

Small complete caps from singular cubics, II

Nurdagül Anbar · Daniele Bartoli ·
Irene Platoni · Massimo Giulietti

Received: 2 December 2013 / Accepted: 7 May 2014 / Published online: 22 May 2014
© Springer Science+Business Media New York 2014

Abstract Small complete arcs and caps in Galois spaces over finite fields \mathbb{F}_q with characteristic greater than three are constructed from singular cubic curves. For m a divisor of $q + 1$ or $q - 1$, 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 in affine spaces of dimension $N \equiv 0 \pmod{4}$ with roughly $\frac{m_1+m_2}{m}q^{N/2}$ points are described. These results substantially widen the spectrum of qs for which complete arcs in $AG(2, q)$ of size approximately $q^{3/4}$ can be constructed. Complete caps in $AG(N, q)$ with roughly $q^{(4N-1)/8}$ points are also provided. For infinitely many qs , these caps are the smallest known complete caps in $AG(N, q)$, $N \equiv 0 \pmod{4}$.

Keywords Galois affine spaces · Bicoverying arcs · Complete caps · Quasi-perfect codes · Cubic curves

Mathematics Subject Classification 51E20

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

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

D. Bartoli
e-mail: daniele.bartoli@dmf.unipg.it

I. Platoni
Dipartimento di Matematica, University of Trento, Via Sommarive, 14, 38123 Povo, TN, Italy
e-mail: irene.platoni@unitn.it

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 [23]. 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; see e.g., [14].

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

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

If q is even and N is odd, then such bound is substantially sharp; see [21]. Otherwise, all known infinite families of complete caps have size far from (1); see the survey papers [17, 18] and the more recent works [1, 4, 5, 7, 8, 12–14]. For q odd and $N = 2$, the smallest explicit constructions go back to the late 80's, when Szőnyi described complete plane arcs of size approximately $(q - 1)/m$ for any divisor m of $q - 1$ smaller than $\frac{1}{C}q^{1/4}$, with C a constant independent of q and greater than 1 [27, 28]¹.

The aim of this paper is twofold: on the one hand, we substantially widen the spectrum of q for which complete arcs in $AG(2, q)$ of size approximately $q^{3/4}$ can actually be constructed; on the other hand, we provide new complete caps in $AG(N, q)$ with roughly $q^{(4N-1)/8}$ points. To this end, both plane cubics with a node and plane cubics with an isolated double point are investigated. Our main achievements here are Theorems 2, 3, and 6. For a divisor m of $q + 1$ or $q - 1$ 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 $m = m_1m_2$ with $(m_1, m_2) = 1$, we also provide complete caps with roughly $\frac{m_1+m_2}{m}q^{N/2}$ points in affine spaces $AG(N, q)$ with dimension $N \equiv 0 \pmod{4}$.

Let \mathcal{X} be an irreducible plane cubic defined over the finite field with q elements \mathbb{F}_q with at least one \mathbb{F}_q -rational inflection point. It was first noted by Zirilli [31] that a non-trivial coset A of the group of the non-singular \mathbb{F}_q -rational points of \mathcal{X} is a plane arc, provided that the index m of A is not divisible by 3. Since then, plane arcs in cubics have been thoroughly investigated, and complete caps have been obtained by recursive constructions from these arcs; see [1, 4, 9, 11, 19, 26–30].

For every $q = p^h$ with $p > 3$, there are exactly three projectively non-equivalent singular (irreducible) plane cubics with at least one \mathbb{F}_q -rational inflection point; see e.g. [6, 16]. Complete caps from singular cubics with a cusp were recently constructed by the same authors in [1]. The present paper can be considered a sequel of [1], in

¹ The condition of m being a divisor of $q - 1$ was not originally required in [28], but it is actually needed in order for the proof of a key lemma by Voloch to be correct; see Remark 4 in [4].

the sense that here, we deal with the two other projectively distinct singular cubics. The complete caps obtained here are significantly smaller than those constructed in [1], which have size roughly $2p^\beta q^{(4N-1)/8}$, with $\beta \in [1/8, 1]$ (see [1, Theorem 6.2]). Also, the proofs here rely on deeper concepts from the theory of Function Fields and need original techniques, especially for the case of a cubic with an isolated double point. In fact, despite Zirilli's paper [31] dating back to 1973, no results about arcs and caps from cubics with an isolated double point have appeared in the literature so far. One of the problems that comes up when dealing with these cubics is that the natural parametrization of the points of A , arising from the natural isomorphism between the group of the non-singular \mathbb{F}_q -rational points 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 a straightforward application of the classical method by Segre [22] and Lombardo Radice [20] for proving that a point P off \mathcal{X} is collinear with two points in A impossible; 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 14 and 15.

