

COMPLETE ARCS AND COMPLETE CAPS FROM CUBICS WITH AN ISOLATED DOUBLE POINT

NURDAGÜL ANBAR, DANIELE BARTOLI, MASSIMO GIULIETTI, AND IRENE PLATONI

ABSTRACT. Small complete arcs and caps in Galois spaces over finite fields \mathbb{F}_q with characteristic greater than 3 are constructed from cubic curves with an isolated double point. For m a divisor of $q + 1$, complete plane arcs of size approximately q/m are obtained, provided that $(m, 6) = 1$ and $m < \frac{1}{4}q^{1/4}$. If in addition $m = m_1m_2$ with $(m_1, m_2) = 1$, then complete caps of size approximately $\frac{m_1+m_2}{m}q^{N/2}$ in affine spaces of dimension $N \equiv 0 \pmod{4}$ are constructed.

1. INTRODUCTION

In an (affine or projective) space over a finite field, a cap is a set of points no three of which are collinear. A cap is said to be complete if it is maximal with respect to set theoretical inclusion. Plane caps are usually called arcs.

Arcs and caps have played an important role in Finite Geometry since the pioneering work by B. Segre [19]. These objects are relevant also in Coding Theory, being the geometrical counterpart of distinguished types of error-correcting and covering linear codes. In this direction, an important issue is to ask for explicit constructions of small complete caps in Galois spaces. In fact, complete caps correspond to quasi-perfect linear codes with covering radius 2, so that the smaller is the size of the cap, the better is the density of the covering code.

The trivial lower bound for the size of a complete cap in a Galois space of dimension N and order q is

$$(1) \quad \sqrt{2}q^{(N-1)/2}.$$

If q is even and N is odd, such bound is substantially sharp; see [17]. Otherwise, all known infinite families of complete caps have size far from (1); see the survey papers [13, 14] and the more recent works [1, 3–6, 10–12]. For $q = p^s$ with $p > 3$ a prime, the smallest explicitly described complete plane caps are due to Szőnyi, who constructed complete arcs with roughly q/m points for any divisor m of $q - 1$ satisfying $m < \frac{1}{C}q^{1/4}$, with $C > 1$ is a constant

This research was supported by the Italian Ministry MIUR, Geometrie di Galois e strutture di incidenza, PRIN 2009–2010, by INdAM, and by Tubitak Proj. Nr. 111T234.

Nurdagül Anbar - Faculty of Engineering and Natural Sciences - Sabanci University
Orhanli-Tuzla - 34956 Istanbul - Turkey.

Daniele Bartoli - Dipartimento di Matematica e Informatica - University of Perugia
Via Vanvitelli 1 - 06123 Perugia - Italy.

Massimo Giulietti - Dipartimento di Matematica e Informatica - University of Perugia
Via Vanvitelli 1 - 06123 Perugia - Italy.

Irene Platoni - Dipartimento di Matematica - University of Trento
Via Sommarive, 14 - 38123, Povo (TN) - Italy.

independent of q [23, 24]¹. From these arcs, by using some lifting methods, complete caps of size roughly $q^{N/2}/\sqrt{m}$ in $AG(N, q)$, $N \equiv 0 \pmod{4}$, are obtained in [2, 3]. The aim of this paper is to obtain similar results for the case where m is a divisor of $q + 1$, in order to significantly widen the range of q 's for which complete arcs in $AG(2, q)$ of size about $q^{3/4}$, as well as complete caps in $AG(N, q)$ with roughly $q^{(4N-1)/8}$ points, can actually be constructed. To this end, plane cubics with an isolated double points are considered.

Let G denote the abelian group of the non-singular \mathbb{F}_q -rational points of an irreducible plane cubic \mathcal{X} defined over \mathbb{F}_q . It was already noted by Zirilli [27] that no three points in a coset A of a subgroup K of G can be collinear, provided that the index m of K in G is not divisible by 3. Since then, arcs in cubics have been thoroughly investigated, as well as caps arising from these arcs by recursive constructions; see [1–3, 7, 9, 15, 22–26]. However, no results about arcs and caps from cubics with an isolated double point have appeared so far. One of the problems that come up when dealing with these cubics is that the natural parametrization of the points of A , arising from the natural isomorphism between G and the subgroup of order $q + 1$ of the multiplicative group of \mathbb{F}_{q^2} , involves polynomial functions defined over \mathbb{F}_{q^2} but not over \mathbb{F}_q . This makes it impossible a straightforward application of the classical method by Segre [18] and Lombardo Radice [16] for proving that a point P off \mathcal{X} is collinear with two points in A ; in fact, such method needs that the algebraic curve \mathcal{C} describing the collinearity with P and two generic points in A is defined over \mathbb{F}_q . A key point of the paper is to overcome such a difficulty by finding a curve which is birationally equivalent to \mathcal{C} , but is defined over \mathbb{F}_q ; see Lemmas 15 and 16.

The main achievements here are Theorems 26 and 29. For a divisor m of $q + 1$ such that $(m, 6) = 1$ and $m \leq \sqrt[4]{q}/4$, we explicitly describe a complete arc of size approximately $m + \frac{q+1}{m}$; if in addition m admits a non-trivial factorization $m = m_1 m_2$ with $(m_1, m_2) = 1$, we also provide complete caps of size approximately $\frac{m_1+m_2}{m} q^{N/2}$ in affine spaces $AG(N, q)$ with dimension $N \equiv 0 \pmod{4}$.

The paper is organized as follows. In Section 2 we review some of the standard facts on curves and algebraic function fields. We also briefly sketch a recursive construction from [10] of complete caps from bicovering arcs, that is arcs for which completeness holds in a stronger sense; see Definition 4. Section 3 presents some preliminary results on the algebraic curve describing the collinearity with P and two generic points in A . The proof that under our assumptions on m almost each point P not on \mathcal{X} is bcovered by the secants of A is the main object of Section 4; see Propositions 19, 20, and 23. The case where P lies in \mathcal{X} is dealt with in Proposition 24. Finally, the proof of our main results is completed in Section 5.

2. PRELIMINARIES

Let q be an odd prime power, and let \mathbb{F}_q denote the finite field with q elements. Throughout the paper, \mathbb{K} will denote the algebraic closure of \mathbb{F}_q .

2.1. Curves and function fields. Let \mathcal{C} be a projective absolutely irreducible algebraic curve, defined over the algebraic closure \mathbb{K} of \mathbb{F}_q . An *algebraic function field* F over \mathbb{K} is an extension F of \mathbb{K} such that F is a finite algebraic extension of $\mathbb{K}(x)$, for some element $x \in F$

¹The condition of m being a divisor of $q - 1$ was not originally required in [24], but is actually needed in order for the proof of a key lemma by Voloch to be correct; see Remark 4 in [3].

transcendental over \mathbb{K} . If $F = \mathbb{K}(x)$, then F is called the *rational function field* over \mathbb{K} . For basic definitions on function fields we refer to [21].

It is well known that to any curve \mathcal{C} defined over \mathbb{K} one can associate a function field $\mathbb{K}(\mathcal{C})$ over \mathbb{K} , namely the field of the rational functions of \mathcal{C} . Conversely, to a function field F over \mathbb{K} one can associate a curve \mathcal{C} , defined over \mathbb{K} , such that $\mathbb{K}(\mathcal{C})$ is \mathbb{K} -isomorphic to F . The genus of F as a function field coincides with the genus of \mathcal{C} .

A place γ of $\mathbb{K}(\mathcal{C})$ can be associated to a single point of \mathcal{C} called the *center* of γ , but not vice versa. A bijection between places of $\mathbb{K}(\mathcal{C})$ and points of \mathcal{C} holds provided that the curve \mathcal{C} is non-singular.

Let F be a function field over \mathbb{K} . If F' is a finite extension of F , then a place γ' of F' is said to be *lying over* a place γ of F , if $\gamma \subset \gamma'$. This holds precisely when $\gamma = \gamma' \cap F$. In this paper $e(\gamma'|\gamma)$ will denote the *ramification index* of γ' over γ .

A finite extension F' of a function field F is said to be *unramified* if $e(\gamma'|\gamma) = 1$ for every γ' place of F' and every γ place of F with γ' lying over γ .

