affine inflection point of $\mathcal{C}$ and let ℓ_{P_0} be the affine tangent line to $\mathcal{C}$ at such a point, namely

$$\ell_{P_0} : \ -f'(x_0)(x - x_0) + y_0 - y = 0.$$

Now, intersecting $g(x, y) = 0$ with ℓ_{P_0}, one gets

$$-f'(x_0)^p(x - x_0)^p + y_0^p + f'(x_0)(x - x_0) - y_0 - f(x) = 0$$

and since $y_0^p - y_0 = f(x_0)$ we have

$$-f'(x_0)^p(x - x_0)^p + f'(x_0)(x - x_0) + f(x_0) - f(x) = 0.$$

Writing $t := x - x_0$ one can rewrite the previous equation as follows

$$-f'(x_0)^p t^p + f'(x_0)t + f(x_0) - f(t + x_0) = 0. \tag{2}$$

Now notice that, for suitable $a_0, \dots, a_m \in \mathbb{F}_q$, one always has

$$\begin{aligned} f(t + x_0) =& \sum_{i=0}^{m} a_i(t + x_0)^i = \sum_{i=0}^{m}\sum_{j=0}^{i} a_i \binom{i}{j} x_0^j t^{i-j} = \\ =& f(x_0) + f'(x_0)t + \frac{1}{2}f''(x_0)t^2 + \sum_{i=0}^{m}\sum_{j=0}^{i-3} a_i \binom{i}{j} x_0^j t^{i-j}. \end{aligned} \tag{3}$$

Using (3) and (2) one gets

$$f'(x_0)^p t^p + \frac{1}{2}f''(x_0)t^2 + \sum_{i=0}^{m}\sum_{j=0}^{i-3} a_i \binom{i}{j} x_0^j t^{i-j} = 0. \tag{4}$$

However, since $P_0 = (x_0, y_0)$ is an inflection point, the order of tangency must be at least 3, namely in the equation (4) the term $f''(x_0)$ should be zero. This means that the

inflection points are contained in the set of solutions of $g(x_0, y_0) = 0$ and $f''(x_0) = 0$. Since $f' \notin \mathbb{F}_q[x^p]$, then f'' is not identically zero, which implies that there are at most $\deg(f'')p = (m-2)p$ inflection tangents. Since $p < m$ we have that the number of inflection tangents is at most m^2. We now apply directly Theorem 4.5. □

Data availability

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

Acknowledgments

This work was supported by the National Science Foundation under Grant No 2127742. We would like to thank Gabriele Mondello for providing deep geometric insight that helped us to simplify some proofs in the paper.

References

[1] N. Anbar Meidl, D. Bartoli, M. Giulietti, I. Platoni, Small complete caps from singular cubics, J. Comb. Des. 22 (2013) 409–424.
[2] N. Anbar Meidl, D. Bartoli, M. Giulietti, I. Platoni, Small complete caps from singular cubics, II, J. Algebraic Comb. 41 (2015) 185–216, https://doi.org/10.1007/s10801-014-0532-7.
[3] N. Anbar Meidl, M. Giulietti, Bicovering arcs and small complete caps from elliptic curves, J. Algebraic Comb. 38 (2013) 371–392.
[4] D. Bartoli, M. Giulietti, G. Zini, Complete $(k, 3)$-arcs from quartic curves, Des. Codes Cryptogr. 79 (2016) 487–505.
[5] D. Bartoli, S. Marcugini, F. Pambianco, On the completeness of plane cubic curves over finite fields, Des. Codes Cryptogr. 83 (2017) 233–267.
[6] D. Bartoli, G. Micheli, Algebraic constructions of complete m-arcs, Combinatorica (2022), https://doi.org/10.1007/s00493-021-4712-5.
[7] D. Bartoli, P. Speziali, G. Zini, Complete $(k, 4)$-arcs from quintic curves, J. Geom. 108 (2017) 985–1011.
[8] M. Giulietti, On plane arcs contained in cubic curves, Finite Fields Appl. 8 (2002) 69–90.
[9] M. Giulietti, F. Pasticci, On the completeness of certain n-tracks arising from elliptic curves, Finite Fields Appl. 13 (2007) 988–1000.
[10] N. Hamilton, T. Penttila, Sets of type (a, b) from subgroups of $\Gamma L(1, p^R)$, J. Algebraic Comb. 13 (2001) 67–76.
[11] K. Hashimoto, K. Miyake, H. Nakamura, Galois Theory and Modular Forms, vol. 11, Springer Science & Business Media, 2004.
[12] J.W.P. Hirschfeld, Algebraic curves, arcs, and caps over finite fields, in: Quaderni del Dipartimento di Matematica dell'Università del Salento (Lecce), 1986.
[13] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, Oxford Mathematical Monographs, Clarendon Press, URL, 1998, https://books.google.com/books?id=RL7GbrBQwd8C.
[14] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic Curves over a Finite Field, Princeton University Press, 2008.
[15] J.W.P. Hirschfeld, L. Storme, The packing problem in statistics, coding theory and finite projective spaces, J. Stat. Plan. Inference 72 (1998) 355–380.
[16] J.W.P. Hirschfeld, J.F. Voloch, The characterization of elliptic curves over finite fields, J. Aust. Math. Soc. 45 (1988) 275–286.
[17] J.H. Kim, V.H. Vu, Small complete arcs in projective planes, Combinatorica 23 (2003) 311–363.
[18] G. Korchmáros, G.P. Nagy, T. Szőnyi, Algebraic approach to the completeness problem for (k, n)-arcs in planes over finite fields, arXiv preprint, arXiv:2302.10162, 2023.