The paper is organized as follows. In Sect. 2, we briefly review some standard facts on bicovery arcs, curves, and algebraic function fields. In Sect. 3 we investigate a family of algebraic curves which play a crucial role for the investigation of the bicovery properties of a coset A , in both the nodal and the isolated-double-point cases. Bicovery arcs from nodal cubics are constructed in Sect. 4, where the main result is Theorem 1. We first prove that under our assumptions on m , each point P not on \mathcal{X} is bicoveryed by the secants of A (see Proposition 10); the case where P lies in \mathcal{X} is dealt with in Proposition 11. In Sect. 5, we discuss the complete caps in $AG(N, q)$ that can be constructed from the bicovery arcs of Theorem 1. The isolated-double-point case is investigated in Sects. 6 and 7. After proving the already mentioned key Lemmas 14 and 15, we show that almost each point P not on \mathcal{X} is bicoveryed by the secants of A in Propositions 16, 17, and 19; the case where P lies in \mathcal{X} is dealt with in Proposition 20. The proof of our main results is completed in Sect. 7. Finally, Sect. 8 contains a brief discussion about the possibility of constructing complete caps for $N \equiv 0 \pmod{4}$ when m is a prime; we show that Theorems 2 and 6 remain substantially valid for m a prime, provided that a suitable factorization of $m + 5$ exists.

We remark that the methods of the present paper could be used for other investigations involving rational curves, that is, curves that can be parametrized by polynomial or rational functions. A plane quartic \mathcal{Q} with a triple point is one of such curves. For instance, it seems that the problem of constructing subsets of points on \mathcal{Q} , where no four points are collinear, and proving their maximality with respect to set-theoretical inclusion, could be addressed with the tools from Function Field theory used in this paper.

The following table summarizes a number of existence results for complete caps constructed from plane cubic curves, including those obtained in this paper. In Table 1, N denotes the dimension of the Galois space and p the characteristic of the ground field.

Table 1 Small complete caps in Galois spaces from cubic curves

p	N	Size \leq	Conditions	Reference
>2	2	$\frac{q-1}{m} + m$	$m \mid q-1$ $m \leq \frac{1}{C} \sqrt[4]{q}, C > 1$ $m \mid q+1$	[4, 27, 28]
>3	2	$\frac{q+1}{m} + m$	$m \leq \frac{1}{\sqrt{6}} \sqrt[4]{q}$ $(m, 6) = 1, \left(m, \frac{q+1}{m}\right) = 1$ $q = p^h, h > 8$	Theorem 3
>3	$\equiv_4 0$	$2p^\beta q^{7/8} q^{\frac{N-2}{2}}$	$\beta = \frac{\log p q}{8} - \lfloor \frac{\lceil \frac{\log p q}{4} \rceil - 1}{2} \rfloor$	[1]
>3	$\equiv_4 0$	$s \left(\left\lfloor \frac{q-2\sqrt{q}+1}{m} \right\rfloor + 31 \right) q^{\frac{N-2}{2}}$	$m \mid q-1, s \leq m/3$ m prime, $7 < m < \frac{1}{8} \sqrt[4]{q}$ $m_1 m_2 \mid q-1$	[4]
>3	$\equiv_4 0$	$\frac{m_1+m_2}{m_1 m_2} q^{N/2}$	$m_1 m_2 \leq \frac{1}{3.5} \sqrt[4]{q}$ $(m_i, 6) = 1, (m_1, m_2) = 1$ $m_1 m_2 \mid q+1$	Theorem 2
>3	$\equiv_4 0$	$\left(\frac{m_1+m_2}{m_1 m_2} (q+1) + 3 \right) q^{\frac{N-2}{2}}$	$m_1 m_2 \leq \frac{1}{4} \sqrt[4]{q}$ $(m_i, 6) = 1, (m_1, m_2) = 1$ m prime, $m \mid q^2 - 1$	Theorem 6
>3	$\equiv_4 0$	$\sim \left(\frac{m_2+(3/2)m_1}{m_1 m_2} \right) q^{N/2}$	$m_1 m_2 = m + 5$ $m_1 > 7$ odd, $m_2 > 4$ $m \leq \frac{1}{4} \sqrt[4]{q}$	Sect. 8

The results of the present paper were originally the object of two separate preprints, available at [2, 3], to which we will sometimes refer for technical or straightforward parts of proofs. We will also refer to [1] for some of the preliminary notions.