Proposition 1 (Proposition 3.7.3 in [21]). *Let F be an algebraic function field over \mathbb{K} , and let $m > 1$ be an integer relatively prime to the characteristic of \mathbb{K} . Suppose that $u \in F$ is an element satisfying $u \neq \omega^e$ for all $\omega \in F$ and $e|m$, $e > 1$. Let*

$$(2) \quad F' = F(y) \text{ with } y^m = u.$$

Then

(i) *for γ' a place of F' lying over a place γ of F , we have $e(\gamma'|\gamma) = \frac{m}{r_\gamma}$ where*

$$(3) \quad r_\gamma := (m, v_\gamma(u)) > 0$$

is the greatest common divisor of m and $v_\gamma(u)$;

(ii) *if g (resp. g') denotes the genus of F (resp. F') as a function field over \mathbb{K} , then*

$$g' = 1 + m \left(g - 1 + \frac{1}{2} \sum_{\gamma} \left(1 - \frac{r_\gamma}{m} \right) \right),$$

where γ ranges over the places of F and r_γ is defined by (3).

An extension such as F' in Proposition 1 is said to be a *Kummer extension* of F .

A curve \mathcal{C} is said to be defined over \mathbb{F}_q if the ideal of \mathcal{C} is generated by polynomials with coefficients in \mathbb{F}_q . In this case, $\mathbb{F}_q(\mathcal{C})$ denotes the subfield of $\mathbb{K}(\mathcal{C})$ consisting of the rational functions defined over \mathbb{F}_q . A place of $\mathbb{K}(\mathcal{C})$ is said to be \mathbb{F}_q -rational if it is fixed by the Frobenius map on $\mathbb{K}(\mathcal{C})$. The center of an \mathbb{F}_q -rational place is an \mathbb{F}_q -rational point of \mathcal{C} ; conversely, if P is a simple \mathbb{F}_q -rational point of \mathcal{C} , then the only place centered at P is \mathbb{F}_q -rational. The following result is a corollary to Proposition 1.

Proposition 2. *Let \mathcal{C} be an irreducible plane curve of genus g defined over \mathbb{F}_q . Let $u \in \mathbb{F}_q(\mathcal{C})$ be a non-square in $\mathbb{K}(\mathcal{C})$. Then the Kummer extension $\mathbb{K}(\mathcal{C})(w)$, with $w^2 = u$, is the function field of some irreducible curve defined over \mathbb{F}_q of genus*

$$g' = 2g - 1 + \frac{M}{2},$$

where M is the number of places of $\mathbb{K}(\mathcal{C})$ with odd valuation of u .

The function field $\mathbb{K}(\mathcal{C})(w)$ as in Proposition 2 is said to be a *double cover* of $\mathbb{K}(\mathcal{C})$ (and similarly the corresponding irreducible curve defined over \mathbb{F}_q is called a double cover of \mathcal{C}).

Finally, we recall the Hasse-Weil bound, which will play a crucial role in our proofs.

Proposition 3 (Hasse-Weil Bound - Theorem 5.2.3 in [21]). *The number N_q of \mathbb{F}_q -rational places of the function field $\mathbb{K}(\mathcal{C})$ of a curve \mathcal{C} defined over \mathbb{F}_q with genus g satisfies*

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

2.2. Complete caps from bicobering arcs. Throughout this section, N is assumed to be a positive integer divisible by 4. Let $q' = q^{\frac{N-2}{2}}$. Fix a basis of $\mathbb{F}_{q'}$ as a linear space over \mathbb{F}_q , and identify points in $AG(N, q)$ with vectors of $\mathbb{F}_{q'} \times \mathbb{F}_{q'} \times \mathbb{F}_q \times \mathbb{F}_q$.

For an arc \mathcal{A} in $AG(2, q)$, let

$$C_{\mathcal{A}} = \{(\alpha, \alpha^2, u, v) \in AG(N, q) \mid \alpha \in \mathbb{F}_{q'}, (u, v) \in \mathcal{A}\}.$$

As noticed in [10], the set $C_{\mathcal{A}}$ is a cap whose completeness in $AG(N, q)$ depends on the bicobering properties of \mathcal{A} in $AG(2, q)$, defined as follows. According to Segre [20], given three pairwise distinct points P, P_1, P_2 on a line ℓ in $AG(2, q)$, P is external or internal to the segment P_1P_2 depending on whether

$$(4) \quad (x - x_1)(x - x_2) \text{ is a non-zero square or a non-square in } \mathbb{F}_q,$$

where x, x_1 and x_2 are the coordinates of P, P_1 and P_2 with respect to any affine frame of ℓ .

Definition 4. *Let \mathcal{A} be a complete arc in $AG(2, q)$. A point $P \in AG(2, q) \setminus \mathcal{A}$ is said to be bicobered by \mathcal{A} if there exist $P_1, P_2, P_3, P_4 \in \mathcal{A}$ such that P is both external to the segment P_1P_2 and internal to the segment P_3P_4 . If every $P \in AG(2, q) \setminus \mathcal{A}$ is bicobered by \mathcal{A} , then \mathcal{A} is said to be a bicobering arc. If there exists precisely one point $Q \in AG(2, q) \setminus \mathcal{A}$ which is not bicobered by \mathcal{A} , then \mathcal{A} is said to be almost bicobering, and Q is called the center of \mathcal{A} .*

A key tool in this paper is the following result from [10].

Proposition 5. *Let τ be a non-square in \mathbb{F}_q . If \mathcal{A} is a bicobering k -arc, then $C_{\mathcal{A}}$ is a complete cap in $AG(N, q)$ of size $kq^{(N-2)/2}$. If \mathcal{A} is almost bicobering with center $Q = (x_0, y_0)$, then either*

$$C = C_{\mathcal{A}} \cup \{(\alpha, \alpha^2 - \tau, x_0, y_0) \mid \alpha \in \mathbb{F}_{q'}\}$$

or

$$C = C_{\mathcal{A}} \cup \{(\alpha, \alpha^2 - \tau^2, x_0, y_0) \mid \alpha \in \mathbb{F}_{q'}\}$$

is a complete cap in $AG(N, q)$ of size $(k+1)q^{(N-2)/2}$. The former case occurs precisely when Q is external to every secant of \mathcal{A} through Q .

3. A FAMILY OF CURVES DEFINED OVER \mathbb{F}_q

Throughout this section $q = p^h$ for some prime $p > 3$, and m is a proper divisor of $q + 1$ with $(m, 6) = 1$. Also, \bar{t} is a non-zero element in \mathbb{F}_{q^2} which is not an m -th power in \mathbb{F}_{q^2} . Let $A, B \in \mathbb{F}_{q^2}$ with $AB \neq (A - 1)^3$. An important role for the present investigation is played by the curve

$$(5) \quad \mathcal{C}_{A,B,\bar{t},m} : f_{A,B,\bar{t},m}(X, Y) = 0,$$

where

$$(6) \quad f_{A,B,\bar{t},m}(X,Y) = A(\bar{t}^3 X^{2m} Y^m + \bar{t}^3 X^m Y^{2m} - 3\bar{t}^2 X^m Y^m + 1) - B\bar{t}^2 X^m Y^m - \bar{t}^4 X^{2m} Y^{2m} + 3\bar{t}^2 X^m Y^m - \bar{t} X^m - \bar{t} Y^m.$$

The curve $\mathcal{C}_{A,B,\bar{t},m}$ was thoroughly investigated in [2].

Proposition 6 (Case 2 of Proposition 9 in [2]). *Let A, B be such that*

- $AB \neq (A-1)^3$;
- $A \neq 0$;
- *either $A^3 \neq -1$ or $B \neq 1 - (A-1)^3$.*

Then the curve $\mathcal{C}_{A,B,\bar{t},m}$ is absolutely irreducible of genus $g \leq 3m^2 - 3m + 1$.

Under the assumptions of Proposition 6, let \bar{x} and \bar{y} denote the rational functions associated to the affine coordinates X and Y , respectively. Then $\mathbb{K}(\mathcal{C}_{A,B,\bar{t},m}) = \mathbb{K}(\bar{x}, \bar{y})$ with $f_{A,B,\bar{t},m}(\bar{x}, \bar{y}) = 0$. Let $\bar{u} = \bar{x}^m$ and $\bar{z} = \bar{y}^m$. The following results from [2] about the function field extension $\mathbb{K}(\bar{x}, \bar{y}) : \mathbb{K}(\bar{u}, \bar{z})$ will be needed.