[19] G. Korchmáros, New examples of complete k-arcs in $\mathbb{PG}(2,q)$, Eur. J. Comb. 4 (1983) 329–334, https://doi.org/10.1016/S0195-6698(83)80029-8, https://www.sciencedirect.com/science/article/pii/S0195669883800298.
[20] E. Kunz, R. Belshoff, Introduction to Plane Algebraic Curves, Birkhäuser, Boston, 2007, URL https://books.google.it/books?id=ZexFAAAAQBAJ.
[21] L. Lombardo-Radice, Sul problema dei k-archi completi in $\mathcal{S}_{2,q}$, ($q = p^t$, p primo dispari), Boll. UMI 11 (1956) 178–181, http://eudml.org/doc/195863.
[22] G. Micheli, On the selection of polynomials for the DLP quasi-polynomial time algorithm for finite fields of small characteristic, SIAM J. Appl. Algebra Geom. 3 (2019) 256–265.
[23] H.D. Nguyen, Invariants of plane curve singularities and Plücker formulas in positive characteristic, in: Annales de l'Institut Fourier, 2016, pp. 2047–2066.
[24] R. Schoof, Nonsingular plane cubic curves over finite fields, J. Comb. Theory, Ser. A 46 (1987) 183–211.
[25] B. Segre, Le geometrie di Galois, Ann. Mat. Pura Appl. 48 (1959) 1–96.
[26] B. Segre, Ovali e curve σ nei piani di Galois di caratteristica due, Atti Accad. Naz. Lincei, VIII. Ser., Rend., Cl. Sci. Fis. Mat. Nat. 32 (1962) 785–790.
[27] I.R. Shafarevich, Basic Algebraic Geometry 1, 3rd ed., Springer, Berlin, 2013, URL https://cds.cern.ch/record/1596976.
[28] J. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, Springer, New York, 2009, URL https://books.google.it/books?id=Z90CA_EUCCkC.
[29] H. Stichtenoth, Algebraic Function Fields and Codes, 2nd ed., Springer Publishing Company, Incorporated, 2008.
[30] T. Szőnyi, Small complete arcs in Galois planes, Geom. Dedic. 18 (1985) 161–172.
[31] T. Szőnyi, Complete arcs in Galois planes: a survey, in: Quaderni del Seminario di Geometrie Combinatorie 94, Dipartimento di Matematica "G. Castelnuovo", Università degli Studi di Roma "La Sapienza", 1989.
[32] T. Szőnyi, Some Applications of Algebraic Curves in Finite Geometry and Combinatorics, London Mathematical Society Lecture Note Series, Cambridge University Press, 1997.
[33] S. Tafazolian, A family of maximal hyperelliptic curves, J. Pure Appl. Algebra 216 (2012) 1528–1532, https://doi.org/10.1016/j.jpaa.2012.01.019, https://www.sciencedirect.com/science/article/pii/S0022404912000369.
[34] M. Tallini Scafati, Graphic curves on a Galois plane, in: Atti del convegno di Geometria combinatoria e sue Applicazioni, Perugia, 1970, pp. 413–419.
[35] J.F. Voloch, On the completeness of certain plane arcs-II, Eur. J. Comb. 11 (1990) 491–496, https://doi.org/10.1016/S0195-6698(13)80032-7, https://www.sciencedirect.com/science/article/pii/S0195669813800327.
[36] J.F. Voloch, Complete arcs in Galois planes of non-square order, in: Advances in Finite Geometries and Designs, 1991, pp. 401–406.
[37] B.L. van der Waerden, Die Zerlegungs- und Trägheitsgruppe als Permutationsgruppen, Math. Ann. 111 (1935) 731–733, https://doi.org/10.1007/BF01472249.