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 . For the preliminary notions not recalled in this section, we refer to [1, Sect. 2].

2.1 Complete caps from bicovering arcs

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 both external to the segment $P_1 P_2$ and internal to the segment $P_3 P_4$. If every $P \in AG(2, q) \setminus A$ is bicovered by A , then A is said to be a bicovering arc. If there exists precisely one point $Q \in AG(2, q) \setminus A$ which is not bicovered by A , then A is said to be almost bicovering, and Q is called the center of A .

For a positive integer $N \equiv 0 \pmod{4}$, let $q' = q^{\frac{N-2}{2}}$. Points in $AG(N, q)$ can be identified with vectors of $\mathbb{F}_{q'} \times \mathbb{F}_{q'} \times \mathbb{F}_q \times \mathbb{F}_q$. A key tool in this paper is the following result from [12].

Proposition 1 *Let τ be a non-square in \mathbb{F}_q . If \mathcal{A} is a bicovering k -arc, then*

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

is a complete cap in $AG(N, q)$ of size $kq^{(N-2)/2}$. If \mathcal{A} is almost bicovering 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 .

2.2 Extensions of function fields

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 . Throughout the paper, we will refer to the following result a number of times.

Proposition 2 ([25, Proposition 3.7.3]) *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 $F' = F(y)$ 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*

$$r_\gamma := (m, v_\gamma(u)) > 0 \tag{2}$$

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 (2).

An extension such as F' in Proposition 2 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 2.

Proposition 3 *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 3 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}).

2.3 The Hasse–Weil bound

Proposition 4 (Hasse–Weil Bound, Theorem 5.2.3 in [25]) *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 $|N_q - (q + 1)| \leq 2g\sqrt{q}$.*

3 A family of curves over a finite field

Throughout this section, $q = p^h$ for some prime $p > 3$. Let m be a proper divisor of $q - 1$ with $(m, 6) = 1$. Also, t is a non-zero element in \mathbb{F}_q which is not an m -th power in \mathbb{F}_q . For $a, b \in \mathbb{F}_q$ with $ab \neq (a - 1)^3$, let $P = (a, b) \in AG(2, q)$. A crucial role for the investigation of the bicovering properties of a coset of the group associated to a singular non-cuspidal cubic is played by the curve

$$\mathcal{C}_P : f_{a,b,t,m}(X, Y) = 0, \quad (3)$$

where

$$f_{a,b,t,m}(X, Y) = a(t^3 X^{2m} Y^m + t^3 X^m Y^{2m} - 3t^2 X^m Y^m + 1) - bt^2 X^m Y^m - t^4 X^{2m} Y^{2m} + 3t^2 X^m Y^m - tX^m - tY^m. \quad (4)$$

In [27, 28], it is claimed without proof that \mathcal{C}_P is absolutely irreducible of genus less than or equal to some absolute constant times m^2 . The proof does not seem to be straightforward. In particular, Segre's criterion ([22]; see also [24, Lemma 8]) cannot be applied. Actually, for $a^3 = -1$ and $b = 1 - (a - 1)^3$, the polynomial $f_{a,b,t,m}(X, Y)$ is reducible; in fact,

$$f_{a,b,t,m}(X, Y) = -(a^2 + t^2 X^m Y^m - atY^m)(a^2 + t^2 X^m Y^m - atX^m).$$

The first result of this section is the existence of an absolutely irreducible component of \mathcal{C}_P defined over \mathbb{F}_q . We distinguish a number of cases.

3.1 $a^3 = -1$ and $b = 1 - (a - 1)^3$

If both $a^3 = -1$ and $b = 1 - (a - 1)^3$ hold, then the component of \mathcal{C}_P with equation $a^2 + t^2 X^m Y^m - atX^m = 0$ is a generalized Fermat curve over \mathbb{F}_q (see [10]). As proven in [10], such component is absolutely irreducible with genus less than m^2 .

Proposition 5 *Assume that $a^3 = -1$ and $b = 1 - (a - 1)^3$. Then, the curve \mathcal{C}_P has an irreducible component defined over \mathbb{F}_q of genus less than m^2 , with equation $a^2 + t^2 X^m Y^m - atX^m = 0$.*

3.2 $a \neq 0$ and either $a^3 \neq -1$ or $b \neq 1 - (a - 1)^3$

Lemma 1 *Assume that $ab \neq (a-1)^3$. Then the plane quartic curve $\mathcal{Q}_P : g_P(X, Y) = 0$ with*

$$g_P(X, Y) = a(t^3 X^2 Y + t^3 X Y^2 - 3t^2 X Y + 1) - bt^2 X Y \\ - t^4 X^2 Y^2 + 3t^2 X Y - tX - tY$$

is absolutely irreducible.