Proposition 7 (Lemma 4 in [2]). *In the function field $\mathbb{K}(\bar{u}, \bar{z})$, there exist six places γ_j , $j = 1, \dots, 6$, such that*

$$\operatorname{div}(\bar{u}) = \gamma_4 + \gamma_5 - \gamma_1 - \gamma_2, \quad \operatorname{div}(\bar{z}) = \gamma_2 + \gamma_6 - \gamma_3 - \gamma_4.$$

Proposition 8 (Case 2 of Proposition 9 in [2]). *For each $j = 1, \dots, 6$, the ramification index of γ_j in the extension $\mathbb{K}(\bar{x}, \bar{y})$ over $\mathbb{K}(\bar{u}, \bar{z})$ is equal to m , and no other place of $\mathbb{K}(\bar{u}, \bar{z})$ is ramified.*

According to [2], for $j = 1, \dots, 6$, let $\bar{\gamma}_j^1, \dots, \bar{\gamma}_j^m$ denote the places of $\mathbb{K}(\bar{x}, \bar{y})$ lying over the place γ_j of $\mathbb{K}(\bar{u}, \bar{z})$.

Proposition 9 (Case 2 of Proposition 9 in [2]). *In $\mathbb{K}(\bar{x}, \bar{y})$,*

$$(7) \quad \operatorname{div}((A - \bar{t}\bar{x}^m)(A - \bar{t}\bar{y}^m)) = m \left(\sum_{i=1}^m (\bar{\gamma}_5^i + \bar{\gamma}_6^i - \bar{\gamma}_4^i - \bar{\gamma}_2^i) \right).$$

In order to investigate the bicoverying properties of a coset of index m in the abelian group of the non-singular \mathbb{F}_q -rational points of a cubic with an isolated double point we need to establish whether

$$\frac{(A - \bar{t}\bar{x}^m)(A - \bar{t}\bar{y}^m)}{(1 - \bar{t}\bar{x}^m)(1 - \bar{t}\bar{y}^m)}$$

is a square in $\mathbb{K}(\bar{x}, \bar{y})$.

Proposition 10. *Assume that A and B satisfy the conditions of Proposition 6. For $d \in \mathbb{K}$, $d \neq 0$, let*

$$\eta = d \frac{(A - \bar{t}\bar{x}^m)(A - \bar{t}\bar{y}^m)}{(1 - \bar{t}\bar{x}^m)(1 - \bar{t}\bar{y}^m)}.$$

If $A \neq 1$, then

(i) *the divisor of η is*

$$m \sum_{i=1}^m (\bar{\gamma}_5^i + \bar{\gamma}_6^i + \bar{\gamma}_1^i + \bar{\gamma}_3^i) - \bar{D},$$

- where $\bar{\bar{D}}$ is a divisor of degree $4m^2$ whose support consists of places not lying over any place in $\{\gamma_j \mid j = 1, \dots, 6\}$;
- (ii) the function field $\mathbb{K}(\bar{x}, \bar{y}, \bar{w})$ with $\bar{w}^2 = \eta$ is a Kummer extension of $\mathbb{K}(\bar{x}, \bar{y})$;
 - (iii) the genus of the function field $\mathbb{K}(\bar{x}, \bar{y}, \bar{w})$ is less than or equal to $8m^2 - 4m + 1$.

Proof. By Propositions 7, from $A \neq 1$ it is easy to deduce that the divisor of $1 - \bar{t}\bar{u}$ in $\mathbb{K}(\bar{u}, \bar{z})$ is

$$-\gamma_1 - \gamma_2 + D_1,$$

where D_1 is the degree-2 divisor of the zeros of $1 - \bar{t}\bar{u}$. Similarly,

$$\operatorname{div}(1 - \bar{t}\bar{z}) = -\gamma_3 - \gamma_4 + D_2,$$

and hence in $\mathbb{K}(\bar{u}, \bar{z})$ we have

$$\operatorname{div}((1 - \bar{t}\bar{u})(1 - \bar{t}\bar{z})) = -\gamma_1 - \gamma_2 - \gamma_3 - \gamma_4 + D,$$

where D is a divisor of degree 4 whose support is disjoint from $\{\gamma_i \mid i = 1, \dots, 6\}$. Therefore, by Proposition 8,

$$\operatorname{div}((1 - \bar{t}\bar{x}^m)(1 - \bar{t}\bar{y}^m)) = m \sum_{i=1}^m (-\bar{\gamma}_1^i - \bar{\gamma}_2^i - \bar{\gamma}_3^i - \bar{\gamma}_4^i) + \bar{\bar{D}},$$

where $\bar{\bar{D}}$ is a divisor of degree $4m^2$ whose support is disjoint from the set of places lying over $\{\gamma_i \mid i = 1, \dots, 6\}$. Then by Proposition 9 the divisor of η is

$$m \sum_{i=1}^m (\bar{\gamma}_5^i + \bar{\gamma}_6^i + \bar{\gamma}_1^i + \bar{\gamma}_3^i) - \bar{\bar{D}}.$$

This proves (i). As η is not a square in $\mathbb{K}(\bar{x}, \bar{y})$, assertion (ii) holds as well. Finally, Proposition 1 yields (iii). \square

4. COVERING PROPERTIES OF CERTAIN SUBSETS OF \mathcal{X}

Throughout this section we fix an element β in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ such that $\beta^2 \in \mathbb{F}_q$. Let \mathcal{X} be the plane cubic with equation

$$Y(X^2 - \beta^2) = 1.$$

The point Y_∞ is an isolated double point with tangents $X = \pm\beta$, and X_∞ is an inflection point with tangent $Y = 0$. We choose X_∞ as the neutral element of the abelian group $(\mathcal{X} \setminus \{Y_\infty\}, \oplus)$ of the non-singular points of \mathcal{X} .

For $v \in \mathbb{K} \setminus \{0, 1\}$, let Q_v be the point on \mathcal{X} with affine coordinates $(\frac{v+1}{v-1}\beta, \frac{(v-1)^2}{4v\beta^2})$. Also, let $Q_0 = Y_\infty$ and $Q_1 = X_\infty$. Such a parametrization actually defines an isomorphism between $(\mathcal{X} \setminus \{Y_\infty\}, \oplus)$ and the multiplicative group of \mathbb{K} . In fact, it is straightforward to check that for $v, w \in \mathbb{K}^*$,

$$(8) \quad Q_v \oplus Q_w = Q_{vw}.$$

The $(q+1)$ non-singular \mathbb{F}_q -rational points of \mathcal{X} form a cyclic subgroup G of $(\mathcal{X} \setminus \{Y_\infty\}, \oplus)$. It is easily seen that

$$G = \{Q_{\frac{u+\beta}{u-\beta}} \mid u \in \mathbb{F}_q\} \cup \{X_\infty\}.$$

For a divisor m of $q+1$, the group G has precisely one subgroup K of index m , consisting of the m -th powers in G . By (8),

$$K = \{Q_{(\frac{u+\beta}{u-\beta})^m} \mid u \in \mathbb{F}_q\} \cup \{X_\infty\}.$$

Let $T = Q_{\bar{t}}$ be a point in $G \setminus K$ and let K_T be the coset $K \oplus T$. Then

$$(9) \quad K_T = \{Q_{\bar{t}(\frac{u+\beta}{u-\beta})^m} \mid u \in \mathbb{F}_q\} \cup \{Q_{\bar{t}}\}.$$

Throughout this section a, b are elements in \mathbb{F}_q with $b(a^2 - \beta^2) \neq 1$, and P is the point in $AG(2, q) \setminus \mathcal{X}$ with affine coordinates (a, b) . We also assume that $(m, 6) = 1$. Let

$$g_{a,b}(X, Y) := bX^2Y^2 - (b\beta^2 + 1)(X^2 + Y^2) - XY + a(X + Y) + \beta^2(b\beta^2 + 1),$$

and

$$L_{a,b,\bar{t},m}(X, Y) = (\bar{t}X^m - 1)^2(\bar{t}Y^m - 1)^2 g_{a,b}\left(\beta \frac{\bar{t}X^m + 1}{\bar{t}X^m - 1}, \beta \frac{\bar{t}Y^m + 1}{\bar{t}Y^m - 1}\right).$$

Lemma 11. *Let (x, y) be an affine point of the curve $L_{a,b,\bar{t},m}(X, Y) = 0$. If*

$$(\bar{t}x^m - 1)(\bar{t}y^m - 1)(x^m - y^m) \neq 0,$$

then P is collinear with $Q_{\bar{t}x^m}$ and $Q_{\bar{t}y^m}$.

