J Algebr Comb (2013) 38:371–392
DOI 10.1007/s10801-012-0407-8

Bicovering arcs and small complete caps from elliptic curves

Nurdagül Anbar · Massimo Giulietti

Received: 6 April 2012 / Accepted: 15 October 2012 / Published online: 25 October 2012

Abstract Bicovering arcs in Galois affine planes of odd order are a powerful tool for the construction of complete caps in spaces of arbitrarily higher dimensions. The aim of this paper is to investigate whether the arcs contained in elliptic cubic curves are bicovering. As a result, bicovering k-arcs in $AG(2,q)$ of size $k \le q/3$ are obtained, provided that $q-1$ has a prime divisor m with $7 < m < (1/8)q^{1/4}$. Such arcs produce complete caps of size $kq^{(N-2)/2}$ in affine spaces of dimension $N \equiv 0 \pmod 4$. When $q = p^h$ with p prime and $h \le 8$, these caps are the smallest known complete caps in $AG(N,q)$, $N \equiv 0 \pmod 4$.

Keywords Galois affine spaces · Bicovering arcs · Complete caps · Quasi-perfect codes · Elliptic curves

1 Introduction

In an (affine or projective) space of dimension $N \ge 2$ over the finite field with q elements $\mathbb{F}_q$, a *k-cap* is a set of k points no three of which are collinear. A k-cap is said to be *complete* if its secants cover all the points of the space. In the plane, that is for $N = 2$, k-caps are also called *k-arcs*. The general theory of k-caps was developed in the 1960s by the pioneering work of Segre; see [20]. Ever since, k-caps and their

N. Anbar
Faculty of Engineering and Natural Sciences, Sabanci University, Orhanli-Tuzla, 34956 Istanbul, Turkey
e-mail: nurdagul@su.sabanciuniv.edu

M. Giulietti (✉)
Dipartimento di Matematica e Informatica, University of Perugia, Via Vanvitelli 1, 06123 Perugia, Italy
e-mail: giuliet@dmi.unipg.it

generalizations, especially (k,d)-arcs, saturating sets and k-arcs in higher dimensions, have played an important role in Finite Geometry; see [10, 11, 14]. All these objects are relevant not only in Finite Geometry but also in Coding Theory, being the geometrical counterpart of distinguished types of error-correcting and covering linear code, such as MDS codes, Near MDS codes, and quasi-perfect codes with minimum distance 4.

In this direction, an important issue is to ask for explicit constructions of complete k-caps in higher dimensional spaces. Since the theory of plane k-arcs is well developed and quite rich of constructions, the natural idea is to try to use some kind of lifting methods for plane k-arcs to obtain complete caps in higher dimension.

For this purpose, bicovering arcs in affine planes have recently emerged as a potential powerful tool. Here, a k-arc A in the affine plane $AG(2,q)$, q odd, is said to be *bicovering* if its completeness holds in a stronger sense: it is required that every point P off A is covered by at least two secants of A, in such a way that P is external to the segment cut out by one of the secants but it is internal when the other secant is considered (cf. Definition 1). Complete caps from bicovering arcs can be obtained via the product method for caps; see Proposition 1.

To establish whether a complete arc is bicovering can be a difficult task. In the simplest case where the arc A consists of the affine points of an irreducible conic, if q is large enough then A bicovers all the points off A with at most one exception. This follows from previous results by Segre [21]. Beside some computer assisted constructions for small q's [4], the only other known examples of bicovering or almost bicovering arcs are some arcs arising from singular cubic curves. In [7] it is shown that if $q > 76^2$, then a certain subset of $(q-3)/2$ $\mathbb{F}_q$-rational points of a singular cubic curve is a bicovering arc. Cosets of subgroups of the abelian group of the non-singular $\mathbb{F}_q$-rational points of a singular cubic with a cusp are considered in [1].

In this paper, we deal with the non-singular (or elliptic) case. We investigate the bicovering properties of the arcs arising from cosets of the abelian group $G = (\mathcal{X}(\mathbb{F}_q), \oplus)$ of the set of $\mathbb{F}_q$-rational points of a non-singular cubic curve $\mathcal{X}$ defined over $\mathbb{F}_q$. Such arcs were introduced by Voloch in [26], and were the main ingredient of some constructions of small complete arcs due to Szőnyi [23, 24]. Their construction relies on the notion of a maximal 3-independent subset of abelian groups. According to [26], a subset X of a finite abelian group G is said to be *maximal 3-independent* if (a) $x_1 + x_2 + x_3 \neq 0$ for all $x_1, x_2, x_3 \in X$, and (b) for each $y \in G \setminus X$ there exist $x_1, x_2 \in X$ with $x_1 + x_2 + y = 0$. Our main achievement is Theorem 1.

Theorem 1 *For an odd prime power q, let m be a prime divisor of $q-1$, with $7 < m < \frac{1}{8}\sqrt[4]{q}$. Assume that the finite group of order m admits a maximal 3-independent subset of size s. Then there exists a bicovering k-arc in $AG(2,q)$ with*

$$s \cdot \left\lfloor \frac{q - 2\sqrt{q} + 1}{m} \right\rfloor \leq k \leq s \cdot \left(\left\lfloor \frac{q - 2\sqrt{q} + 1}{m} \right\rfloor + 31 \right),$$

consisting of the union of s cosets of a subgroup of index m of the abelian group of the $\mathbb{F}_q$-rational points of a non-singular plane cubic curve.

The proof of Theorem 1 heavily relies on concepts and results from Algebraic Geometry in positive characteristic; see Propositions 2, 4, 6, 7 and 8. It should be noted that Proposition 6 fills a gap in the proof of a major result in [26] on the completeness of the arcs arising from cosets of subgroups of index m of G, in the case where m is a prime dividing $q-1$, see Remark 4.

It has been shown in [26] that if $m > 7$ is a prime, then there always exists a maximal 3-independent subset of size $s \le (m+1)/3$ in the finite group of order m. Then a straightforward corollary to Theorem 1 and Proposition 1 is the following result on complete caps.

Theorem 2 *For an odd prime power q, let m be a prime divisor of $q-1$, with $7 < m < \frac{1}{8}\sqrt[4]{q}$. Assume that the finite group of order m admits a maximal 3-independent subset of size s. Then for any positive integer $N \equiv 0 \pmod 4$, there exists a complete cap in $AG(N,q)$ of size k with*

$$s \cdot q^{\frac{N-2}{2}} \cdot \left\lfloor \frac{q-2\sqrt{q}+1}{m} \right\rfloor \le k \le s \cdot q^{\frac{N-2}{2}} \cdot \left(\left\lfloor \frac{q-2\sqrt{q}+1}{m} \right\rfloor + 31 \right).$$

In particular, in $AG(N,q)$, $N \equiv 0 \pmod 4$, there exists a complete cap of size less than or equal to

$$\frac{m+1}{3} \cdot q^{\frac{N-2}{2}} \cdot \left(\left\lfloor \frac{q-2\sqrt{q}+1}{m} \right\rfloor + 31 \right) \sim \frac{1}{3} q^{N/2}.$$

Theorem 2 is of particular relevance in the context of small complete caps in Galois spaces, which are the geometrical counterpart of quasi-perfect 3-error-detecting linear codes with small density (see [2, 3, 13] and the references therein). For the size of the smallest complete cap in $AG(N,q)$ the trivial lower bound is $\sqrt{2}q^{(N-1)/2}$. Complete caps of size about $cq^{\frac{N-1}{2}}$, with c a constant less than 3, are known to exist for q even and N odd [3, 8, 9, 18]. On the other hand, when either q is odd or N is even, constructions of complete caps of size less than $q^{N/2}$ are quite rare. Theorem 2 yields the existence of complete caps in $AG(N,q)$ of size of the same order of magnitude as $cq^{N/2}$ with $c \le 1/3$, provided that $q-1$ has a prime divisor m greater than 7 and smaller than $\sqrt[4]{q}/8$. For specific values of m, the upper bound on c can be improved, as there exist maximal 3-independent subsets of the finite group of order m of size significantly less than $m/3$, see Propositions 10 and 11.

The paper is organized as follows. In Sect. 2 we review some of the standard facts on algebraic function fields. We also briefly sketch the connection between complete caps and bicovering arcs; moreover, we summarize without proofs the material on plane algebraic curves that will be relevant to our proofs. Section 3 presents preliminary results on some covers of low degree of non-singular plane cubic curves defined over a finite field. The proof that under the assumptions of Theorem 1 each point P_0 not on $\mathcal{X}$ is bicovered by a coset of a subgroup of index m in G is the object of Sect. 4, see Theorem 4. In Sect. 5 we deal with the case $P_0 \in \mathcal{X}$. The proof of our main result is completed in Sect. 6.

2 Notation and preliminaries

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

2.1 Complete caps from bicovering arcs

Throughout this section, N is assumed to be a positive integer divisible by 4. Let $q' = q^{(N-2)/2}$. 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 A in $AG(2,q)$, let

$$C_A = \left\{ \left(\alpha, \alpha^2, u, v\right) \in AG(N,q) \;\middle|\; \alpha \in \mathbb{F}_{q'},\ (u,v) \in A \right\}.$$

As noticed in [7], the set C_A is a cap whose completeness in $AG(N,q)$ depends on whether the completeness of A in $AG(2,q)$ holds in a stronger sense, see Proposition 1 below. According to Segre [21], 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

$$(x - x_1)(x - x_2) \quad \text{is a non-zero square or a non-square in } \mathbb{F}_q, \tag{1}$$

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 1 Let A be a complete arc in $AG(2,q)$. A point $P \in AG(2,q) \setminus A$ is said to be *bicovered* by A if there exist $P_1, P_2, P_3, P_4 \in A$ such that P is external to the segment P_1P_2 and internal to the segment P_3P_4. If every $P \in AG(2,q) \setminus A$ is bicovered by A, then A is said to be a *bicovering* arc.

The following result is proven in [7].

Proposition 1 *If A is a bicovering k-arc, then C_A is a complete cap in $AG(N,q)$ of size $kq^{(N-2)/2}$.*

2.2 Curves and function fields

Throughout this paper, by curve we will mean a projective absolutely irreducible algebraic curve defined over $\mathbb{K}$. We recall that a *function field* over a field L is an extension F of L such that F is a finite algebraic extension of $L(\alpha)$, with α transcendental over L. For basic definitions on function fields we refer to [22].

To a curve $\mathcal{C}$ one can associate a function field over $\mathbb{K}$, namely the field of rational functions of $\mathcal{C}$, which will be denoted by $\mathbb{K}(\mathcal{C})$.

A curve $\mathcal{C}$ is *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 $\mathbb{F}_q$. This subfield is a function field over $\mathbb{F}_q$.