Proof The claim can be proved by standard arguments. Details can be found in the preliminary version of the present paper ([2, Lemma 1]). \square

Let \bar{u} and \bar{z} denote the rational functions of $\mathbb{K}(\mathcal{Q}_P)$ associated to the affine coordinates X and Y , respectively. Then

$$a(t^3 \bar{u}^2 \bar{z} + t^3 \bar{u} \bar{z}^2 - 3t^2 \bar{u} \bar{z} + 1) - bt^2 \bar{u} \bar{z} - t^4 \bar{u}^2 \bar{z}^2 + 3t^2 \bar{u} \bar{z} - t\bar{u} - t\bar{z} = 0. \quad (5)$$

By the proof of Lemma 1, as given in the preliminary version of the present paper [2], both X_∞ and Y_∞ are ordinary double points of \mathcal{Q}_P ; hence, they both are the center of two linear places of $\mathbb{K}(\bar{u}, \bar{z})$.

Lemma 2 *Let γ_1 be the linear place of $\mathbb{K}(\bar{u}, \bar{z})$ centered at X_∞ with tangent $Y = a/t$, and γ_2 the linear place of $\mathbb{K}(\bar{u}, \bar{z})$ centered at X_∞ with tangent $Y = 0$. Then*

$$v_{\gamma_1}(\bar{u}) = -1, \quad v_{\gamma_1}(\bar{z}) = 0,$$

and

$$v_{\gamma_2}(\bar{u}) = -1, \quad v_{\gamma_2}(\bar{z}) > 0.$$

Proof We keep the notation of Section 2.3 in [1]. Here, the roles of \bar{x} and \bar{y} are played by \bar{u} and \bar{z} , respectively. Then

$$v_{\gamma_1}(\bar{z} - a/t) + e_{\gamma_1} = j_2(\gamma_1), \quad (6)$$

$$v_{\gamma_1}(\bar{u}) + e_{\gamma_1} = 0, \quad (7)$$

$$v_{\gamma_1}(\bar{z}) + e_{\gamma_1} = 1. \quad (8)$$

From here, one can easily deduce that $v_{\gamma_1}(\bar{z}) = 0$. In fact, if $v_{\gamma_1}(\bar{z}) > 0$, then $v_{\gamma_1}(\bar{z} - a/t) = 0$, and hence $e_{\gamma_1} = j_2(\gamma_1)$; also, (8) implies $j_2(\gamma_1) = 1$, a contradiction. On the other hand, if $v_{\gamma_1}(\bar{z}) < 0$, then $v_{\gamma_1}(\bar{z} - a/t) = v_{\gamma_1}(\bar{z})$; hence, (6) and (8) yield that $j_2(\gamma_1) = 1$, a contradiction. From (8), it follows that $e_{\gamma_1} = 1$; then $v_{\gamma_1}(\bar{u}) = -1$ is obtained from (7).

As far as γ_2 is concerned, note that

$$v_{\gamma_2}(\bar{z} - a/t) + e_{\gamma_2} = 1, \quad (9)$$

$$v_{\gamma_2}(\bar{u}) + e_{\gamma_2} = 0, \quad (10)$$

$$v_{\gamma_2}(\bar{z}) + e_{\gamma_2} = j_2(\gamma_2). \quad (11)$$

Then, the assertion about γ_2 can be easily obtained from $j_2(\gamma_2) > 1$. \square

As \mathcal{Q}_P is left invariant by the transformation $X \mapsto Y$, $Y \mapsto X$, the following result is obtained at once.

Lemma 3 *Let γ_3 be the linear place of $\mathbb{K}(\bar{u}, \bar{z})$ centered at Y_∞ with tangent $X = a/t$, and γ_4 the linear place of $\mathbb{K}(\bar{u}, \bar{z})$ centered at Y_∞ with tangent $X = 0$. Then*

$$v_{\gamma_3}(\bar{u}) = 0, \quad v_{\gamma_3}(\bar{z}) = -1,$$

and

$$v_{\gamma_4}(\bar{u}) > 0, \quad v_{\gamma_4}(\bar{z}) = -1.$$

Let $Q_1 = (0, a/t)$ and $Q_2 = (a/t, 0)$. It is easily seen that both Q_1 and Q_2 are simple points of \mathcal{Q}_P , and hence they both are the center of precisely one linear place of $\mathbb{K}(\bar{u}, \bar{z})$.