Proof. We first note that for u, v distinct elements in $\mathbb{K} \setminus \{\pm\beta\}$, the point P is collinear with $(u, \frac{1}{u^2-\beta^2})$ and $(v, \frac{1}{v^2-\beta^2})$ if and only if $g_{a,b}(u, v) = 0$. In fact,

$$\det \begin{pmatrix} u & \frac{1}{u^2-\beta^2} & 1 \\ v & \frac{1}{v^2-\beta^2} & 1 \\ a & b & 1 \end{pmatrix}$$

is equal to

$$\frac{1}{(u^2 - \beta^2)(v^2 - \beta^2)}(v - u)[bu^2v^2 - (b\beta^2 + 1)(u^2 + v^2) - uv + a(u + v) + b\beta^4 + \beta^2].$$

It is straightforward to check that $Q_{\bar{t}x^m}$ coincides with $(u, \frac{1}{u^2-\beta^2})$ precisely when $u = \beta \frac{\bar{t}x^m + 1}{\bar{t}x^m - 1}$. Then the claim follows by the definition of $L_{a,b,\bar{t},m}$. \square

The curve with equation $L_{a,b,\bar{t},m}(X, Y) = 0$ actually belongs to the family described in Section 3.

Lemma 12. *Let*

$$A = \frac{a + \beta}{a - \beta}, \quad B = \frac{8b\beta^3}{a - \beta}.$$

Then

$$L_{a,b,\bar{t},m}(X, Y) = -2\beta(a - \beta)f_{A,B,\bar{t},m}(X, Y)$$

where $f_{A,B,\bar{t},m}$ is defined as in (6).

Proof. The proof is a straightforward computation. \square

Henceforth, $\sqrt{-3}$ will denote a fixed square root of -3 in \mathbb{F}_{q^2} .

Lemma 13. *If*

$$(10) \quad (a, b) \notin \left\{ \left(0, -\frac{9}{8\beta^2}\right), (\beta\sqrt{-3}, 0), (-\beta\sqrt{-3}, 0) \right\}$$

then $L_{a,b,\bar{t},m}(X, Y) = 0$ is an absolutely irreducible curve with genus less than or equal to $3m^2 - 3m + 1$.

Proof. For A, B as in Lemma 12, let $\mathcal{C}_{A,B,\bar{t},m}$ be as in (5). By Lemma 12, the curve $L_{a,b,\bar{t},m}(X, Y) = 0$ is actually $\mathcal{C}_{A,B,\bar{t},m}$. Note that m divides $q^2 - 1$ and that each coefficient of $f_{A,B,\bar{t},m}(X, Y)$ lies in \mathbb{F}_{q^2} . Then by Proposition 6 the curve $\mathcal{C}_{A,B,\bar{t},m}$ is absolutely irreducible of genus $g \leq 3m^2 - 3m + 1$, provided that none of the following holds:

- (1) $AB = (A - 1)^3$;
- (2) $A = 0$;
- (3) $A^3 = -1$ and $B = 1 - (A - 1)^3$.

Case (1) cannot occur as $b(a^2 - \beta^2) \neq 1$. Also, $a \in \mathbb{F}_q$ implies $a + \beta \neq 0$, which rules out (2). Assume then that (3) holds. Then $A^3 = -1$ implies $a(a^2 + 3\beta^2) = 0$. From $B = 1 - (A - 1)^3$ we deduce

$$b = 3 \frac{a^2 + 3\beta^2}{8\beta^2(\beta a - \beta^2)}.$$

Then either $(a, b) = (0, -\frac{9}{8\beta^2})$ or $(a, b) = (\pm\beta\sqrt{-3}, 0)$, a contradiction. \square

Remark 14. *Let $q = p^s$ with $p > 3$ a prime. Then -3 is a non-square in \mathbb{F}_q if and only if s is odd and $p \equiv 2 \pmod{3}$; see e.g. [9, Lemma 4.5].*

In order to show that if (10) holds then P is collinear with two points in K_T , we need to ensure the existence of a point (x, y) of the curve $L_{a,b,\bar{t},m}(X, Y) = 0$ such that $Q_{\bar{t}x^m}$ and $Q_{\bar{t}y^m}$ are distinct points in K_T . To this end, it is useful to consider a curve which is birationally equivalent to $L_{a,b,\bar{t},m}(X, Y) = 0$, but, unlike $L_{a,b,\bar{t},m}(X, Y) = 0$, is defined over \mathbb{F}_q .

Let

$$M_{a,b,\bar{t},m}(R, V) := (R - \beta)^{2m}(V - \beta)^{2m} L_{a,b,\bar{t},m}\left(\frac{R + \beta}{R - \beta}, \frac{V + \beta}{V - \beta}\right) = 0.$$

Lemma 15. *If (10) holds, then $M_{a,b,\bar{t},m}(R, V) = 0$ is an absolutely irreducible curve birationally equivalent to $L_{a,b,\bar{t},m}(X, Y) = 0$.*

Proof. Let $\mathbb{K}(\bar{x}, \bar{y})$ be the function field of $L_{a,b,\bar{t},m}(X, Y) = 0$, so that $L_{a,b,\bar{t},m}(\bar{x}, \bar{y}) = 0$. Both the degrees of the extensions $\mathbb{K}(\bar{x}, \bar{y}) : \mathbb{K}(\bar{x})$ and $\mathbb{K}(\bar{x}, \bar{y}) : \mathbb{K}(\bar{y})$ are equal to $2m$. Let

$$\bar{r} := \beta \frac{\bar{x} + 1}{\bar{x} - 1}, \quad \bar{v} := \beta \frac{\bar{y} + 1}{\bar{y} - 1}.$$

Then $M_{a,b,\bar{t},m}(\bar{r}, \bar{v}) = 0$. As

$$\bar{x} = \frac{\bar{r} + \beta}{\bar{r} - \beta}, \quad \bar{y} = \frac{\bar{v} + \beta}{\bar{v} - \beta}$$

we have

$$\mathbb{K}(\bar{x}, \bar{y}) = \mathbb{K}(\bar{r}, \bar{v}), \quad \mathbb{K}(\bar{x}) = \mathbb{K}(\bar{r}), \quad \mathbb{K}(\bar{y}) = \mathbb{K}(\bar{v}).$$

Therefore, both the degrees of the extensions $\mathbb{K}(\bar{r}, \bar{v}) : \mathbb{K}(\bar{r})$ and $\mathbb{K}(\bar{r}, \bar{v}) : \mathbb{K}(\bar{v})$ are equal to $2m$. As the degrees of $M_{a,b,\bar{t},m}(R, V)$ in both R and V are also equal to $2m$, the polynomial $M_{a,b,\bar{t},m}(R, V)$ cannot be reducible. \square

Lemma 16. *The curve with equation $M_{a,b,\bar{t},m}(R, V) = 0$ is defined over \mathbb{F}_q .*

Proof. We are going to show that up to a scalar factor in \mathbb{K}^* the coefficients of $M_{a,b,\bar{t},m}(R, V)$ lie in \mathbb{F}_q . Consider the following polynomials in $\mathbb{F}_{q^2}[Z]$:

$$\theta_1(Z) = (Z + \beta)^m + (Z - \beta)^m, \quad \theta_2(Z) = \frac{1}{\beta}((Z + \beta)^m - (Z - \beta)^m),$$

Let

$$t = \beta \frac{\bar{t} + 1}{\bar{t} - 1},$$

As both t and β^2 belong to \mathbb{F}_q , the polynomials

$$(11) \quad h(Z) = t\theta_1(Z) + \beta^2\theta_2(Z), \quad l(Z) = \theta_1(Z) + t\theta_2(Z)$$

actually lie in $\mathbb{F}_q[Z]$. Taking into account that $t = \beta \frac{\bar{t}+1}{\bar{t}-1}$, a straightforward computation gives

$$(12) \quad \bar{t} \left(\frac{Z + \beta}{Z - \beta} \right)^m = \frac{\frac{h(Z)}{l(Z)} + \beta}{\frac{h(Z)}{l(Z)} - \beta}.$$