A place γ of $\mathbb{K}(\mathcal{C})$ determines a unique point of $\mathcal{C}$, called the *center* of γ. If $\mathcal{C}$ is non-singular, this correspondence is a bijection, and sometimes in this paper points of a non-singular curve $\mathcal{C}$ will be identified with places of $\mathbb{K}(\mathcal{C})$. If in addition $\mathcal{C}$ is defined over $\mathbb{F}_q$, then the places of $\mathbb{F}_q(\mathcal{C})$ correspond to the orbits of points of $\mathcal{C}$ under the q-Frobenius map. A place of $\mathbb{F}_q(\mathcal{C})$ is *rational* precisely when the corresponding orbit consists of a single point.

Given a place γ of $\mathbb{K}(\mathcal{C})$ and a rational function $\alpha \in \mathbb{K}(\mathcal{C})$ such that γ is not a pole of α, the image of α by the residue class map with respect to γ is $\alpha(\gamma) \in \mathbb{K}$. If $\mathcal{C}$ is defined over $\mathbb{F}_q$ the same definition can be given for a place γ of $\mathbb{F}_q(\mathcal{X})$ and $\alpha \in \mathbb{F}_q(\mathcal{X})$. In this case, $\alpha(\gamma)$ is an element of the residue class field of γ, which is a finite extension of $\mathbb{F}_q$. If γ is a rational place, then $\alpha(\gamma)$ belongs to $\mathbb{F}_q$.

Let F be a function field over $\mathbb{F}_q$. The *full constant field* of F (also called the *field of constants* of F) is the finite extension of $\mathbb{F}_q$ consisting of the elements in F that are algebraic over $\mathbb{F}_q$. It is contained in every residue class field with respect to a place of F. To a function field F over $\mathbb{F}_q$ whose full constant field is $\mathbb{F}_{q^m}$ one can associate a curve $\mathcal{C}$ defined over $\mathbb{F}_{q^m}$ (up to $\mathbb{F}_{q^m}$-birational equivalence) such that $\mathbb{F}_{q^m}(\mathcal{C})$ is $\mathbb{F}_{q^m}$-isomorphic to F. The genus of F as a function field coincides with the genus of $\mathcal{C}$ as a curve.

If F is a function field over $\mathbb{F}_q$ such that the full constant field of F is $\mathbb{F}_q$, then by the Hasse–Weil bound the number N of rational places of F satisfies

$$q + 1 - 2g\sqrt{q} \le N \le q + 1 + 2g\sqrt{q},$$

where g is the genus of F.

If F' is a finite extension of a function field 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, and $f(\gamma'|\gamma)$ the *relative degree* of γ' over γ, that is the degree of the extension of the residue class field of γ' over the residue class field of γ. By the Fundamental Equality ([22, Theorem 3.1.11]), for a place γ of F we have $\sum e(\gamma'|\gamma) f(\gamma'|\gamma) = \deg(F'/F)$, where γ' ranges over the places of F' lying over γ. If F is a function field over $\mathbb{F}_q$, then a rational place γ of F is said to *split completely* over F' if $e(\gamma'|\gamma) = f(\gamma'|\gamma) = 1$ for each γ' lying 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.

If F_1 and F_2 are finite extensions of a function field F over $\mathbb{F}_q$, then the *compositum* F_1F_2 is the subfield of the algebraic closure of F generated by F_1 and F_2. It is possible that the full constant field of F_1F_2 is a proper extension of $\mathbb{F}_q$, even when $\mathbb{F}_q$ is the full constant field of both F_1 and F_2. In order to investigate the full constant field of the compositum of two function fields, the following results can be useful.

Lemma 1 *Let F_1/F and F_2/F be finite separable extensions of a function field F. Assume that $\mathbb{F}_q$ is the full constant field of both F_1 and F_2. Let F' be the compositum of F_1 and F_2. Let γ' be a place of F' lying over the place γ of F, and set $\gamma_i := \gamma' \cap F_i$ for $i = 1, 2$. If*

$$e(\gamma_1|\gamma) = 1 \quad \textit{and} \quad e(\gamma_2|\gamma) = \deg(F_2/F),$$

then the full constant field of F' is $\mathbb{F}_q$.

Proof Note that

$$e\big(\gamma' \mid \gamma_1\big) \le \deg\big(F'/F_1\big) \le \deg(F_2/F).$$

By Abhyankar's Lemma (see e.g. [22, Theorem 3.9.1]) we have

$$e\big(\gamma'|\gamma\big) = \deg(F_2/F) = e\big(\gamma'|\gamma_1\big).$$

Therefore, both

$$\deg\big(F'/F_1\big) = \deg(F_2/F) \quad \text{and} \quad e\big(\gamma'|\gamma_1\big) = \deg\big(F'/F_1\big)$$

hold. From $e(\gamma'|\gamma_1) = \deg(F'/F_1)$ it is easy to deduce that there cannot exist any intermediate constant field extension between F_1 and F'. □

Lemma 2 *Let F_1/F and F_2/F be finite separable extensions of a function field F, and let F' be the compositum of F_1 and F_2. Assume that the full constant field of F is $\mathbb{F}_q$. If γ is a rational place of F splitting completely in both F_1/F and F_2/F, then the full constant field of F' is $\mathbb{F}_q$.*

Proof By [22, Proposition 3.9.6(b)], the place γ splits completely in F'/F. In particular, $f(\gamma'|\gamma) = 1$ holds for every place γ' of F' lying over γ. As γ is rational and the full constant field of F is $\mathbb{F}_q$, the residue class field of γ' is $\mathbb{F}_q$. This proves that the full constant field of F' is contained in $\mathbb{F}_q$. As $\mathbb{F}_q \subset F'$, the claim follows. □

2.3 Order and class of a place with respect to a plane model

Let $\mathcal{C}$ be the algebraic plane curve defined by the equation $f(X, Y) = 0$, where $f(X, Y)$ is an irreducible polynomial over the algebraically closed field $\mathbb{K}$, and let $\mathbb{K}(\mathcal{C})$ be the function field of $\mathcal{C}$. Let $\bar{x}$ and $\bar{y}$ denote the rational functions associated to the affine coordinates X and Y, respectively. Then $\mathbb{K}(\mathcal{C}) = \mathbb{K}(\bar{x}, \bar{y})$ with $f(\bar{x}, \bar{y}) = 0$. Let $\mathbb{P}_{\mathcal{C}}$ denote the set of all places of $\mathbb{K}(\mathcal{C})$, and let $\mathrm{Div}(\mathbb{K}(\mathcal{C}))$ be the *group of divisors* of $\mathbb{K}(\mathcal{C})$, that is the free abelian group generated by $\mathbb{P}_{\mathcal{C}}$.

Let $\mathcal{D}$ be the subset of $\mathrm{Div}(\mathbb{K}(\mathcal{C}))$ given by

$$\mathcal{D} := \big\{\mathrm{div}(a\bar{x} + b\bar{y} + c) + E \;\big|\; a, b, c \in \mathbb{K}, (a, b, c) \neq (0, 0, 0)\big\},$$

where

$$E = \sum_{\gamma \in \mathbb{P}_{\mathcal{C}}} e_\gamma \gamma, \quad \text{with } e_\gamma = -\min\big\{v_\gamma(\bar{x}), v_\gamma(\bar{y}), v_\gamma(1)\big\}.$$

This set $\mathcal{D}$ is a linear series, which is usually called the *linear series cut out by the lines* of $\mathbb{P}^2(\mathbb{K})$. For basic definitions on linear series we refer to [12]. There is a one-to-one correspondence between $\mathcal{D}$ and the set of all lines in $\mathbb{P}^2(\mathbb{K})$: a line ℓ with homogeneous equation $aX_0 + bX_1 + cX_2 = 0$ corresponds to the divisor $D(\ell) := \mathrm{div}(a\bar{x} + b\bar{y} + c) + E$.

For a place γ with $(\mathcal{D}, \gamma)$ order sequence $(0, j_1(\gamma), j_2(\gamma))$, and for every line ℓ, we have

$$v_\gamma\big(D(\ell)\big) \in \big\{0, j_1(\gamma), j_2(\gamma)\big\}.$$

A line ℓ passes through the center of γ if and only if $v_\gamma(D(\ell)) > 0$; also, there exists a unique line ℓ with $v_\gamma(D(\ell)) = j_2(\gamma)$, which is called the *tangent line of the place* γ. The tangent line of a place γ is one of the tangent lines of $\mathcal{C}$ at the center of γ. The integers $j_1(\gamma)$ and $j_2(\gamma) - j_1(\gamma)$ are called the *order* and the *class* of γ, respectively. A place with order equal to 1 is called a *linear* place of $\mathcal{C}$.

Theorem 3 *Let Q be a point of $\mathcal{C}$ and ℓ be a line in $\mathbb{P}^2(\mathbb{K})$. Then the sum*

$$\sum_{\gamma \text{ centered at } Q} v_\gamma\big(D(\ell)\big)$$

is equal to the intersection multiplicity $\mathrm{I}(Q, \mathcal{C} \cap \ell)$ of $\mathcal{C}$ and ℓ at Q.

If ℓ is a line through Q which is not a tangent of $\mathcal{C}$ at Q, then $v_\gamma(D(\ell)) = j_1(\gamma)$ for each place γ centered at Q. Therefore, if Q is an m-fold point of $\mathcal{C}$, then the sum of the orders of the places centered at Q coincides with m. Also, the number of places centered at Q is greater than or equal to the number of distinct tangents at Q.

3 On some covers of small degree of non-singular cubic curves

Let $\mathcal{X}$ be a plane elliptic curve with affine equation $Y^2 = g(X)$, with $g(X) = X^3 + AX^2 + BX + C$, $A, B, C \in \mathbb{F}_q$. As $\mathcal{X}$ is non-singular, the places of $\mathbb{K}(\mathcal{X})$ can be identified with the points of $\mathcal{X}$, and the rational places of $\mathbb{F}_q(\mathcal{X})$ with the points in $\mathcal{X}(\mathbb{F}_q)$. Assume that the j-invariant $j(\mathcal{X})$ of $\mathcal{X}$ is different from 0.

For a point $P_0 = (a, b) \in AG(2, q) \setminus \mathcal{X}$, let $\mathcal{Y}$ be the following space curve:

$$\mathcal{Y}: \begin{cases} \dfrac{1}{Z - X}\left(\left(\left(\dfrac{Y - b}{X - a}\right)(Z - a) + b\right)^2 - g(Z)\right) = 0 \\ \\ Y^2 - g(X) = 0. \end{cases}$$

It has been shown in [15] that the hypothesis $j(\mathcal{X}) \neq 0$ guarantees that $\mathcal{Y}$ is absolutely irreducible (and defined over $\mathbb{F}_q$); see also [5]. In [25] it has been observed that if $P = (\tilde{x}, \tilde{y}, \tilde{z})$ is an affine $\mathbb{F}_q$-rational point in $\mathcal{Y}$ with $\tilde{x} \neq a$, then $(\tilde{x}, \tilde{y})$ and $(\tilde{z}, ((\tilde{y} - b)/(\tilde{x} - a))(\tilde{z} - a) + b)$ are both $\mathbb{F}_q$-rational points of $\mathcal{X}$; moreover, if they are distinct, then the line passing through them contains P_0.