Lemma 4 *Let γ_5 be the place of $\mathbb{K}(\bar{u}, \bar{z})$ centered at Q_1 , and γ_6 the place centered at Q_2 . Then*

$$\text{div}(\bar{u}) = \gamma_4 + \gamma_5 - \gamma_1 - \gamma_2,$$

and

$$\text{div}(\bar{z}) = \gamma_2 + \gamma_6 - \gamma_3 - \gamma_4.$$

Proof Clearly, γ_5 is a zero of \bar{u} , whereas γ_6 is a zero of \bar{z} . From (5), the number of zeros (and poles) of either \bar{u} or \bar{z} is 2. Then, the assertion follows from Lemmas 2 and 3. \square

We now consider the extension $\mathbb{K}(\bar{u}, \bar{z})(\bar{y})$ of $\mathbb{K}(\bar{u}, \bar{z})$ defined by the equation $\bar{y}^m = \bar{z}$. Clearly, $\mathbb{K}(\bar{u}, \bar{z}, \bar{y}) = \mathbb{K}(\bar{u}, \bar{y})$ holds. By Lemma 4, $\mathbb{K}(\bar{u}, \bar{y})$ is a Kummer extension of $\mathbb{K}(\bar{u}, \bar{z})$. For a place γ of $\mathbb{K}(\bar{u}, \bar{z})$, let $r_\gamma = \gcd(m, v_\gamma(\bar{z}))$. Then by Lemma 4, we have

$$\begin{cases} r_\gamma = 1, & \text{if } \gamma \in \{\gamma_2, \gamma_3, \gamma_4, \gamma_6\}, \\ r_\gamma = m, & \text{otherwise.} \end{cases}$$

By Proposition 2, the genus of $\mathbb{K}(\bar{u}, \bar{y})$ is equal to $2m - 1 + m(g - 1)$, where g denotes the genus of \mathcal{Q}_P . Since \mathcal{Q}_P is a quartic with two double points, $g \leq 1$ holds, and hence the genus of $\mathbb{K}(\bar{u}, \bar{z}, \bar{y})$ is less than or equal to $2m - 1$. Also, the places of $\mathbb{K}(\bar{u}, \bar{z})$ which ramify in the extension $\mathbb{K}(\bar{u}, \bar{y}) : \mathbb{K}(\bar{u}, \bar{z})$ are precisely $\gamma_2, \gamma_3, \gamma_4, \gamma_6$; their ramification index is m . For $i \in \{2, 3, 4, 6\}$ let $\bar{\gamma}_i$ be the only place of $\mathbb{K}(\bar{u}, \bar{y})$ lying over γ_i ; also, let $\bar{\gamma}_1^1, \dots, \bar{\gamma}_1^m$ be the places of $\mathbb{K}(\bar{u}, \bar{y})$ lying over γ_1 , and let $\bar{\gamma}_5^1, \dots, \bar{\gamma}_5^m$ be the places of $\mathbb{K}(\bar{u}, \bar{y})$ lying over γ_5 . Taking into account Lemma 4, the divisor of \bar{u} in $\mathbb{K}(\bar{u}, \bar{y})$ can be easily computed.

Lemma 5 *In $\mathbb{K}(\bar{u}, \bar{y})$,*

$$\text{div}(\bar{u}) = m\bar{\gamma}_4 + \sum_{i=1}^m \bar{\gamma}_5^i - m\bar{\gamma}_2 - \sum_{i=1}^m \bar{\gamma}_1^i.$$

We can now apply Proposition 2, together with Lemma 5, in order to deduce that the extension $\mathbb{K}(\bar{u}, \bar{y})(\bar{x}) = \mathbb{K}(\bar{y}, \bar{x})$ of $\mathbb{K}(\bar{u}, \bar{y})$ defined by the equation $\bar{x}^m = \bar{u}$ is a Kummer extension of $\mathbb{K}(\bar{u}, \bar{y})$ of genus

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

where g' is the genus of $\mathbb{K}(\bar{u}, \bar{y})$. Taking into account that $g' \leq 2m - 1$, the following result is obtained.