Whence,

$$\bar{t} \left(\frac{Z + \beta}{Z - \beta} \right)^m + 1 = \frac{2h(Z)}{h(Z) - \beta l(Z)} \quad \text{and} \quad \bar{t} \left(\frac{Z + \beta}{Z - \beta} \right)^m - 1 = \frac{2\beta l(Z)}{h(Z) - \beta l(Z)}.$$

We then have that $M_{a,b,\bar{t},m}(R, V)$ coincides with

$$(R - \beta)^{2m}(V - \beta)^{2m} \left(\frac{2\beta l(R)}{h(R) - \beta l(R)} \right)^2 \left(\frac{2\beta l(V)}{h(V) - \beta l(V)} \right)^2 g_{a,b} \left(\frac{h(R)}{l(R)}, \frac{h(V)}{l(V)} \right).$$

From

$$h(Z) - \beta l(Z) = 2(t - \beta)(Z - \beta)^m$$

we obtain

$$M_{a,b,\bar{t},m}(R, V) = \frac{\beta^4}{(t - \beta)^4} l(R)^2 l(V)^2 g_{a,b} \left(\frac{h(R)}{l(R)}, \frac{h(V)}{l(V)} \right),$$

whence the assertion. \square

Remark 17. *By the proof of Lemma 11, for any $z \in \mathbb{F}_q$, the X -coordinate of the point $Q_{\bar{t}(\frac{z+\beta}{z-\beta})^m}$ is $u = \beta(\bar{t}(\frac{z+\beta}{z-\beta})^m + 1)/(\bar{t}(\frac{z+\beta}{z-\beta})^m - 1)$. Then, by (12), $u = \frac{h(z)}{l(z)}$ holds, with $h(Z)$ and $l(Z)$ as in (11).*

Remark 18. *If (r, v) is an \mathbb{F}_q -rational affine point of the curve $M_{a,b,\bar{t},m}(R, V) = 0$ with*

$$\left(\frac{r + \beta}{r - \beta} \right)^m \neq \left(\frac{v + \beta}{v - \beta} \right)^m$$

then $P = (a, b)$ is collinear with $Q_{\bar{t}(\frac{r+\beta}{r-\beta})^m}$ and $Q_{\bar{t}(\frac{v+\beta}{v-\beta})^m}$, which are two distinct points in K_T by (9).

Proposition 19. *Let $P = (a, b)$ be a point in $AG(2, q)$ off \mathcal{X} . Assume that (10) holds. If*

$$q + 1 - (6m^2 - 6m + 2)\sqrt{q} \geq 4m^2 + 8m + 1$$

then P is collinear with two distinct points of K_T .

Proof. Let $\mathbb{K}(\bar{r}, \bar{v})$ be the function field of $M_{a,b,\bar{t},m}(R, V) = 0$, so that $M_{a,b,\bar{t},m}(\bar{r}, \bar{v}) = 0$ holds. Let E be the set of places γ of $\mathbb{K}(\bar{r}, \bar{v})$ for which at least one of the following holds:

- (1) γ is a pole of either \bar{r} or \bar{v} ;
- (2) γ is a pole of either $\left(\frac{\bar{r}+\beta}{\bar{r}-\beta}\right)$ or $\left(\frac{\bar{v}+\beta}{\bar{v}-\beta}\right)$;
- (3) γ is a zero of $\left(\frac{\bar{r}+\beta}{\bar{r}-\beta}\right)^m - \left(\frac{\bar{v}+\beta}{\bar{v}-\beta}\right)^m$.

As both degrees of the extensions $\mathbb{K}(\bar{r}, \bar{v}) : \mathbb{K}(\bar{r})$ and $\mathbb{K}(\bar{r}, \bar{v}) : \mathbb{K}(\bar{v})$ are equal to $2m$, the number of places satisfying (1) is at most $4m$. According to the proof of Lemma 15, we have that

$$\bar{x} = \frac{\bar{r} + \beta}{\bar{r} - \beta}, \quad \bar{y} = \frac{\bar{v} + \beta}{\bar{v} - \beta}$$

satisfy $f_{A,B,\bar{t},m}(\bar{x}, \bar{y}) = 0$. Therefore, by Propositions 7 and 8 the number places satisfying (2) is $4m$. It is easily seen that in $\mathbb{K}(\bar{u}, \bar{z})$ the rational function $\bar{u} - \bar{z}$ has at most 4 distinct zeros; hence, the set of poles of $\bar{x}^m - \bar{y}^m$ in $\mathbb{K}(\bar{x}, \bar{y})$ has size less than or equal to $4m^2$. This shows that E comprises at most $4m^2 + 8m$ places. Our assumption on q and m , together with the Hasse-Weil bound, ensures the existence of at least $4m^2 + 8m + 1$ \mathbb{F}_q -rational places of $\mathbb{K}(\bar{r}, \bar{v})$; hence, there exists at least one \mathbb{F}_q -rational place γ_0 of $\mathbb{K}(\bar{r}, \bar{v})$ not in E . Let $\bar{r} = \bar{r}(\gamma_0)$ and $\bar{v} = \bar{v}(\gamma_0)$. By Remark 18, $P = (a, b)$ is collinear with $Q_{\bar{t}(\frac{\bar{r}+\beta}{\bar{r}-\beta})^m}$ and $Q_{\bar{t}(\frac{\bar{v}+\beta}{\bar{v}-\beta})^m}$, which are two distinct points in K_T . \square

The following technical variant of Proposition 19 will also be needed.

Proposition 20. *Let $P = (a, b)$ be a point in $AG(2, q)$ off \mathcal{X} . Assume that (10) holds. If*

$$(13) \quad q + 1 - (6m^2 - 6m + 2)\sqrt{q} \geq 8m^2 + 8m + 1$$

then P is collinear with two distinct points of $K_T \setminus \{T\}$.

Proof. One can argue as in the proof of Proposition 19. We need to ensure that neither $Q_{\bar{t}(\frac{\bar{r}+\beta}{\bar{r}-\beta})^m}$ or $Q_{\bar{t}(\frac{\bar{v}+\beta}{\bar{v}-\beta})^m}$ coincides with T . As $T = Q_{\bar{t}}$, this is equivalent to γ_0 not being a zero of either $\left(\frac{\bar{r}+\beta}{\bar{r}-\beta}\right)^m - 1$ or $\left(\frac{\bar{v}+\beta}{\bar{v}-\beta}\right)^m - 1$ in the function field $\mathbb{K}(\bar{r}, \bar{v})$. By Proposition 7, in $\mathbb{K}(\bar{u}, \bar{z})$ both rational functions $\bar{u} - 1$ and $\bar{z} - 1$ have at most two distinct zeros. Therefore, there are at most $4m^2$ places γ_0 that need to be ruled out. \square

If (10) is not satisfied, then P is not collinear with any two points of K_T . Actually, a stronger statement holds.

Proposition 21. *Let $a, b \in \mathbb{F}_q$ be such that*

$$(a, b) \in \left\{ \left(0, -\frac{9}{8\beta^2}\right), (\beta\sqrt{-3}, 0), (-\beta\sqrt{-3}, 0) \right\}.$$

Then the point $P = (a, b)$ is not collinear with any two \mathbb{F}_q -rational affine points of \mathcal{X} .

Proof. We recall that by the proof of Lemma 11, the point P is collinear with $(x, \frac{1}{x^2 - \beta^2})$ and $(y, \frac{1}{y^2 - \beta^2})$, with $x, y \in \mathbb{F}_q$, if and only if $g_{a,b}(x, y) = 0$. If $(a, b) = (0, -\frac{9}{8\beta^2})$ then

$$g_{a,b}(X, Y) = -\frac{1}{8\beta^2}(9X^2Y^2 - \beta^2(X^2 + Y^2) + 8\beta^2XY + \beta^4) =$$

$$= -\frac{1}{8\beta^2}(3XY - X\beta + Y\beta + \beta^2)(3XY + X\beta - Y\beta + \beta^2).$$

If $g_{a,b}(x, y) = 0$, then either

$$(14) \quad 3xy - x\beta + y\beta + \beta^2 = 0 \quad \text{or} \quad 3xy + x\beta - y\beta + \beta^2 = 0.$$

If $(x, y) \in \mathbb{F}_q$, then both x and y are fixed by the Frobenius map over \mathbb{F}_q , and hence both equalities in (14) hold. This easily implies $x = y$. Then no two distinct \mathbb{F}_q -rational affine points of \mathcal{X} can be collinear with (a, b) .