Let $\bar{x}$, $\bar{y}$ and $\bar{z}$ denote the rational functions on $\mathcal{Y}$ associated to the affine coordinates X, Y, Z.

Lemma 3 *The map $\phi : \mathbb{F}_q(\mathcal{Y}) \to \mathbb{F}_q(\mathcal{Y})$ fixing $\mathbb{F}_q$ elementwise and such that*

$$\bar{x} \mapsto \bar{z}, \qquad \bar{y} \mapsto \left(\frac{\bar{y} - b}{\bar{x} - a}\right)(\bar{z} - a) + b, \qquad \bar{z} \mapsto \bar{x}$$

is an involutory $\mathbb{F}_q$-automorphism of $\mathbb{F}_q(\mathcal{Y})$.

Proof It is straightforward to check that the equations of $\mathcal{Y}$ are satisfied by $(\bar{z}, (\frac{\bar{y}-b}{\bar{x}-a})(\bar{z}-a)+b, \bar{x})$. As

$$\left(\frac{((\frac{\bar{y}-b}{\bar{x}-a})(\bar{z}-a)+b)-b}{\bar{z}-a}\right)(\bar{x}-a)+b=\bar{y}$$

holds, the order of ϕ is 2. □

Lemma 4 (Theorem 5.1 in [15]) *The genus of $\mathcal{Y}$ is at most* 4.

Let E be the set of places γ of $\mathbb{K}(\mathcal{Y})$ for which at least one of the following holds:

- γ is a pole of one of the functions $\bar{x}, \bar{y}, \bar{z}$;
- $\bar{x}(\gamma)=a$;
- the line through (a,b) and $(\bar{x}(\gamma), \bar{y}(\gamma))$ is a tangent to $\mathcal{X}$.

Note that if $\gamma \notin E$, then $\bar{z}(\gamma) \neq a$ since $(a,b) \notin \mathcal{X}$ yields the result that $(\tilde{x}(\gamma), \tilde{y}(\gamma), a)$ cannot satisfy the equations of $\mathcal{Y}$ whenever $\tilde{x}(\gamma) \neq a$.

By the proof of [15, Theorem 5.1] (see also [6, Lemma 3.2]), we have an upper bound on the size of E.

Lemma 5 *The size of E is at most* 18.

Remark 1 If γ is a rational place of $\mathbb{F}_q(\mathcal{Y})$, $\gamma \notin E$, then let $\tilde{x}=\bar{x}(\gamma)$, $\tilde{y}=\bar{y}(\gamma)$, $\tilde{z}=\bar{z}(\gamma)$. It has already been pointed out that P_0 is collinear with $(\tilde{x}, \tilde{y})$ and $(\tilde{z}, (\frac{\tilde{y}-b}{\tilde{x}-a})(\tilde{z}-a)+b)$, which are distinct $\mathbb{F}_q$-rational points of $\mathcal{X}$. As $\gamma \notin E$, the line joining P_0 and $(\tilde{x}, \tilde{y})$ meets $\mathcal{X}$ in a third point $(\tilde{z}', (\frac{\tilde{y}-b}{\tilde{x}-a})(\tilde{z}'-a)+b)$, which lies in $\mathcal{X}(\mathbb{F}_q)$ as well. It is easily seen that $\tilde{z}'=\bar{z}(\gamma')$, where γ, γ' are the places of $\mathbb{F}_q(\mathcal{Y})$ lying over $(\tilde{x}, \tilde{y})$.

The aim of the remaining part of this section is to show that the equation $T^2 = c(\bar{x}-a)(\bar{z}-a)$, with c a non-zero element in $\mathbb{F}_q$, defines a double cover of $\mathbb{K}(\mathcal{Y})$. To this end, it will be useful to deal with a plane model of the space curve $\mathcal{Y}$. Let $\bar{x}'=\bar{x}-a$ and $\bar{z}'=\bar{z}-a$. Clearly, $\mathbb{K}(\bar{x}', \bar{z}')=\mathbb{K}(\bar{x}, \bar{z})$ holds.

Lemma 6 *If $b \neq 0$, then $\bar{y}$ belongs to $\mathbb{K}(\bar{x}, \bar{z})$. Moreover,*

$$H(\bar{x}, \bar{z})=0, \tag{2}$$

where $H(X,Z)$ is the polynomial

$$4b^2 g(X+a)Z^2 - \left(X^2Z^2 - XZ\left(2Aa+B+3a^2\right) - (X+Z)g(a) + b^2(X-Z)\right)^2.$$

Proof From

$$\left(\left(\frac{\bar{y}-b}{\bar{x}-a}\right)(\bar{z}-a)+b\right)^2 - g(\bar{z})=0$$

we obtain

$$\big((\bar{y}-b)\bar{z}'+b\bar{x}'\big)^2-g\big(\bar{z}'+a\big)\big(\bar{x}'\big)^2=0.$$

Then

$$\big(\bar{y}^2+b^2-2b\bar{y}\big)\big(\bar{z}'\big)^2+b^2\big(\bar{x}'\big)^2+2b\bar{x}'(\bar{y}-b)\bar{z}'-g\big(\bar{z}'+a\big)\big(\bar{x}'\big)^2=0.$$

Taking into account that $\bar{y}^2=g(\bar{x})=g(\bar{x}'+a)$ we get

$$2b\bar{y}\big(\bar{x}'\bar{z}'-\big(\bar{z}'\big)^2\big)=-\big(g\big(\bar{x}'+a\big)+b^2\big)\big(\bar{z}'\big)^2-b^2\big(\bar{x}'\big)^2+2b^2\bar{x}'\bar{z}'+g\big(\bar{z}'+a\big)\big(\bar{x}'\big)^2.$$

As $b\neq 0$, this proves that $\bar{y}\in\mathbb{K}(\bar{x}',\bar{z}')=\mathbb{K}(\bar{x},\bar{z})$. In order to find an equation involving $\bar{x}'$ and $\bar{z}'$ we take the square of both sides of the previous equation; then, we substitute $\bar{y}^2$ with $g(\bar{x}'+a)$ and divide both sides by $(\bar{x}'-\bar{z}')^2$, so that

$$4b^2g\big(\bar{x}'+a\big)\big(\bar{z}'\big)^2-\left(\frac{g(\bar{z}'+a)(\bar{x}')^2-g(\bar{x}'+a)(\bar{z}')^2}{\bar{x}'-\bar{z}'}-b^2\big(\bar{x}'-\bar{z}'\big)\right)^2=0.$$

By straightforward computation

$$\frac{g(\bar{z}'+a)(\bar{x}')^2-g(\bar{x}'+a)(\bar{z}')^2}{\bar{x}'-\bar{z}'}=-\big(\bar{x}'\bar{z}'\big)^2+\bar{x}'\bar{z}'\big(2Aa+B+3a^2\big)+\big(\bar{z}'+\bar{x}'\big)g(a),$$

whence (2) holds. □

Note that for $b\neq 0$, (2) defines an irreducible plane curve. In fact, the degree of the extension $\mathbb{K}(\bar{x},\bar{z}):\mathbb{K}(\bar{x})$ is equal to 4. This follows from $\mathbb{K}(\bar{x},\bar{z})=\mathbb{K}(\bar{x},\bar{y},\bar{z})=\mathbb{K}(\mathcal{Y})$, together with

$$\big[\mathbb{K}(\mathcal{Y}):\mathbb{K}(\bar{x})\big]=\big[\mathbb{K}(\mathcal{Y}):\mathbb{K}(\mathcal{X})\big]\cdot\big[\mathbb{K}(\mathcal{X}):\mathbb{K}(\bar{x})\big]=2\cdot 2=4.$$

If $b=0$, then by the proof of Lemma 6 it follows that

$$\big(\bar{x}'\bar{z}'\big)^2-\bar{x}'\bar{z}'\big(2Aa+B+3a^2\big)-\big(\bar{z}'+\bar{x}'\big)g(a)=0. \tag{3}$$

In particular, the degree of $\mathbb{K}(\bar{x},\bar{z})$ over $\mathbb{K}(\bar{x})$ is equal to 2.

From now on in this section we distinguish two cases, according to whether b is zero or not.

3.1 Case (1): $b\neq 0$

Let $\mathcal{C}$ be the irreducible plane curve with equation $H(X,Z)=0$, where $H(X,Z)$ is as in Lemma 6. By Lemma 6, $\mathcal{C}$ is an irreducible plane model of $\mathcal{Y}$.

In order to prove that $T^2=c(\bar{x}-a)(\bar{z}-a)=c\bar{x}'\bar{z}'$, with c a non-zero element in $\mathbb{F}_q$, defines a double cover of $\mathbb{K}(\mathcal{Y})\cong\mathbb{K}(\mathcal{C})$, we need to compute the divisors of the rational functions $\bar{x}'$ and $\bar{z}'$. Note that if $\bar{x}'$ and $\bar{z}'$ are viewed as rational functions of $\mathcal{C}$, then $\bar{x}'=X/T$ and $\bar{z}'=Z/T$.

It is straightforward to check that the only affine point that is the center of a zero of either $\bar{x}'$ or $\bar{z}'$ is $O := (0,0)$. Note that O is a double point of $\mathcal{C}$. One can check that up to the constant factor $(g(a) - b^2)$ the quadratic part of $H(X,Z)$ is

$$X^2\big(g(a) - b^2\big) + 2XZ\big(g(a) + b^2\big) + Z^2\big(g(a) - b^2\big).$$

Its discriminant is equal to

$$\big(g(a) + b^2\big)^2 - \big(g(a) - b^2\big)^2 = 4b^2 g(a).$$

If $g(a) \neq 0$, then O is a node and hence two distinct places of $\mathbb{K}(\mathcal{C})$ are centered at O. Otherwise, we have the only tangent $X - Z = 0$, and at this stage it is not possible to deduce the number of places centered at O.

The ideal points of $\mathcal{C}$ are clearly the infinite points of the X-axis and the Z-axis, say X_∞ and Z_∞. It is easily seen that they are both 4-fold points of $\mathcal{C}$. There is a unique tangent at both points: the line with equation $X = 0$ at Z_∞, and the line $Z = 0$ at X_∞. The intersection multiplicity of both of these tangents and $\mathcal{C}$ at their tangency point is equal to 6.