Lemma 6 *The genus of $\mathbb{K}(\bar{x}, \bar{y})$ is at most $3m^2 - 3m + 1$.*

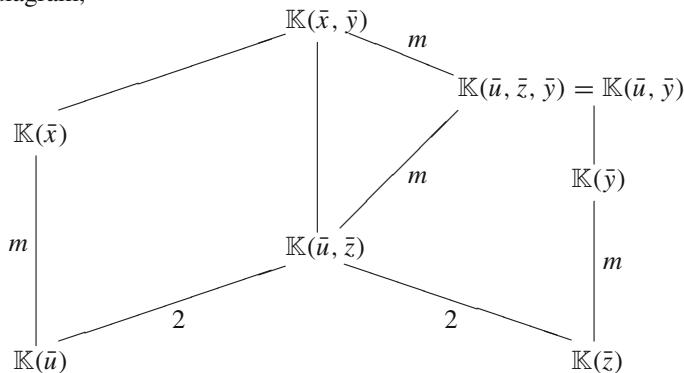
Proposition 6 *Assume that $a \neq 0$ and either $a^3 \neq -1$ or $b \neq 1 - (a - 1)^3$. Then, the curve \mathcal{C}_P is an absolutely irreducible curve defined over \mathbb{F}_q with genus less than or equal to $3m^2 - 3m + 1$.*

Proof Suppose that $f_{a,b,t,m}(X, Y)$ admits a non-trivial factorization

$$f_{a,b,t,m}(X, Y) = g_1(X, Y)^{m_1} \cdots g_s(X, Y)^{m_s}.$$

By construction, $f_{a,b,t,m}(\bar{x}, \bar{y}) = 0$ holds, and hence there exists $i_0 \in \{1, \dots, s\}$ such that $g_{i_0}(\bar{x}, \bar{y}) = 0$. Clearly, either $\deg_X(g_{i_0}) < 2m$ or $\deg_Y(g_{i_0}) < 2m$ holds. To get a contradiction, it is then enough to show that the extensions $\mathbb{K}(\bar{x}, \bar{y}) : \mathbb{K}(\bar{x})$ and $\mathbb{K}(\bar{x}, \bar{y}) : \mathbb{K}(\bar{y})$ have both degree $2m$.

From the diagram,



it follows that $[\mathbb{K}(\bar{x}, \bar{y}) : \mathbb{K}(\bar{u})] = [\mathbb{K}(\bar{x}, \bar{y}) : \mathbb{K}(\bar{z})] = 2m^2$; hence, both $[\mathbb{K}(\bar{x}, \bar{y}) : \mathbb{K}(\bar{y})] = 2m$ and $[\mathbb{K}(\bar{x}, \bar{y}) : \mathbb{K}(\bar{x})] = 2m$ hold.

Then $\mathbb{K}(\bar{x}, \bar{y})$ is the function field of \mathcal{C}_P , and the assertion on the genus follows from Lemma 6. \square

3.3 $a = 0$

Lemma 7 *The plane quartic curve \mathcal{Q}_P with equation*

$$-bt^2XY - t^4X^2Y^2 + 3t^2XY - tX - tY = 0$$

is absolutely irreducible of genus $g \leq 1$.

Proof The claim can be proved by standard arguments. Details can be found in the preliminary version of the present paper ([2, Lemma 7]). \square

Let $\mathbb{K}(\bar{u}, \bar{z})$ be the function field of \mathcal{Q}_P . Here, \bar{u} and \bar{z} are rational functions on \mathcal{Q}_P such that

$$-bt^2\bar{u}\bar{z} - t^4\bar{u}^2\bar{z}^2 + 3t^2\bar{u}\bar{z} - t\bar{u} - t\bar{z} = 0.$$

Let γ_1 be the only place of $\mathbb{K}(\bar{u}, \bar{z})$ centered at the (simple) point of \mathcal{Q}_P with coordinates $(0, 0)$. From the proof of Lemma 7, as given in [2], there is precisely one place of $\mathbb{K}(\bar{u}, \bar{z})$, say γ_2 , centered at Y_∞ . As \mathcal{Q}_P is left invariant by the transformation $X \mapsto Y$, $Y \mapsto X$, the same holds for X_∞ ; we denote by γ_3 the only place of $\mathbb{K}(\bar{u}, \bar{z})$ centered at X_∞ . Arguing as in the proofs of Lemmas 2, 3, and 4, the divisors of both \bar{u} and \bar{z} can be computed.