Note that $(a, b) = (\pm\beta\sqrt{-3}, 0)$ can only occur when -3 is a non-square in \mathbb{F}_q , otherwise $\pm\beta\sqrt{-3} \notin \mathbb{F}_q$. In this case, $(\sqrt{-3})^q = -\sqrt{-3}$ holds; also,

$$\begin{aligned} g_{\beta\sqrt{-3},0}(X, Y) &= -(X^2 + Y^2) - XY + \beta\sqrt{-3}(X + Y) + \beta^2 = \\ &= -\left(X + \frac{1 + \sqrt{-3}}{2}Y + \frac{-\beta\sqrt{-3} + \beta}{2}\right)\left(X + \frac{1 - \sqrt{-3}}{2}Y + \frac{-\beta\sqrt{-3} - \beta}{2}\right) \end{aligned}$$

and

$$\begin{aligned} g_{-\beta\sqrt{-3},0}(X, Y) &= -(X^2 + Y^2) - XY - \beta\sqrt{-3}(X + Y) + \beta^2 = \\ &= -\left(X + \frac{1 - \sqrt{-3}}{2}Y + \frac{\beta\sqrt{-3} + \beta}{2}\right)\left(X + \frac{1 + \sqrt{-3}}{2}Y + \frac{\beta\sqrt{-3} - \beta}{2}\right) \end{aligned}$$

The assertion for $(a, b) = (\pm\beta\sqrt{-3}, 0)$ then follows by the same arguments used for $(a, b) = (0, -\frac{9}{8\beta^2})$. \square

In order to investigate the bicovery properties of the arc K_t , according to Remark 17 we need to consider the rational function $(a - \frac{h(\bar{r})}{l(\bar{r})})(a - \frac{h(\bar{v})}{l(\bar{v})})$ in the function field of $M_{a,b,\bar{l},m}(R, V) = 0$.

Lemma 22. *Let $P = (a, b)$ be a point in $AG(2, q)$ off \mathcal{X} satisfying (10). Let $\mathbb{K}(\bar{r}, \bar{v})$ be the function field of $M_{a,b,\bar{l},m}(R, V) = 0$, so that $M_{a,b,\bar{l},m}(\bar{r}, \bar{v}) = 0$. Then the rational function $(a - \frac{h(\bar{r})}{l(\bar{r})})(a - \frac{h(\bar{v})}{l(\bar{v})})$ is not a square in $\mathbb{K}(\bar{r}, \bar{v})$.*

Proof. Let \bar{x} and \bar{y} be as in the proof of Proposition 19, so that $\mathbb{K}(\bar{r}, \bar{v}) = \mathbb{K}(\bar{x}, \bar{y})$ with $f_{A,B,\bar{l},m}(\bar{x}, \bar{y}) = 0$. By straightforward computation,

$$\left(a - \frac{h(\bar{r})}{l(\bar{r})}\right)\left(a - \frac{h(\bar{v})}{l(\bar{v})}\right) = \frac{4\beta^2(\bar{t}\bar{x}^m - A)(\bar{t}\bar{y}^m - A)}{(A - 1)^2(\bar{t}\bar{x}^m - 1)(\bar{t}\bar{y}^m - 1)}.$$

Then the assertion follows from Proposition 10. \square

Proposition 23. *Let $P = (a, b)$ be a point in $AG(2, q)$ off \mathcal{X} . Assume that (10) holds. If*

$$(15) \quad q + 1 - (16m^2 - 8m + 2)\sqrt{q} \geq 16m^2 + 24m + 1$$

then P is bicoveryed by the points of K_T .

Proof. Let $\mathbb{K}(\bar{r}, \bar{v})$ be the function field of $M_{a,b,\bar{t},m}(R, V) = 0$, so that $M_{a,b,\bar{t},m}(\bar{r}, \bar{v}) = 0$. By Proposition 10 and Lemma 22, for every $c \in \mathbb{F}_q^*$ the equation

$$\bar{w}^2 = c \left(a - \frac{h(\bar{r})}{l(\bar{r})} \right) \left(a - \frac{h(\bar{v})}{l(\bar{v})} \right)$$

defines a Kummer extension $\mathbb{K}(\bar{r}, \bar{v}, \bar{w})$ of $\mathbb{K}(\bar{r}, \bar{v})$ with genus less than or equal to $8m^2 - 4m + 1$. Let E be as in the proof of Proposition 19, and let E' be the set of places of $\mathbb{K}(\bar{r}, \bar{v}, \bar{w})$ that either lie over a place in E or over a zero or a pole of $(a - \frac{h(\bar{r})}{l(\bar{r})})(a - \frac{h(\bar{v})}{l(\bar{v})})$. By Proposition 10, together with the proof of Proposition 19, an upper bound for the size of E' is $16m^2 + 24m$. Our assumption on q and m , together with Proposition 3, ensures the existence of at least $16m^2 + 24m + 1$ \mathbb{F}_q -rational places of $\mathbb{K}(\bar{r}, \bar{v}, \bar{w})$; hence, there exists at least one \mathbb{F}_q -rational place γ_c of $\mathbb{K}(\bar{r}, \bar{v}, \bar{w})$ not in E' . Let

$$\tilde{r} = \bar{r}(\gamma_c), \quad \tilde{v} = \bar{v}(\gamma_c), \quad \tilde{w} = \bar{w}(\gamma_c).$$

Note that $P_c = (\tilde{r}, \tilde{v})$ is an \mathbb{F}_q -rational affine point of the curve with equation $M_{a,b,\bar{t},m}(R, V) = 0$. Therefore, by Remark 18, P is collinear with two distinct points

$$P_{1,c} = Q_{\bar{t}(\frac{\tilde{r}+\beta}{\tilde{r}-\beta})^m}, \quad P_{2,c} = Q_{\bar{t}(\frac{\tilde{v}+\beta}{\tilde{v}-\beta})^m} \in K_T.$$

If c is chosen to be a square, then P is external to $P_{1,c}P_{2,c}$; on the other hand, if c is not a square, then P is internal to $P_{1,c}P_{2,c}$. This proves the assertion. \square

In the final part of this section we deal with points in \mathcal{X} .

Proposition 24. *Let $K_{T'}$ be a coset of K such that $K_T \cup K_{T'}$ is an arc. For $u \in \mathbb{F}_q$, let $P_u = (u, \frac{1}{u^2 - \beta^2})$ be an \mathbb{F}_q -rational affine point of \mathcal{X} not belonging to $K_T \cup K_{T'}$ but collinear with a point of K_T and a point of $K_{T'}$.*

- (i) *If $u \neq 0$ and (15) holds, then P_u is biconvered by $K_T \cup K_{T'}$.*
- (ii) *The point $P_0 = (0, -\frac{1}{\beta^2})$ is not biconvered by $K_T \cup K_{T'}$. It is internal (resp. external) to every segment cut out on $K_T \cup K_{T'}$ by a line through P_0 when $q \equiv 1 \pmod{4}$ (resp. $q \equiv 3 \pmod{4}$).*

Proof. Note that when P ranges over K_T , then the point $Q = \ominus(P_u \oplus P)$ ranges over $K_{T'}$ and is collinear with P_u and P . Recall that P belongs to K_T if and only if $P = (e, \frac{1}{e^2 - \beta^2})$ with

$$e = \beta \frac{\bar{t}(\frac{x+\beta}{x-\beta})^m + 1}{\bar{t}(\frac{x+\beta}{x-\beta})^m - 1}$$

for some $x \in \mathbb{F}_q$. In this case, $Q = (s(e), \frac{1}{s(e)^2 - \beta^2})$ with $s(e) = -\frac{ue + \beta^2}{u + e}$. For an element \bar{x} transcendental over \mathbb{K} let

$$e(\bar{x}) = \beta \frac{\bar{t}(\frac{\bar{x}+\beta}{\bar{x}-\beta})^m + 1}{\bar{t}(\frac{\bar{x}+\beta}{\bar{x}-\beta})^m - 1} = \frac{\beta \bar{t}(\bar{x} + \beta)^m + \beta(\bar{x} - \beta)^m}{\bar{t}(\bar{x} + \beta)^m - (\bar{x} - \beta)^m} \in \mathbb{K}(\bar{x}).$$