Write $v_P(\xi) = \sum_{\gamma \text{ centered at } P} v_\gamma(\xi)$. Then by Theorem 3 we have

$$v_O(X/T) = v_O(Z/T) = 2.$$

We investigate the valuations of $\bar{x}'$ and $\bar{z}'$ at the places centered at X_∞ and Z_∞. By Theorem 3, we have

$$v_{X_\infty}(X/T) = -4, \qquad v_{X_\infty}(Z/T) = 2,$$
$$v_{Z_\infty}(X/T) = 2, \qquad v_{Z_\infty}(Z/T) = -4.$$

Therefore,

$$v_O\big(XZ/T^2\big) = 4, \qquad v_{X_\infty}\big(XZ/T^2\big) = -2, \qquad v_{Z_\infty}\big(XZ/T^2\big) = -2.$$

Note that $Z = 0$ is the common tangent of all places centered at X_∞, and that similarly $X = 0$ is the common tangent of all places centered at Z_∞. Therefore, by Theorem 3, we have

$$\sum_{\gamma \in \mathbb{P}_\mathcal{C}, \gamma \text{ centered at } X_\infty} j_1(\gamma) = 4, \qquad \sum_{\gamma \in \mathbb{P}_\mathcal{C}, \gamma \text{ centered at } X_\infty} j_2(\gamma) = 6, \tag{4}$$

$$\sum_{\gamma \in \mathbb{P}_\mathcal{C}, \gamma \text{ centered at } Z_\infty} j_1(\gamma) = 4, \qquad \sum_{\gamma \in \mathbb{P}_\mathcal{C}, \gamma \text{ centered at } Z_\infty} j_2(\gamma) = 6. \tag{5}$$

Hence,

$$\sum_{\gamma \in \mathbb{P}_\mathcal{C}, \gamma \text{ centered at } X_\infty} \big(j_2(\gamma) - j_1(\gamma)\big) = \sum_{\gamma \in \mathbb{P}_\mathcal{C}, \gamma \text{ centered at } Z_\infty} \big(j_2(\gamma) - j_1(\gamma)\big) = 2. \tag{6}$$

As $j_2(\xi) - j_1(\xi)$ is a positive integer for any place ξ, this implies that there are at most two places of $\mathbb{K}(\mathcal{C})$ centered at X_∞, and similarly for Z_∞. Assume that

there are precisely two places of $\mathbb{K}(\mathcal{C})$ centered at X_∞, say γ_1 and γ_2. Then we can assume that either $j_1(\gamma_1) = j_1(\gamma_2) = 2$, or $j_1(\gamma_1) = 1$ and $j_1(\gamma_2) = 3$. In the former case, $j_2(\gamma_1) = j_2(\gamma_1) = 3$ and hence $v_{\gamma_1}(XZ/T^2) = v_{\gamma_2}(XZ/T^2) = -1$. In the latter case, $j_2(\gamma_1) = 2$ and $j_2(\gamma_2) = 4$, which yields $v_{\gamma_1}(Z/T) = v_{\gamma_2}(Z/T) = 1$, $v_{\gamma_1}(X/T) = -1$, $v_{\gamma_2}(X/T) = -3$. Therefore, $\bar{z}' = Z/T$ would be a local parameter at γ_1. Then the valuation of $4b^2 g(\bar{x}' + a)(\bar{z}')^2$ at γ_1 would be odd, contradicting the fact that by (2) the rational function $4b^2 g(\bar{x}' + a)(\bar{z}')^2$ is a square in $\mathbb{K}(\mathcal{C})$.

Similarly, it can be proved that if there are precisely two places of $\mathbb{K}(\mathcal{C})$ centered at Z_∞, then they both have order 2, and the valuation of XZ/T^2 at each of them is -1.

The following result is then obtained.

Lemma 7 *One of the following holds*:

(I) *there exists a place* γ *in* $\mathbb{K}(\mathcal{Y}) \cong \mathbb{K}(\mathcal{C})$ *with* $v_\gamma((\bar{x} - a)(\bar{z} - a)) = -1$;
(II) *there exist two places* γ_1, γ_2 *in* $\mathbb{K}(\mathcal{Y}) \cong \mathbb{K}(\mathcal{C})$ *with* $v_{\gamma_i}((\bar{x} - a)(\bar{z} - a)) = -2$ *for* $i = 1, 2$, $v_{\gamma_1}(\bar{x} - a) = -4$, $v_{\gamma_2}(\bar{x} - a) = 2$; *also, any other place different from* γ_1 *and* γ_2 *is not a pole of either* $\bar{x} - a$ *or* $\bar{z} - a$.

Proposition 2 *If* $b \neq 0$, *then the rational function* $(\bar{x} - a)(\bar{z} - a)$ *is not a square in* $\mathbb{K}(\mathcal{Y})$. *For a non-zero element* c *in* $\mathbb{F}_q$, *the equation* $cT^2 = (\bar{x} - a)(\bar{z} - a)$ *defines a double cover of* $\mathbb{F}_q(\mathcal{Y})$ *whose full constant field is* $\mathbb{F}_q$.

Proof The assertion is trivial in Case (I). Therefore, we can assume that Case (II) holds. Then

$$v_{\gamma_i}\big((\bar{x} - a)(\bar{z} - a)\big) = -2 \quad \text{for } i = 1, 2,$$

and

$$v_{\gamma_1}(\bar{x} - a) = -4, \qquad v_{\gamma_2}(\bar{x} - a) = 2.$$

Note also that for any place ξ of $\mathbb{K}(\mathcal{Y})$ different from γ_i we have $v_\xi((\bar{x} - a)(\bar{z} - a)) \geq 0$.

Suppose, contrary to our claim, that $(\bar{x} - a)(\bar{z} - a)$ is a square in $\mathbb{K}(\mathcal{Y})$, and let $s \in \mathbb{K}(\mathcal{Y})$ be such that $s^2 = (\bar{x} - a)(\bar{z} - a)$. Then,

$$v_{\gamma_i}(s) = -1 \quad \text{for } i = 1, 2.$$

Note that

- the pole divisor of $\bar{x} - a$ is $4\gamma_1$;
- the pole divisor of $s \cdot (\bar{x} - a)$ is $5\gamma_1$;
- the pole divisor of $s^{-1} \cdot (\bar{x} - a)$ is $3\gamma_1$.

Therefore, the Weierstrass semigroup at γ_1 contains $\{3, 4, 5, 6, \ldots\}$. This means that the genus g of $\mathcal{Y}$ is at most 2. By applying the Hurwitz genus formula to the double cover $\mathcal{Y} \to \mathcal{X}$ we deduce that $g = 2$ and that the degree of the ramification divisor is 2. One of the ramification places is γ_1, which is the only pole of $\bar{x} - a$. So there exists precisely one affine point (x_0, y_0) of $\mathcal{X}$ over which $\mathcal{Y}$ ramifies. We are going to show

that actually this cannot occur. Note that if (u, v) is a point in $\mathcal{X}$ with $u \neq a$ whose tangent line ℓ passes through (a, b), then the line ℓ contains a point over which $\mathcal{Y}$ ramifies.

If $g(a) \neq 0$, then in $\mathcal{X}$ there are two zeros of $\bar{x} - a$. In $\mathbb{K}(\mathcal{C})$, the number of zeros of $\bar{x} - a$ is 3. Therefore, one of these zeros is a ramification place. In order to get a contradiction, we only need one tangent at an affine point passing through (a, b).

If $g(a) = 0$, then in $\mathcal{X}$ there is one zero of $\bar{x} - a$ (of multiplicity 2). In $\mathbb{K}(\mathcal{C})$, $\bar{x} - a$ has either two or three zeros. Actually, they must be two because the degree of the covering is 2; this means that there is precisely one place centered at $(0, 0)$. Note that there is no ramification at these points. Here, to get a contradiction we need two tangents (at affine points) passing through (a, b), other than the vertical tangent $X = a$.

It is a classical result from Algebraic Geometry that through a point $P \notin \mathcal{X}$ there pass six tangents to $\mathcal{X}$, counted with multiplicity. For $p > 3$, this multiplicity is 2 if the tangency point is a flex, 1 otherwise. Therefore, if $p > 3$, there are at least two tangents (at affine points of $\mathcal{X}$) passing through (a, b), other than the vertical tangent $X = a$. Actually, it is easy to show by straightforward computation that the same holds for $p = 3$. This completes the proof. □

Proposition 3 *The genus of the double cover defined in Proposition 2 is at most* 10.

Proof By the previous proofs, we know that the number of places of $\mathbb{K}(\mathcal{Y})$ that are either a zero or a pole of $\bar{x}'\bar{z}'$ is less than or equal to six. Then the assertion follows from the genus formula for Kummer extensions (see e.g. [22, Proposition 3.7.3]). □

3.2 Case (2): $b = 0$

Here the equation which relates $\bar{x}'$ and $\bar{z}'$ is $(\bar{x}'\bar{z}')^2 - \bar{x}'\bar{z}'(2Aa + B + 3a^2) - (\bar{x}' + \bar{z}')g(a) = 0$. Let $\mathcal{C}'$ be the plane curve with equation

$$H'(X, Z) : X^2Z^2 - XZ\left(2Aa + B + 3a^2\right) - (X + Z)g(a) = 0.$$

Note that in this case $\mathbb{K}(\bar{x}', \bar{z}')$ is not the whole $\mathbb{K}(\mathcal{Y})$.

In order to prove that $\bar{x}'\bar{z}' = cT^2$, with c a non-zero element in $\mathbb{F}_q$, defines a double cover of $\mathbb{K}(\mathcal{Y})$, first we show that $\bar{x}'\bar{z}' = cT^2$ defines a double cover of $\mathbb{K}(\mathcal{C}')$.

Both X_∞ and Z_∞ are double points of $\mathcal{C}'$. The unique tangent of $\mathcal{C}'$ at X_∞ is the line with equation $Z = 0$, and the intersection multiplicity $\mathrm{I}(X_\infty, \mathcal{X} \cap \{Z = 0\})$ is equal to 3. Similarly, the unique tangent of $\mathcal{C}'$ at Z_∞ is $X = 0$, and $\mathrm{I}(Z_\infty, \mathcal{X} \cap \{X = 0\}) = 3$. Then there exists precisely one place of $\mathbb{K}(\bar{x}', \bar{z}')$, say γ_1, centered at X_∞, and one place, say γ_2, centered at Z_∞. Also, let γ_O be the only place centered at $(0, 0)$. Both γ_1 and γ_2 have order 2 and class 1. From Theorem 3 it follows that

$$\begin{aligned} v_{\gamma_1}(\bar{x}') &= -2, \qquad v_{\gamma_1}(\bar{z}') = 1, \\ v_{\gamma_2}(\bar{x}') &= 1, \qquad v_{\gamma_2}(\bar{z}') = -2, \\ v_{\gamma_O}(\bar{x}') &= 1, \qquad v_{\gamma_O}(\bar{z}') = 1. \end{aligned}$$

Therefore,

$$v_{\gamma_1}(\bar{x}'\bar{z}') = -1, \qquad v_{\gamma_2}(\bar{x}'\bar{z}') = -1, \qquad v_{\gamma_O}(\bar{x}'\bar{z}') = 2. \tag{7}$$

Then clearly the rational function $\bar{x}'\bar{z}'$ is not a square in $\mathbb{K}(\bar{x}', \bar{z}')$, and hence $\bar{x}'\bar{z}' = cT^2$ defines a double cover of $\mathbb{K}(\mathcal{C}')$. Let $\mathbb{K}(\bar{x}', \bar{z}')(\bar{w})$ be such a double cover, where $c\bar{w}^2 = \bar{x}'\bar{z}'$.