Lemma 8 *In $\mathbb{K}(\bar{u}, \bar{z})$,*

$$\operatorname{div}(\bar{u}) = \gamma_1 + \gamma_2 - 2\gamma_3, \quad \operatorname{div}(\bar{z}) = \gamma_1 + \gamma_3 - 2\gamma_2.$$

In order to prove that \mathcal{C}_P is absolutely irreducible, the same arguments as in Sect. 3.2 can be used. Let $\mathbb{K}(\bar{u}, \bar{z})(\bar{y})$ be the extension of $\mathbb{K}(\bar{u}, \bar{z})$ defined by the equation $\bar{y}^m = \bar{z}$. Clearly, $\mathbb{K}(\bar{u}, \bar{z}, \bar{y}) = \mathbb{K}(\bar{u}, \bar{y})$ holds. By Lemma 8, $\mathbb{K}(\bar{u}, \bar{y})$ is a Kummer extension of $\mathbb{K}(\bar{u}, \bar{z})$. As m is odd, by Lemma 8, we have that

$$\begin{cases} r_\gamma = 1, & \text{if } \gamma \in \{\gamma_1, \gamma_2, \gamma_3\}, \\ r_\gamma = m, & \text{otherwise.} \end{cases}$$

By Proposition 2, the genus of $\mathbb{K}(\bar{u}, \bar{y})$ is equal to

$$g' = m(g - 1) + \frac{3m - 1}{2}, \quad (12)$$

where $g \in \{0, 1\}$ denotes the genus of \mathcal{Q}_P . Also, the places of $\mathbb{K}(\bar{u}, \bar{z})$ which ramify in the extension $\mathbb{K}(\bar{u}, \bar{y}) : \mathbb{K}(\bar{u}, \bar{z})$ are precisely $\gamma_1, \gamma_2, \gamma_3$; their ramification index is m . For $i \in \{1, 2, 3\}$, let $\bar{\gamma}_i$ be the only place of $\mathbb{K}(\bar{u}, \bar{y})$ lying over γ_i . Taking into account Lemma 8, the divisors of both \bar{u} and \bar{y} in $\mathbb{K}(\bar{u}, \bar{y})$ can be easily computed.

Lemma 9 In $\mathbb{K}(\bar{u}, \bar{y})$,

$$\text{div}(\bar{u}) = m\bar{\gamma}_1 + m\bar{\gamma}_2 - 2m\bar{\gamma}_3, \quad \text{div}(\bar{y}) = \bar{\gamma}_1 + \bar{\gamma}_3 - 2\bar{\gamma}_2.$$

We now consider the extension $\mathbb{K}(\bar{u}, \bar{y})(\bar{x}) = \mathbb{K}(\bar{y}, \bar{x})$ of $\mathbb{K}(\bar{u}, \bar{y})$ such that $\bar{x}^m = \bar{u}$. In order to apply Proposition 2, we need to determine whether the rational function \bar{u} is an e -th power in $\mathbb{K}(\bar{u}, \bar{y})$, for some divisor e of m .

Lemma 10 The rational function \bar{u} is not an e -th power in $\mathbb{K}(\bar{u}, \bar{y})$ for any divisor $e > 1$ of m .

Proof Assume that $\bar{u} = \bar{v}^e$, with e a non-trivial divisor of m . Then

$$\text{div}(\bar{v}) = \frac{m}{e}\bar{\gamma}_1 + \frac{m}{e}\bar{\gamma}_2 - \frac{2m}{e}\bar{\gamma}_3.$$

Consider the rational function $\bar{v}\bar{y}^i$ for $-\frac{m}{e} \leq i \leq (\frac{m}{e} - 1)/2$. The pole divisor of $\bar{v}\bar{y}^i$ is $(\frac{2m}{e} - i)\bar{\gamma}_3$, which shows that the Weierstrass semigroup $H(\bar{\gamma}_3)$ at $\bar{\gamma}_3$ contains

$$\frac{3m}{2e} + \frac{1}{2}, \frac{3m}{2e} + \frac{3}{2}, \dots, \frac{3m}{e},$$

and hence every integer greater than or equal to $\frac{3m}{2e} + \frac{1}{2}$. As g' is equal to the number of gaps in $H(\bar{\gamma}_3)$, we have

$$g' \leq \frac{3m}{2e} - \frac{1}{2};$$

by (12), this can only happen when both $e = 3$ and $g' = (m - 1)/2$ hold. This is impossible as $(m, 6) = 1$ is assumed. \square

Arguing as in the proofs of Lemma 6 and Proposition 6, the following result is obtained.

Proposition 7 *Assume that $a = 0$. Then, the curve \mathcal{C}_P is an absolutely irreducible curve defined over \mathbb{F}_q with genus less than or equal to $\frac{3m^2-3m+2}{2}$.*

3.4 Some double covers of \mathcal{C}_P

In the three-dimensional space over \mathbb{K} , fix an affine coordinate system (X, Y, W) and for any $c \in \mathbb{K}$, $c \neq 0$, let \mathcal{Y}_P be the curve defined by

$$\mathcal{Y}_P : \begin{cases} W^2 = c(a - tX^m)(a - tY^m) \\ f_{a,b,t,m}(X, Y) = 0 \end{cases}.$$

The existence of a suitable \mathbb{F}_q -rational point of \mathcal{Y}_P will guarantee that P is bicovered by the arc comprising the points of a coset of index m in the abelian group of the non-singular \mathbb{F}_q -rational points of a nodal cubic; see Sect. 4.