Note that $e(\bar{x})$ is defined over \mathbb{F}_q . In order to determine whether P_u is biconvered by $K_T \cup K_{T'}$ we need to investigate whether the following rational function is a square in $\mathbb{K}(\bar{x})$:

$$\eta(\bar{x}) = (u - e(\bar{x}))(u - s(e(\bar{x}))) = \frac{u - e(\bar{x})}{u + e(\bar{x})}(u^2 + 2ue(\bar{x}) + \beta^2)$$

Let γ be a zero of $\bar{t}(\frac{\bar{x}+\beta}{\bar{x}-\beta})^m - 1$ in $\mathbb{K}(\bar{x})$. Note that since $(m, p) = 1$, the polynomial $tZ^m - 1$ has no multiple roots in $\mathbb{K}[Z]$. Then the valuation $v_\gamma(e(\bar{x}))$ of $e(\bar{x})$ at γ is -1 . If in addition $u \neq 0$, then $v_\gamma(\eta(\bar{x})) = v_\gamma(e(\bar{x})) = -1$, whence $\eta(\bar{x})$ is not a square in $\mathbb{K}(\bar{x})$ and Proposition 2 applies to $c\eta(\bar{x})$ for each $c \in \mathbb{F}_q^*$. Since the number of poles of $\eta(\bar{x})$ is at most $2m$, the genus of the Kummer extension $\mathbb{K}(\bar{x}, \bar{w})$ of $\mathbb{K}(\bar{x})$ with $\bar{w}^2 = c\eta(\bar{x})$ is at most $2m - 1$.

Our assumption on q , together with the Hasse-Weil bound, yield the existence of an \mathbb{F}_q -rational place γ_c of $\mathbb{K}(\bar{x}, \bar{w})$ which is not a zero nor a pole of \bar{w} . Let $\tilde{x} = \bar{x}(\gamma_c)$, $\tilde{w} = \bar{w}(\gamma_c)$,

$$\tilde{e} = \beta \frac{\bar{t}(\frac{\tilde{x}+\beta}{\tilde{x}-\beta})^m + 1}{\bar{t}(\frac{\tilde{x}+\beta}{\tilde{x}-\beta})^m - 1} \quad \text{and} \quad s(\tilde{e}) = -\frac{u\tilde{e} + \beta^2}{u + \tilde{e}}.$$

Therefore, if $u \neq 0$, then P_u is collinear with two distinct points

$$P(c) = \left(\tilde{e}, \frac{1}{\tilde{e}^2 - \beta^2} \right) \in K_T \quad Q(c) = \left(s(\tilde{e}), \frac{1}{s(\tilde{e})^2 - \beta^2} \right) \in K_{T'}.$$

If c is chosen to be a square, then P_u is external to $P(c)Q(c)$; on the other hand, if c is not a square, then P_u is internal to $P(c)Q(c)$.

Assume now that $u = 0$. First note that P_0 coincides with Q_{-1} , and hence belongs to K . Therefore, as m is odd, P_0 cannot be collinear with any two points from the same coset of K . Assume then that P_0 is collinear with $P = (e, \frac{1}{e^2 - \beta^2}) \in K_T$ and $Q = (s(e), \frac{1}{s(e)^2 - \beta^2}) \in K_{T'}$. It is straightforward to check that $(u - e)(u - s(e)) = e \cdot s(e) = -\beta^2$. Since β^2 is not a square in \mathbb{F}_q , the assertion follows from the well-known fact that -1 is a square in \mathbb{F}_q precisely when $q \equiv 1 \pmod{4}$. \square

5. COMPLETE ARCS AND COMPLETE CAPS FROM CUBICS WITH AN ISOLATED DOUBLE POINT

Throughout this section $q = p^s$ with p a prime, $p > 3$. Also, \mathcal{X} , G , m , K and K_T are as in Section 4.

We recall the notion of a maximal-3-independent subset of a finite abelian group \mathcal{G} , as given in [26]. A subset M of \mathcal{G} is said to be *maximal 3-independent* if

- (a) $x_1 + x_2 + x_3 \neq 0$ for all $x_1, x_2, x_3 \in M$, and
- (b) for each $y \in \mathcal{G} \setminus M$ there exist $x_1, x_2 \in M$ with $x_1 + x_2 + y = 0$.

If in (b) $x_1 \neq x_2$ can be assumed, then M is said to be *good*.

Assume that S is a good maximal 3-independent subset of G . Since three points in G are collinear if and only if their sum is equal to the neutral element, S is an arc whose secants cover all the points in G .

For direct products of abelian groups of order at least 4, an explicit construction of good maximal 3-independent subsets was provided by Szőnyi; see e.g. [23, Example 1.2]. If m and $(q + 1)/m$ are coprime, such a construction applies to G .

Proposition 25. *Assume that m and $(q + 1)/m$ are coprime. Let H be the subgroup of G of order m , so that G is the direct product of K and H . Fix two elements $R \in K$ and $R' \in H$ of order greater than 3, and let $T = R' \oplus 2R$. Then*

$$\mathcal{A} = K_T \setminus \{T\} \bigcup (H \oplus R) \setminus \{\oplus 2T \oplus R\}$$

is a good maximal 3-independent subset of G .

Let \mathcal{E} denote the set of points P in $AG(2, q) \setminus \mathcal{X}$ whose affine coordinates (a, b) do not satisfy (10). By Remark 14, the size of \mathcal{E} is 3 precisely when s is odd and $p \equiv 2 \pmod{3}$; otherwise, \mathcal{E} consists of the point with coordinates $(0, -\frac{9}{8\beta^2})$.

5.1. Small complete arcs in $AG(2, q)$. Let \mathcal{A} be as in Proposition 25. We use Propositions 20, 21, and 25 in order to construct small complete arcs in Galois planes. Note that (13) is implied by $m \leq \frac{\sqrt[4]{q}}{\sqrt{6}}$.

Theorem 26. *Let $q = p^s$ with $p > 3$ a prime. Let m be a divisor of $q+1$ such that $(m, 6) = 1$ and $(m, \frac{q+1}{m}) = 1$. If $m \leq \frac{\sqrt[4]{q}}{\sqrt{6}}$, then*

- *if either s is even or $p \equiv 1 \pmod{3}$, the set $\mathcal{A} \cup \mathcal{E}$ is a complete arc in $AG(2, q)$ of size $m + \frac{q+1}{m} - 2$;*
- *if s is odd and $p \equiv 2 \pmod{3}$, the set $\mathcal{A} \cup \mathcal{E}$ contains a complete arc in $AG(2, q)$ of size at most $m + \frac{q+1}{m}$.*

5.2. Small complete caps in $AG(N, q)$, $N \equiv 0 \pmod{4}$. Let M be a maximal 3-independent subset of the factor group G/K containing K_T . Then the union S of the cosets of K corresponding to M is a good maximal 3-independent subset of G ; see [26], Lemma 1, together with Remark 5(5). It has already been noticed that S is an arc whose secants cover all the points in G . Note also that K is disjoint from S , and hence the point $P_0 = (0, -\frac{1}{\beta^2})$ does not belong to S .

If either s is even or $p \equiv 1 \pmod{3}$, by Propositions 21, 23, and 24, then $S \cup \{(0, -\frac{9}{8\beta^2})\}$ is an almost bicovering arc with center P_0 , provided that m is small enough with respect to q .

Theorem 27. *Let $q = p^s$ with $p > 3$ a prime, and assume that either s is even or $p \equiv 1 \pmod{3}$. Let m be a proper divisor of $q+1$ such that $(m, 6) = 1$ and (15) holds. Let K be the subgroup of G of index m . For M a maximal 3-independent subset of the factor group G/K , the point set*

$$(16) \quad \mathcal{B} = \left(\bigcup_{K_{T_i} \in M} K_{T_i} \right) \bigcup \mathcal{E}$$

is an almost bicovering arc in $AG(2, q)$ with center $P_0 = (0, -\frac{1}{\beta^2})$. The size of \mathcal{B} is $\#M \cdot \frac{q+1}{m} + 1$.