Our goal is to show that the compositum of the function fields $\mathbb{K}(\bar{x}', \bar{z}')(\bar{y})$ and $\mathbb{K}(\bar{x}', \bar{z}')(\bar{w})$ is defined over $\mathbb{F}_q$. To this end, we investigate the ramification places of the extensions $\mathbb{K}(\bar{x}', \bar{z}')(\bar{y})$ over $\mathbb{K}(\bar{x}', \bar{z}')$, and $\mathbb{K}(\bar{x}', \bar{z}')(\bar{w})$ over $\mathbb{K}(\bar{x}', \bar{z}')$. Note first that since $g(a) \neq 0$ we have

$$v_{\gamma_1}(g(\bar{x}' + a)) = -6, \qquad v_{\gamma_2}(g(\bar{x}' + a)) = 0, \qquad v_{\gamma_O}(g(\bar{x}' + a)) = 0. \tag{8}$$

Let $\bar{\gamma}$ be any place of $K(\bar{x}', \bar{z}', \bar{y})$ lying over γ_1. Then $e(\bar{\gamma}|\gamma_1) = 1$. On the other hand, let $\bar{\delta}$ be any place of $K(\bar{x}', \bar{z}', \bar{w})$ lying over γ_1; then $e(\bar{\delta}|\gamma_1) = 2$. This follows for instance from [22, Proposition 3.7.3]. Then Lemma 1 applies, and the following result is obtained.

Proposition 4 *If $b = 0$, then the rational function $(\bar{x} - a)(\bar{z} - a)$ is not a square in $\mathbb{F}_q(\mathcal{Y})$. For a non-zero element c in $\mathbb{F}_q$, the equation $cT^2 = (\bar{x} - a)(\bar{z} - a)$ defines a double cover of $\mathbb{F}_q(\mathcal{Y})$ whose full constant field is $\mathbb{F}_q$.*

Proposition 5 *The genus of the double cover defined in Lemma 4 is at most* 10.

Proof The proof is similar to that of Proposition 3. □

4 Bicovered points off the elliptic curve

Let $\mathcal{X}$ be as in the previous section, and let $\oplus$ denote the point addition on $\mathcal{X}$ such that the only infinite point of $\mathcal{X}$ is the neutral element O of $(\mathcal{X}, \oplus)$.

Let $m > 2$ be a prime divisor of the size of $\mathcal{X}(\mathbb{F}_q)$, m different from the characteristic p of $\mathbb{F}_q$. Let K be a subgroup of $(\mathcal{X}(\mathbb{F}_q), \oplus)$ of index m, and let K_e be a coset of K.

The main result of this section is the following.

Theorem 4 *Assume that the j-invariant of $\mathcal{X}$ is different from zero, and that $m > 2$ is a prime dividing both the size of $\mathcal{X}(\mathbb{F}_q)$ and $q - 1$, and such that $(\mathcal{X}(\mathbb{F}_q), \oplus)$ has a unique subgroup K of index m. If $m \leq \frac{\sqrt[4]{q}}{8}$, then the bisecants of any coset of K bicover all the points of $AG(2, q)$ not on $\mathcal{X}$.*

We first prove the following key lemma.

Lemma 8 *Assume that $m > 2$ is a prime dividing both the size of $\mathcal{X}(\mathbb{F}_q)$ and $q - 1$, and that $(\mathcal{X}(\mathbb{F}_q), \oplus)$ has a unique subgroup K of index m. Let $K_1, \ldots, K_m$ be the cosets of K. Then there exist m coverings of algebraic curves $\eta_i : \mathcal{X}_i \to \mathcal{X}$, $i = 1, \ldots, m$, defined over $\mathbb{F}_q$, satisfying the following properties.*

(A) $\mathbb{F}_q(\mathcal{X}_i) = \mathbb{F}_q(\mathcal{X})(t_i)$ *is an unramified Kummer extension of* $\mathbb{F}_q(\mathcal{X})$ *of degree* m; *in particular,* $\mathcal{X}_i$ *is an elliptic curve.*
(B) $\eta_i(\mathcal{X}_i(\mathbb{F}_q)) = K_i$.

Let $M_i = \mathbb{F}_q(\bar{x}, \bar{y}, \bar{z}, t_i)$ *be the compositum of* $\mathbb{F}_q(\mathcal{X}_i)$ *and* $\mathbb{F}_q(\mathcal{Y})$.

(C) *The extension* $M_i/\mathbb{F}_q(\mathcal{Y})$ *is Galois.*
(D) *The full constant field of* M_i *is* $\mathbb{F}_q$. *Also, the extension* $M_i/\mathbb{F}_q(\mathcal{Y})$ *is unramified.*
(E) *Let* $1 \le i, j \le m$, $i \ne j$. *Then*
  (i) $M_i \cap M_j = \mathbb{F}_q(\mathcal{Y})$;
  (ii) *the compositum* $M_i M_j$ *coincides with* $\mathbb{F}_{q^m} M_1$.

Proof

Let P_1 be a point of order m in $(\mathcal{X}(\mathbb{F}_q), \oplus)$, and let $\alpha(\bar{x}, \bar{y})$ be a rational function on $\mathcal{X}$ such that $\mathrm{div}(\alpha) = m P_1 - m O$. We can assume that α is defined over $\mathbb{F}_q$ (see e.g. Lemma 11.10 in [28]). Note that $\alpha(\bar{x}, \bar{y})$ is a polynomial function in $\bar{x}, \bar{y}$, since O is the only pole of α. Write K_i as $K \oplus Q_i$, with $Q_i \in \mathcal{X}(\mathbb{F}_q)$, $Q_i \ne P_1$, $Q_i \ne O$. Note that:

- α is not an mth power, since otherwise $P_1 - O$ would be a principal divisor, and $\mathcal{X}$ would be rational and not elliptic;
- $d_i := \alpha(Q_i)$ is a non-zero element in $\mathbb{F}_q$;
- the Kummer extension defined by the equation $t^m = d_i^{-1}\alpha(\bar{x}, \bar{y})$ is unramified; therefore, the associated curve $\mathcal{X}_i$ is elliptic;
- the points of $\mathcal{X}_i$ lying over Q_i are all $\mathbb{F}_q$-rational; they can be described as (x_0, y_0, μ) where $Q_i = (x_0, y_0)$ and $\mu^m = 1$;
- if we choose the neutral element of $(\mathcal{X}_i, \oplus)$ to be $(x_0, y_0, 1)$, then the map

$$\sigma_i : (\bar{x}, \bar{y}, t) \mapsto (\bar{x}, \bar{y}) \ominus Q_i$$

  is an isogeny of degree m from $\mathcal{X}_i$ to $\mathcal{X}$, defined over $\mathbb{F}_q$, and whose kernel consists of the $\mathbb{F}_q$-rational points (x_0, y_0, μ) where $Q_i = (x_0, y_0)$ and $\mu^m = 1$; then $\sigma_i(\mathcal{X}_i(\mathbb{F}_q))$ coincides with K, since K is the unique subgroup of $(\mathcal{X}(\mathbb{F}_q), \oplus)$ of index m.

Note that

$$\eta_i : (\bar{x}, \bar{y}, t) \mapsto \sigma_i(\bar{x}, \bar{y}, t) \oplus Q_i = (\bar{x}, \bar{y})$$

maps $\mathcal{X}_i(\mathbb{F}_q)$ to K_i. Then for every coset K_i of K, there exists an element $c_i \in \mathbb{F}_q$ such that the extension defined by $t_i^m = c_i\alpha(\bar{x}, \bar{y})$ is an elliptic function field, and the natural projection of the associated elliptic curve $\mathcal{X}_i$ on $\mathcal{X}$ maps the $\mathbb{F}_q$-rational points of $\mathcal{X}_i$ precisely on K_i. This means that both (A) and (B) hold for $\mathcal{X}_i$ and η_i.

(C) Note that $\deg(M_i/\mathbb{F}_q(\mathcal{Y})) = m$. Also, $M_i = \mathbb{F}_q(\mathcal{Y})(t_i)$, with $t_i^m = c_i\alpha(\bar{x}, \bar{y})$. Therefore $M_i/\mathbb{F}_q(\mathcal{Y})$ is a Kummer extension.

(D) Every tangent to $\mathcal{X}$ passing through (a, b) corresponds to some ramification place in $\mathbb{F}_q(\mathcal{Y})/\mathbb{F}_q(\mathcal{X})$. Then the constant field of M_i is $\mathbb{F}_q$ by Lemma 1. The second assertion follows from [22, Proposition 3.9.6(a)].

To prove (E), we need to show that there is no common $\mathbb{F}_q$-rational place of M_i and M_j, so that $M_i \ne M_j$. Assume on the contrary that c_i/c_j is an mth power in $\mathbb{F}_q^*$,

then $c_i = \lambda^m c_j$ for some $\lambda \in \mathbb{F}_q$. The map that fixes $\mathbb{F}_q(\mathcal{X})$ elementwise and maps t_j in λt_j is an $\mathbb{F}_q$-isomorphism from $\mathbb{F}_q(\mathcal{X}_j)$ to $\mathbb{F}_q(\mathcal{X}_i)$: from $t_j^m = c_j\alpha(\bar{x}, \bar{y})$ it follows $(\lambda t_j)^m = \lambda^m c_j \alpha(\bar{x}, \bar{y}) = c_i\alpha(\bar{x}, \bar{y})$. This is a contradiction as $(x_0, y_0, t) \in \mathcal{X}_j(\mathbb{F}_q)$ and $(x_0, y_0, \lambda t) \in \mathcal{X}_i(\mathbb{F}_q)$ would imply that (x_0, y_0) belongs to two distinct cosets of K. Therefore, $\mathbb{F}_q(\mathcal{Y}) \subseteq M_i \cap M_j \subsetneq M_i$. As $m = \deg(M_i/\mathbb{F}_q(\mathcal{Y}))$ is a prime, (i) follows. A solution of $c_i t^m = \alpha(\bar{x}, \bar{y})$ is $t_i = \lambda t_1$, with $\lambda \in \mathbb{F}_{q^m}$ such that $\lambda^m = c_1/c_i$. This shows that $M_i \subset \mathbb{F}_{q^m} M_1$ for each $i = 1, \ldots, m$, which clearly implies (ii). □

Remark 2 Let E be as in Remark 1. Assume that γ' is a rational place of M_i such that $\gamma' \cap \mathbb{F}_q(\mathcal{Y})$ is not a place in E. Let $\tilde{x} = \bar{x}(\gamma')$, $\tilde{y} = \bar{y}(\gamma')$, $\tilde{z} = \bar{z}(\gamma')$, $\tilde{t} = t_i(\gamma')$. Then, on one hand, $(\tilde{x}, \tilde{y}, \tilde{t})$ is an $\mathbb{F}_q$-rational point of $\mathcal{X}_i$ and hence $(\tilde{x}, \tilde{y}) \in K_i$; on the other hand, by Remark 1 the line through P_0 and $(\tilde{x}, \tilde{y})$ meets $\mathcal{X}$ in other two $\mathbb{F}_q$-rational points, one of which being $(\tilde{z}, (\frac{\tilde{y}-b}{\tilde{x}-a})(\tilde{z} - a) + b)$.