When s is odd and $p \equiv 2 \pmod{3}$ a further condition on M is needed in order to ensure that \mathcal{B} as in (16) is an almost bicovering arc. Note that by Proposition 21 there is precisely one point in G collinear with any two points in \mathcal{E} .

Theorem 28. *Let $q = p^s$ with $p > 3$ a prime. Assume that s is odd and $p \equiv 2 \pmod{3}$. Let m be a proper divisor of $q+1$ such that $(m, 6) = 1$ and (15) holds. Let K be the subgroup of G of index m . Let Q_1 denote the only point in G collinear with $(0, -\frac{9}{8\beta^2})$ and $(\beta\sqrt{-3}, 0)$; similarly, let $Q_2 \in G$ be collinear with $(0, -\frac{9}{8\beta^2})$ and $(-\beta\sqrt{-3}, 0)$. For M a maximal 3-independent subset of the factor group G/K not containing $K \oplus Q_1$ nor $K \oplus Q_2$, the point*

set

$$\mathcal{B} = \left(\bigcup_{K_{T_i} \in M} K_{T_i} \right) \bigcup \mathcal{E}$$

is an almost bicovering arc in $AG(2, q)$ with center $P_0 = (0, -\frac{1}{\beta^2})$. The size of \mathcal{B} is $\#M \cdot \frac{q+1}{m} + 3$.

We use Theorems 27 and 28, together with Proposition 5, in order to construct small complete caps in affine spaces $AG(N, q)$. Assume that $m = m_1 m_2$ with $(m_1, m_2) = 1$. Then the factor group G/K is the direct product of two subgroups of order $m_1 > 4$ and $m_2 > 4$, and the aforementioned construction by Szőnyi [23, Example 1.2] of a maximal 3-independent set M of size $m_1 + m_2 - 3$ applies. It is easily seen that M can be chosen in such a way that it does not contain any two fixed cosets of K . As (15) is implied by $m \leq \frac{\sqrt[4]{q}}{4}$, the following result holds.

Theorem 29. *Let $q = p^h$ with $p > 3$, and let m be a proper divisor of $q + 1$ such that $(m, 6) = 1$ and $m \leq \frac{\sqrt[4]{q}}{4}$. Assume that $m = m_1 m_2$ with $(m_1, m_2) = 1$. Then for $N \equiv 0 \pmod{4}$, $N \geq 4$, there exists a complete cap in $AG(N, q)$ of size less than or equal to*

$$\left((m_1 + m_2 - 3) \cdot \frac{q + 1}{m} + 3 \right) q^{\frac{N-2}{2}}.$$

REFERENCES

- [1] Nurdagül Anbar, Daniele Bartoli, Massimo Giulietti, and Irene Platoni. Small complete caps from singular cubics. Submitted, 2013.
- [2] Nurdagül Anbar, Daniele Bartoli, Massimo Giulietti, and Irene Platoni. Small complete caps from nodal cubics. Submitted, 2013. arXiv:1305.3019 [math.CO].
- [3] Nurdagül Anbar and Massimo Giulietti. Bicovering arcs and small complete caps from elliptic curves. *J. Algebraic Combin.* In press. Published online October 2012. DOI: 10.1007/s10801-012-0407-8.
- [4] Daniele Bartoli, Giorgio Faina, and Massimo Giulietti. Small complete caps in three-dimensional Galois spaces. Submitted, 2013.
- [5] Alexander A. Davydov, Massimo Giulietti, Stefano Marcugini, and Fernanda Pambianco. New inductive constructions of complete caps in $PG(N, q)$, q even. *J. Combin. Des.*, 18(3):177–201, 2010.
- [6] Alexander A. Davydov and Patric R. J. Östergård. Recursive constructions of complete caps. *J. Statist. Plann. Inference*, 95(1-2):167–173, 2001. Special issue on design combinatorics: in honor of S. S. Shrikhande.
- [7] Giorgio Faina, Fabio Pasticci, and Lorenzo Schmidt. Small complete caps in Galois spaces. *Ars Combin.*, 105:299–303, 2012.
- [8] Stefania Fanali and Massimo Giulietti. On the number of rational points of generalized fermat curves over finite fields. *Int. J. Number Theory*, 8(4):1087–1097, 2012.
- [9] Massimo Giulietti. On plane arcs contained in cubic curves. *Finite Fields Appl.*, 8:69–90, 2002.
- [10] Massimo Giulietti. Small complete caps in Galois affine spaces. *J. Algebraic Combin.*, 25(2):149–168, 2007.
- [11] Massimo Giulietti. Small complete caps in $PG(N, q)$, q even. *J. Combin. Des.*, 15(5):420–436, 2007.
- [12] Massimo Giulietti and Fabio Pasticci. Quasi-Perfect Linear Codes With Minimum Distance 4. *IEEE Trans. Inform. Theory*, 53(5): 1928–1935, 2007.
- [13] James W. P. Hirschfeld and Leo Storme. The packing problem in statistics, coding theory and finite projective spaces. *J. Statist. Plann. Inference*, 72(1-2):355–380, 1998. R. C. Bose Memorial Conference (Fort Collins, CO, 1995).
- [14] James W. P. Hirschfeld and Leo Storme, *The packing problem in statistics, coding theory, and finite projective spaces*: update 2001, in: Finite Geometries, Proceedings of the Fourth Isle of Thorns Conference,

- A. Blokhuis, J. W. P. Hirschfeld, D. Jungnickel and J. A. Thas, Eds., *Developments in Mathematics* 3, Kluwer Academic Publishers, Boston, (2000), 201-246.
- [15] James W. P. Hirschfeld and José Felipe Voloch. The characterisation of elliptic curves over finite fields. *J. Austral. Math. Soc. Ser. A*, 45: 275–286, 1988.
 - [16] Lucio Lombardo-Radice. Sul problema dei k -archi completi in $S_{2,q}$. ($q = p^t$, p primo dispari.). *Boll. Un. Mat. Ital. (3)*, 11:178–181, 1956.
 - [17] Fernanda Pambianco and Leo Storme. Small complete caps in spaces of even characteristic. *J. Combin. Theory Ser. A*, 75(1):70–84, 1996.
 - [18] Beniamino Segre. Ovali e curve σ nei piani di Galois di caratteristica due. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. (8)*, 32:785–790, 1962.
 - [19] Beniamino Segre. Introduction to Galois geometries. *Atti Accad. Naz. Lincei Mem. Cl. Sci. Fis. Mat. Natur. Sez. I (8)*, 8:133–236, 1967.
 - [20] Beniamino Segre. Proprietà elementari relative ai segmenti ed alle coniche sopra un campo qualsiasi ed una congettura di Seppo Ilkka per il caso dei campi di Galois. *Ann. Mat. Pura Appl. (4)*, 96:289–337, 1972.
 - [21] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.
 - [22] Tamás Szőnyi. Small complete arcs in Galois planes. *Geom. Dedicata*, 18(2):161–172, 1985.
 - [23] Tamás Szőnyi. Arcs in cubic curves and 3-independent subsets of abelian groups. In *Combinatorics (Eger, 1987)*, volume 52 of *Colloq. Math. Soc. János Bolyai*, pages 499–508. North-Holland, Amsterdam, 1988.
 - [24] Tamás Szőnyi. Complete arcs in Galois planes: a survey. Quaderni del Seminario di Geometrie Combinatorie 94, Dipartimento di Matematica “G. Castelnuovo”, Università degli Studi di Roma “La Sapienza”, Roma, January 1989.
 - [25] José Felipe Voloch. On the completeness of certain plane arcs, *European J. Combin.*, 8:453–456, 1987.
 - [26] José Felipe Voloch. On the completeness of certain plane arcs. II. *European J. Combin.*, 11(5):491–496, 1990.
 - [27] Francesco Ziriilli. Su una classe di k -archi di un piano di Galois, *Atti Accad. Naz. Lincei Rend.* 54:393–397, 1973.

E-mail address: nurdagul@su.sabanciuniv.edu

E-mail address: bartoli@dmf.unipg.it

E-mail address: giuliet@dmf.unipg.it

E-mail address: irene.platoni@unitn.it