Without loss of generality, assume that K_e coincides with K_1.

Now, consider the field $M_1' = \mathbb{F}_q(\mathcal{Y})(u)$, where the minimal polynomial of u over $\mathbb{F}_q(\mathcal{Y})$ is

$$c_1 T^m = \alpha\big(\phi(\bar{x}), \phi(\bar{y})\big) = \alpha\left(\bar{z}, \left(\frac{\bar{y} - b}{\bar{x} - a}\right)(\bar{z} - a) + b\right)$$

(here ϕ is as in Lemma 3 and α is as in the proof of Lemma 8). Then it is possible to define an $\mathbb{F}_q$-isomorphism $\tilde{\phi} : M_1 \to M_1'$ such that $\tilde{\phi}(t_1) = u$ and $\tilde{\phi}(v) = \phi(v)$ for every $v \in \mathbb{F}_q(\mathcal{Y})$.

As the extensions $M_1/\mathbb{F}_q(\mathcal{Y})$ and $M_1'/\mathbb{F}_q(\mathcal{Y})$ are $\mathbb{F}_q$-isomorphic, the full constant field of M_1' is $\mathbb{F}_q$. Also, $M_1'/\mathbb{F}_q(\mathcal{Y})$ is Galois and unramified.

Remark 3 Let γ'' be a rational place of M_1' such that $\gamma'' \cap \mathbb{F}_q(\mathcal{Y})$ is not a place of E. Let $\tilde{x} = \bar{x}(\gamma'')$, $\tilde{y} = \bar{y}(\gamma'')$, $\tilde{z} = \bar{z}(\gamma'')$, $\tilde{u} = u(\gamma'')$. Note that $\gamma' := \tilde{\phi}^{-1}(\gamma'')$ does not lie over a place in E. Then Remark 2 applies to γ'. This means that $(\tilde{z}, (\frac{\tilde{y}-b}{\tilde{x}-a})(\tilde{z} - a) + b)$ is a point of K_1 collinear with P_0 and such that the line through P_0 and $(\tilde{z}, (\frac{\tilde{y}-b}{\tilde{x}-a})(\tilde{z} - a) + b)$ meets $\mathcal{X}$ in three $\mathbb{F}_q$-rational points.

Proposition 6 *Let $W = \mathbb{F}_q(\mathcal{Y})(t_1, u)$ be the compositum of M_1 and M_1'. Under the hypotheses of Lemma 8, the full constant field of W is $\mathbb{F}_q$, provided that q is large enough with respect to m.*

Proof Assume on the contrary that the constant field of W is not $\mathbb{F}_q$. Then $M_1 \subsetneq W$; also, as m is a prime, the degree of the extension $W/\mathbb{F}_q(\mathcal{Y})$ is m^2, and both $\deg(W/M_1)$ and $\deg(W/M_1')$ are equal to m. As the full constant field of M_1 is $\mathbb{F}_q$, the only possibility for the full constant field of W is clearly $\mathbb{F}_{q^m}$. Therefore,

$$W = \mathbb{F}_{q^m} M_1 = \mathbb{F}_{q^m} M_1'$$

holds. Also, the extension $W/\mathbb{F}_q(\mathcal{Y})$ is Galois, and the Galois group of $W/\mathbb{F}_q(\mathcal{Y})$ is isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_m$ (see e.g. [17, Chap. VI, Theorem 1.14]).

By (E) of Lemma 8, all function fields $M_1, \ldots, M_m$ are contained in W, and any intersection $M_i \cap M_j$ coincides with $\mathbb{F}_q(\mathcal{Y})$. Also, $M_i \cap \mathbb{F}_{q^m}(\mathcal{Y}) = \mathbb{F}_q(\mathcal{Y})$ holds as the constant field of M_i is $\mathbb{F}_q$.

The key point of the present proof is that M_1' must coincide with some M_i. This can be proven as follows. The Galois groups $\mathrm{Gal}(W/M_i)$, $i = 1, \ldots, m$, together with $\mathrm{Gal}(W/\mathbb{F}_{q^m}(\mathcal{Y}))$, form a set of $m+1$ cyclic subgroups of order m of $\mathrm{Gal}(W/\mathbb{F}_q(\mathcal{Y}))$ with pairwise trivial intersection, and whose union is the whole $\mathrm{Gal}(W/\mathbb{F}_q(\mathcal{Y})) \cong Z_m \times \mathbb{Z}_m$. As m is prime and $\mathrm{Gal}(W/M_1')$ is non-trivial, $\mathrm{Gal}(W/M_1')$ must coincide either with some $\mathrm{Gal}(W/M_i)$, or with $\mathrm{Gal}(W/\mathbb{F}_{q^m}(\mathcal{Y}))$. As $W/\mathbb{F}_q(\mathcal{Y})$ is Galois, the Galois correspondence is bijective. Clearly $\mathrm{Gal}(W/M_1') = \mathrm{Gal}(W/\mathbb{F}_{q^m}(\mathcal{Y}))$ cannot occur since the full constant field of M_1' is $\mathbb{F}_q$. Therefore, $M_1' = M_j$ holds for some j.

Now let E be as in Remark 1, and let γ be a rational place of $\mathbb{F}_q(\mathcal{Y})$ not in E. Let $\tilde{x} = \bar{x}(\gamma)$, $\tilde{y} = \bar{y}(\gamma)$, and $\tilde{z} = \bar{z}(\gamma)$. Note that on one hand γ splits completely in M_1' if and only if $(\tilde{z}, (\frac{\tilde{y}-b}{\tilde{x}-a})(\tilde{z}-a)+b)$ is a point in K_1; on the other hand, γ splits completely in M_j if and only if $(\tilde{x}, \tilde{y})$ lies in K_j. As $M_1' = M_j$, the two conditions are equivalent, and since the latter is independent of $\tilde{z}$, so is the former. Therefore, if γ splits completely in M_1', so does the other rational place of $\mathbb{F}_q(\mathcal{Y})$ lying over $(\tilde{x}, \tilde{y})$, say γ'. In this case, $(\bar{z}(\gamma'), (\frac{\bar{y}-b}{\bar{x}-a})(\bar{z}(\gamma')-a)+b)$ lies in K_1 as well. If q is large enough with respect to m, by the Hasse–Weil bound we can ensure the existence of a rational place γ_j of M_j lying over a rational place γ of $\mathbb{F}_q(\mathcal{Y})$, $\gamma \notin E$. By the above discussion, this implies the existence of three distinct $\mathbb{F}_q$-rational points in $\mathcal{X}(\mathbb{F}_q)$, collinear with $P_0 = (a, b)$, two of which lying in K_1. This means that there exists a rational place of $\mathbb{F}_q(\mathcal{Y})$ splitting completely over $M_1/\mathbb{F}_q(\mathcal{Y})$ and $M_1'/\mathbb{F}_q(\mathcal{Y})$. Then Lemma 2 provides a contradiction. □

Proposition 7 *Let c be a non-zero element in $\mathbb{F}_q$, and let $\bar{w}$ be an element in the algebraic closure of $\mathbb{F}_q(\mathcal{Y})$ such that $c\bar{w}^2 = (\bar{x}-a)(\bar{z}-a)$. Then the full constant field of the compositum $W_c' = W \cdot \mathbb{F}_q(\mathcal{Y})(\bar{w})$ is $\mathbb{F}_q$.*

Proof Here we are using Propositions 2, 4 and 6. Let ℓ be the degree of the extension $W/\mathbb{F}_q(\mathcal{Y})$. As ℓ divides m^2, we see that ℓ is odd. Therefore, the degree of W_c'/W is two, and $\deg(W_c'/\mathbb{F}_q(\mathcal{Y})(\bar{w})) = \ell$. As the full constant field of W is $\mathbb{F}_q$, then the constant field of W_c' is either $\mathbb{F}_q$ or $\mathbb{F}_{q^2}$. In the latter case, we have a quadratic extension $\mathbb{F}_{q^2}(\mathcal{Y})(\bar{w})$ of $\mathbb{F}_q(\mathcal{Y})(\bar{w})$ contained in W_c', which is clearly impossible as the degree of the extension $W_c'/\mathbb{F}_q(\mathcal{Y})(\bar{w})$ is odd. □

We are now in a position to prove Theorem 4.

Proof of Theorem 4 We prove that the point $P_0 = (a, b)$ is bicovered by the secants of K_e. The assertion will follow as P_0 is an arbitrary point not on $\mathcal{X}$. For a non-zero element $c \in \mathbb{F}_q$, let W_c' and $\bar{w}$ be as in Proposition 7. As the full constant field of W_c' is $\mathbb{F}_q$, we will use the Hasse–Weil bound in order to obtain at least one rational place γ_W of W_c' such that $\gamma_W \cap \mathbb{F}_q(\mathcal{Y}) \notin E$.

The degree of the extension $W_c'/\mathbb{F}_q(\mathcal{Y})$ is at most $2m^2$. Therefore, the number of rational places of W_c' lying over places of E is at most $36m^2$. By Propositions 3 and 5

the genus of $\mathbb{F}_q(\mathcal{Y})(\bar{w})$ is at most 10. It is pointed out in [26] that the genus of W is at most $7m^2+1$. Then by Castelnuovo's Inequality (see e.g. [22, 3.11.3]) the genus of W'_c is at most $14m^2+2+10m^2+m^2-1=25m^2+1$.

Therefore it is enough to assume that

$$q+1-2\big(25m^2+1\big)\sqrt{q}>36m^2,$$

that is,

$$q>\Big(25m^2+1+\sqrt{\big(25m^2+1\big)^2+36m^2}\Big)^2.$$

This clearly holds for $m\le\frac{\sqrt[4]{q}}{8}$.

Let γ_W be a rational place of W'_c such that $\gamma_W\cap\mathbb{F}_q(\mathcal{Y})\notin E$. Note that γ_W is not a zero nor a pole of $\bar{w}$. The places $\gamma_W\cap M_1$ and $\gamma_W\cap M'_1$ are rational places (of M_1 and M'_1, respectively) lying over $\gamma_W\cap\mathbb{F}_q(\mathcal{Y})$. Let

$$\tilde{x}=\bar{x}(\gamma_W),\qquad \tilde{y}=\bar{y}(\gamma_W),\qquad \tilde{z}=\bar{z}(\gamma_W),$$
$$\tilde{t}=t_1(\gamma_W),\qquad \tilde{u}=u(\gamma_W),\qquad \tilde{w}=\bar{w}(\gamma_W).$$

Then by Remarks 2 and 3 we find that $P_{1,c}=(\tilde{x},\tilde{y})$ and $P_{2,c}=(\tilde{z},(\frac{\tilde{y}-b}{\tilde{x}-a})(\tilde{z}-a)+b)$ are two points on K_e collinear with P_0. Moreover, $(\tilde{x}-a)(\tilde{z}-a)=c\tilde{w}^2$ holds. If c is chosen to be a square, then P_0 is external to $P_{1,c}P_{2,c}$; if c is not a square, then P_0 is internal to $P_{1,c}P_{2,c}$. □

Remark 4 The idea of associating to a point $P_0=(a,b)\in AG(2,q)\setminus\mathcal{X}$ a function field W whose $\mathbb{F}_q$-rational places correspond to the secants of K_e passing through P_0 is taken from [26], where the following result is stated: if the j-invariant $j(\mathcal{X})$ of $\mathcal{X}$ is different from 0, then the bisecants of a coset K_e of a subgroup of index m cover all the points of $AG(2,q)$ not on $\mathcal{X}$, provided that q is large enough with respect to m.

However, in [26], the possibility that the constant field of W properly contains $\mathbb{F}_q$ is not considered, and it actually might have been overlooked by the author [27]. The proof of Proposition 6 shows that actually the full constant field of W is $\mathbb{F}_q$, under the additional hypotheses that m is an odd prime dividing $q-1$ and $(\mathcal{X}(\mathbb{F}_q),\oplus)$ has a unique subgroup of index m. As a corollary, complete arcs in $PG(2,q)$ of size of the same order of magnitude as $q^{3/4}$ can be obtained with the arguments of [23], provided that $q-1$ has a prime divisor m slightly less than $\frac{1}{8}q^{1/4}$.

5 Bicovered points on the elliptic curve

We keep the notation of the previous sections, but here we assume that $P_0=(a,b)$ is an affine point on $\mathcal{X}$, with $a,b\in\mathbb{F}_q$. Let $\mathbb{K}(\mathcal{X})=\mathbb{K}(\bar{x},\bar{y})$ with $\bar{y}^2=\bar{x}^3+A\bar{x}^2+B\bar{x}+C$. For a point Q in $\mathbb{A}^2(\mathbb{K}(\mathcal{X}))$, let Q_X denote the first coordinate of Q.

Note that for a point $P=(x,y)\in\mathcal{X}$, the points belonging to $\mathcal{X}\cap\ell_{P_0,P}$ are P_0, P and $\ominus(P_0\oplus P)=(a,-b)\oplus(x,-y)$. Let $\beta(\bar{x},\bar{y})$ be the rational function

$$\beta:=(\bar{x}-a)\cdot\big(\big((a,-b)\oplus(\bar{x},-\bar{y})\big)_X-a\big).$$

From the definition of $\oplus$ it follows that

$$\big((a,-b)\oplus(\bar{x},-\bar{y})\big)_X=\left(\frac{-\bar{y}+b}{\bar{x}-a}\right)^2-\bar{x}-a-A,$$

whence

$$\beta(\bar{x},\bar{y})=\frac{1}{\bar{x}-a}\cdot\big((b-\bar{y})^2-(\bar{x}+2a+A)(\bar{x}-a)^2\big).$$

We would like to prove that an equation $cT^2=\beta(\bar{x},\bar{y})$ with c a non-zero element in $\mathbb{F}_q$ defines a double cover of $\mathbb{K}(\mathcal{X})$ which ramifies at some point. To this end, it is enough to show that $v_R(\beta)$ is odd for some point R of $\mathbb{K}(\mathcal{X})$.

By straightforward computation $(\bar{x}-a)\beta(\bar{x},\bar{y})$ is equal to

$$b^2+\bar{y}^2-2b\bar{y}-\bar{x}^3-A\bar{x}^2+4a^2\bar{x}+2aA\bar{x}-a^2\bar{x}-2a^3-a^2A.$$

Taking into account that $\bar{y}^2-\bar{x}^3-A\bar{x}^2=B\bar{x}+C$, we obtain

$$\beta(\bar{x},\bar{y})=\frac{1}{\bar{x}-a}\big(b^2-2b\bar{y}+B\bar{x}+3a^2\bar{x}+2aA\bar{x}-2a^3-a^2A+C\big).$$

Recall that $v_{Y_\infty}(\bar{x})=-2$ and $v_{Y_\infty}(\bar{y})=-3$. Then if $b\neq 0$ we have $v_{Y_\infty}(\beta)=-1$. On the other hand, if $b=0$ then $C=-a^3-Aa^2-Ba$. In this case,

$$\begin{aligned}\beta(\bar{x},\bar{y})&=\frac{1}{\bar{x}-a}\big(\bar{x}\big(B+3a^2+2aA\big)-2a^3-a^2A+C\big)\\&=\frac{1}{\bar{x}-a}\big(\bar{x}\big(B+3a^2+2aA\big)-3a^3-2a^2A-Ba\big),\end{aligned}$$

and hence

$$\beta(\bar{x},\bar{y})=\frac{1}{\bar{x}-a}\big(B+3a^2+2aA\big)(\bar{x}-a)=\big(B+3a^2+2aA\big).$$

Then the following result is obtained.

Proposition 8 *If $g(a)\neq 0$, then the equation $cT^2=\beta(\bar{x},\bar{y})$, for $c\in\mathbb{F}_q$, $c\neq 0$, defines a double cover of $\mathbb{K}(\mathcal{X})$ which is defined over $\mathbb{F}_q$ and ramifies at some point of $\mathcal{X}$.*

The main result of this section is the following.

Proposition 9 *Assume that the j-invariant of $\mathcal{X}$ is different from zero, and that $m>2$ is a prime dividing both the size of $\mathcal{X}(\mathbb{F}_q)$ and $q-1$, and such that $(\mathcal{X}(\mathbb{F}_q),\oplus)$ has a unique subgroup K of index m. Assume that $m<\frac{\sqrt[4]{q}}{8}$. Let K_1 and K_2 be two distinct cosets of K such that $K_1\cup K_2$ is an arc. Let $P_0=(a,b)$ be an affine point on $\mathcal{X}$, with $a,b\in\mathbb{F}_q$ and $g(a)\neq 0$. If P_0 is collinear with $P_1\in K_1$ and $P_2\in K_2$, then P_0 is bicovered by $K_1\cup K_2$.*

Proof As P_0, P_1 and P_2 are collinear, $P_2 = \ominus P_0 \ominus P_1$ holds. Let P be any point in K_1 and write $P = Q \oplus P_1 \in K_1$, with $Q \in K$. The point $\ominus P_0 \ominus P$ is collinear with P_0 and P. Also, as

$$\ominus P_0 \ominus P = \ominus Q \oplus (\ominus P_0 \ominus P_1) = \ominus Q \oplus P_2$$

we see that $\ominus P_0 \ominus P$ is a point in $K \oplus P_2 = K_2$.

Therefore, to prove the assertion it is enough to find a point P in K_1 such that $\beta(P)$ is a non-zero square in $\mathbb{F}_q$, and another point $P' \in K_1$ with $\beta(P')$ a non-square in $\mathbb{F}_q$.

For a non-zero element in $\mathbb{F}_q$, let $\bar{w}$ be an element in the algebraic closure of $\mathbb{F}_q(\mathcal{X})$ such that $c\bar{w}^2 = \beta(\bar{x}, \bar{y})$. By Lemma 8 the extension $\mathbb{F}_q(\mathcal{X})(\bar{w})/\mathbb{F}_q(\mathcal{X})$ has degree 2, and the full constant field of $\mathbb{F}_q(\mathcal{X})(\bar{w})$ is $\mathbb{F}_q$. Let also $\mathcal{X}_1$ and t_1 be as in Lemma 8, and let $W_c = \mathbb{F}_q(\bar{x}, \bar{y}, t_1, \bar{w})$ be the compositum of $\mathbb{F}_q(\mathcal{X}_1)$ and $\mathbb{F}_q(\mathcal{X})(\bar{w})$. By Lemma 8(A), the extension $\mathbb{F}_q(\mathcal{X}_1)/\mathbb{F}_q(\mathcal{X})$ is unramified. On the other hand, by Lemma 8 the extension $\mathbb{F}_q(\mathcal{X})(\bar{w})/\mathbb{F}_q(\mathcal{X})$ fully ramifies at some point. Then Lemma 1 applies, and therefore the full constant field of W_c is $\mathbb{F}_q$.

Arguing as in the proof of Theorem 4, it is not difficult to prove that there exists a rational place γ_W of W_c such that it is neither a zero nor a pole of any of the rational functions $\bar{x}$, $\bar{y}$, $\bar{t}_1$ and $\bar{w}$. Let

$$\tilde{x} = \bar{x}(\gamma_W), \qquad \tilde{y} = \bar{y}(\gamma_W), \qquad \tilde{t} = t_1(\gamma_W), \qquad \tilde{w} = \bar{w}(\gamma_W).$$

Then $P = (\tilde{x}, \tilde{y})$ is a point of K_1. Moreover, $\beta(\tilde{x}, \tilde{y}) = c\tilde{w}^2$ holds. This completes the proof of the assertion. □

6 Proof of Theorem 1

Let $p = \mathrm{char}(\mathbb{F}_q)$. Let Z denote the set of the possible sizes of $\mathcal{X}(\mathbb{F}_q)$, where $\mathcal{X}$ ranges over the family of the elliptic curves defined over $\mathbb{F}_q$ with $j(\mathcal{X}) = 0$. It can be deduced from [19, Proposition 5.7] that in Z there at most three elements not greater than q.

Let $r = \lfloor \frac{q-2\sqrt{q}+1}{m} \rfloor$. As $m \geq 5$, among the integers $\{r + j \mid j = 1, \ldots, 31\}$ certainly there is an element i_0 such that $m \nmid i_0$, $i_0 m \not\equiv 1 \pmod{p}$, $2 \nmid i_0$, and $i_0 m \notin Z$.

Note that $q + 1 - i_0 m$ is not divisible by p and its absolute value is at most $2\sqrt{q}$. Then there exists an elliptic curve $\mathcal{X}'$ defined over $\mathbb{F}_q$ with $i_0 m$ $\mathbb{F}_q$-rational points, see [29]. As $i_0 m \not\equiv 1 \pmod{p}$, by a result in [25] there exists an elliptic curve $\mathcal{X}$ defined over $\mathbb{F}_q$ with the same number of $\mathbb{F}_q$-rational points, and such that $(\mathcal{X}(\mathbb{F}_q), \oplus)$ is cyclic. As $i_0 m \notin Z$, the j-invariant of $\mathcal{X}$ is different from 0. Write $\mathcal{X}(\mathbb{F}_q) = H \times K$, where H is the subgroup of $\mathcal{X}(\mathbb{F}_q)$ of order m. As $m < \sqrt[4]{q}/8$, by Theorem 4 any coset of K bicovers every affine point not on $\mathcal{X}$.

Let X be a maximal 3-independent subset of H of size s. The union S of the cosets of K corresponding to X is a good maximal 3-independent subset of $(\mathcal{X}(\mathbb{F}_q), \oplus)$,

that is, for each $P \in \mathcal{X}(\mathbb{F}_q) \setminus S$ there exist distinct $P_1, P_2 \in S$ with $P_1 \oplus P_2 \oplus P = 0$ (see [26], Lemma 1, together with Remark 5(5)). Note that as the size of $\mathcal{X}(\mathbb{F}_q)$ is odd, no element in $(\mathcal{X}(\mathbb{F}_q), \oplus)$ has order 2, and hence no $\mathbb{F}_q$-rational point $(a, b) \in \mathcal{X}$ is such that $g(a) = 0$. Therefore, by Theorem 4 and Proposition 9, S is a bicovering arc in $AG(2, q)$ with size si_0.

7 Maximal 3-independent subsets in finite groups of prime order

Let $m > 7$ be a prime number and let $\mathbb{C}_m \cong (\mathbb{F}_m, +)$ denote the finite group of order m.

It has been shown in [26] that there exists a maximal 3-independent subset of C_m of size $s \leq (m+1)/3$. As a result of a computer assisted computation, it turned out that for primes $37 \leq m \leq 1187$ there exists a maximal 3-independent subset of C_m size j, with j as in Table 1. An explicit description of these subsets as integers modulo m can be found in [16]. A straightforward consequence is the following result.

Proposition 10 *Let m be a prime with $37 \leq m \leq 1187$. Then there exists a maximal 3-independent subset of C_m with size $s \leq s(m)$, with $s(m)$ as in the following table*

m	$\in [37, 79]$	$\in [83, 149]$	$\in [151, 271]$	$\in [277, 359]$	$\in [367, 521]$
$s(m)$	$m/4$	$m/5$	$m/6$	$m/7$	$m/8$
m	$\in [523, 677]$	$\in [683, 829]$	$\in [839, 1087]$	$\in [1091, 1187]$	
$s(m)$	$m/9$	$m/10$	$m/11$	$m/12$	

As a corollary to Theorem 2 the following result is then obtained.

Proposition 11 *For an odd prime power q, let m be a prime divisor of $q-1$, with $37 \leq m < \min\{1188, \frac{1}{8}\sqrt[4]{q}\}$. Let $s(m)$ be as in Proposition 10. Then for any positive integer $N \equiv 0 \pmod 4$, there exists a complete cap in $AG(N, q)$ of size k with*

$$k \leq s(m) \cdot q^{\frac{N-2}{2}} \cdot \left(\left\lfloor \frac{q - 2\sqrt{q} + 1}{m} \right\rfloor + 31 \right).$$

We remark that by [23, Example 3.21] it is possible to construct a subset X of C_m of size greater than $\sqrt{m}$ and less than $30\sqrt{m}$, with the following properties:

(a) $x_1 + x_2 + x_3 \neq 0$ for all $x_1, x_2, x_3 \in X$;
(c) for each $y \in G \setminus X$, $X \cup \{y\}$ does not satisfy (a).

However, the subset X is not a maximal 3-independent subset of C_m in general. In fact, it is possible that there exists some $y \in C_m \setminus X$ with either $2y \in -X$ or $3y = 0$, but $y + x_1 + x_2 \neq 0$ for all $x_1, x_2 \in X$.

Table 1 Small maximal 3-independent subsets

m	j	m	j	m	j	m	j	m	j
13	4	17	6	19	6	23	7	29	8
31	9	37	9	41	10	43	10	47	11
53	12	59	12	61	14	67	15	71	14
73	15	79	16	83	16	89	17	97	16
101	19	103	20	107	20	109	21	113	20
127	21	131	24	137	23	139	24	149	25
151	24	157	26	163	27	167	26	173	27
179	27	181	27	191	30	193	29	197	29
199	31	211	35	223	33	227	34	229	33
233	33	239	33	241	35	251	35	257	34
263	36	269	38	271	39	277	37	281	39
283	38	293	41	307	40	311	42	313	41
317	42	331	43	337	42	347	43	349	44
353	42	359	47	367	45	373	44	379	46
383	46	389	47	397	48	401	48	409	48
419	48	421	52	431	51	433	51	439	53
443	53	449	50	457	52	461	53	463	54
467	54	479	55	487	53	491	56	499	54
503	56	509	57	521	58	523	57	541	54
547	60	557	61	563	61	569	62	571	59
577	61	587	60	593	62	599	65	601	62
607	62	613	65	617	61	619	63	631	62
641	67	643	65	647	70	653	64	659	64
661	64	673	61	677	68	683	68	691	67
701	69	709	69	719	70	727	69	733	71
739	72	743	68	751	69	757	73	761	68
769	64	773	72	787	74	797	76	809	75
811	76	821	72	823	77	827	76	829	78
839	75	853	75	857	77	859	76	863	77
877	79	881	77	883	80	887	80	907	82
911	82	919	78	929	79	937	80	941	83
947	79	953	82	967	81	971	80	977	85
983	84	991	81	997	84	1009	87	1013	85
1019	86	1021	86	1031	84	1033	86	1039	89
1049	87	1051	88	1061	87	1063	84	1069	87
1087	91	1091	88	1093	91	1097	87	1103	90
1109	90	1117	91	1123	92	1129	92	1151	92
1153	93	1163	93	1171	95	1181	95	1187	97

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

References

1. Anbar, N., Bartoli, D., Giulietti, M., Platoni, I.: Small complete caps from singular cubic plane curves. Preprint
2. Bierbrauer, J.: Large caps. J. Geom. **76**(1–2), 16–51 (2003)
3. Davydov, A.A., Giulietti, M., Marcugini, S., Pambianco, F.: New inductive constructions of complete caps in $PG(N,q)$, q even. J. Comb. Des. **18**(3), 177–201 (2010)
4. Faina, G., Pasticci, F., Schmidt, L.: Small complete caps in Galois spaces. Ars Comb. **105**, 299–303 (2012)
5. Giulietti, M.: On plane arcs contained in cubic curves. Finite Fields Appl. **8**(1), 69–90 (2002)
6. Giulietti, M.: On the extendibility of near-MDS elliptic codes, AAECC. Appl. Algebra Eng. Commun. Comput. **15**, 1–11 (2004)
7. Giulietti, M.: Small complete caps in Galois affine spaces. J. Algebr. Comb. **25**(2), 149–168 (2007)
8. Giulietti, M.: Small complete caps in $PG(N,q)$, q even. J. Comb. Des. **15**(5), 420–436 (2007)
9. Giulietti, M., Pasticci, F.: Quasi-perfect linear codes with minimum distance 4. IEEE Trans. Inf. Theory **53**(5), 1928–1935 (2007)
10. Hirschfeld, J.W.P.: Finite Projective Spaced of Three Dimensions. Oxford Univ. Press, Oxford (1985)
11. Hirschfeld, J.W.P.: Projective Geometries over Finite Fields, 2nd edn. Oxford Univ. Press, Oxford (1998)
12. Hirschfeld, J.W.P., Korchmáros, G., Torres, F.: Algebraic Curves over Finite Fields. Princeton University Press, Princeton (2008)
13. Hirschfeld, J.W.P., Storme, L.: The packing problem in statistics, coding theory and finite projective spaces: update 2001. Dev. Math. **3**, 201–246 (2001)
14. Hirschfeld, J.W.P., Thas, J.F.: General Galois Geometries. Oxford Univ. Press, Oxford (1991)
15. Hirschfeld, J.W.P., Voloch, J.F.: The characterisation of elliptic curves over finite fields. J. Aust. Math. Soc. A **45**, 275–286 (1988)
16. http://www.dmi.unipg.it/giuliet/3-ind.txt
17. Lang, S.: Algebra, revised 3rd edn. Springer, New York (2002)
18. Pambianco, F., Storme, L.: Small complete caps in spaces of even characteristic. J. Comb. Theory, Ser. A **75**(1), 70–84 (1996)
19. Schoof, R.: Nonsingular plane cubic curves over finite fields. J. Comb. Theory, Ser. A **46**(2), 183–211 (1987)
20. Segre, B.: Introduction to Galois geometries, edited by J.W.P. Hirschfeld. Atti Accad. Naz. Lincei Mem. **8**, 133–236 (1967)
21. Segre, B.: 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. **96**, 289–337 (1972)
22. Stichtenoth, H.: Algebraic Function Fields and Codes, 2nd edn. Springer, Berlin (2009)
23. Szőnyi, T.: Complete arcs in $PG(2,q)$: a survey. Quad. Sem. Geom. Comb. Univ. Roma "La Sapienza" **94** (1989)
24. Szőnyi, T.: Arcs, caps, codes, and 3-independent subsets. In: Faina, G., Tallini, G. (eds.) Proc. International Conference "Giornate di Geometrie Combinatorie", Perugia, 1992, pp. 57–80. Università degli Studi di Perugia, Perugia (1993)
25. Voloch, J.F.: A note on elliptic curves over finite fields. Bull. Soc. Math. Fr. **116**, 455–458 (1988)
26. Voloch, J.F.: On the completeness of certain plane arcs II. Eur. J. Comb. **11**, 491–496 (1990)
27. Voloch, J.F.: Private communication
28. Washington, L.C.: Elliptic Curves: Number Theory and Cryptography, 2nd edn. Chapman & Hall/CRC, Boca Raton (2008)
29. Waterhouse, W.G.: Abelian varieties over finite fields. Ann. Sci. Éc. Norm. Super. **2**, 521–560 (1969)