Proposition 8 *Let $a, b \in \mathbb{F}_q$ be such that $ab \neq (a-1)^3$. For each $c \in \mathbb{F}_q$, $c \neq 0$, the space curve \mathcal{Y}_P has an irreducible component defined over \mathbb{F}_q with genus less than or equal to $6m^2 - 4m + 1$.*

Proof We distinguish a number of cases.

Case 1: $a^3 = -1$ and $b = 1 - (a-1)^3$.

Notation here is as in Sect. 3.1. The function field of an \mathbb{F}_q -rational irreducible component \mathcal{C} of \mathcal{C}_P is $\mathbb{K}(\bar{x}, \bar{y})$ with

$$a^2 + t^2 \bar{x}^m \bar{y}^m - at \bar{x}^m = 0.$$

By the results on generalized Fermat curves presented in [10], the genus of \mathcal{C} is $(m^2 - 3m + 2)/2$; also, there are m places, say $\gamma_1^1, \dots, \gamma_1^m$ of $\mathbb{K}(\bar{x}, \bar{y})$ centered at X_∞ , and m places, say $\gamma_2^1, \dots, \gamma_2^m$ of $\mathbb{K}(\bar{x}, \bar{y})$ centered at Y_∞ . Let $\gamma_3^1, \dots, \gamma_3^m$ denote the places centered at the m simple affine points of \mathcal{C} with coordinates $(v, 0)$ with $v^m = a/t$. We have

$$\begin{aligned} \operatorname{div}(\bar{x}) &= \gamma_2^1 + \dots + \gamma_2^m - (\gamma_1^1 + \dots + \gamma_1^m), \\ \operatorname{div}(\bar{y}) &= \gamma_3^1 + \dots + \gamma_3^m - (\gamma_2^1 + \dots + \gamma_2^m). \end{aligned}$$

Then, it is easy to see that

$$\begin{aligned} \operatorname{div}(a - t\bar{x}^m) &= m(\gamma_3^1 + \dots + \gamma_3^m) - m(\gamma_1^1 + \dots + \gamma_1^m), \\ \operatorname{div}(a - t\bar{y}^m) &= m(\gamma_1^1 + \dots + \gamma_1^m) - m(\gamma_2^1 + \dots + \gamma_2^m), \end{aligned}$$

whence

$$\operatorname{div}((a - t\bar{x}^m)(a - t\bar{y}^m)) = m(\gamma_3^1 + \dots + \gamma_3^m) - m(\gamma_2^1 + \dots + \gamma_2^m).$$

As m is odd, this yields that $(a - t\bar{x}^m)(a - t\bar{y}^m)$ is not a square in $\mathbb{K}(\bar{x}, \bar{y})$. By Proposition 3, for each $c \in \mathbb{F}_q, c \neq 0$, the space curve with equations

$$\begin{cases} W^2 = c(a - tX^m)(a - tY^m) \\ a^2 + t^2X^mY^m - atX^m = 0 \end{cases}$$

has an irreducible component defined over \mathbb{F}_q with genus $m^2 - 2m + 1$. The claim then follows as such curve is contained in \mathcal{Y}_P as well.

Case 2: $a \neq 0$ and either $a^3 \neq -1$ or $b \neq 1 - (a - 1)^3$.

We keep the notation of Sect. 3.2. By Lemma 5, the only places of $\mathbb{K}(\bar{u}, \bar{y})$ which ramify in the extension $\mathbb{K}(\bar{x}, \bar{y}) : \mathbb{K}(\bar{u}, \bar{y})$ are $\bar{\gamma}_1^1, \dots, \bar{\gamma}_1^m$ and $\bar{\gamma}_5^1, \dots, \bar{\gamma}_5^m$; their common ramification index is m . Therefore, 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. 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 $\mathbb{K}(\bar{u}, \bar{z})$.

From Eqs. (6)–(11), together with Lemma 4, we deduce that in $\mathbb{K}(\bar{u}, \bar{z})$,

$$\operatorname{div}(a - t\bar{z}) = \operatorname{div}(\bar{z} - a/t) = \gamma_1 + \gamma_5 - \gamma_3 - \gamma_4$$

holds; similarly,

$$\operatorname{div}(a - t\bar{u}) = \operatorname{div}(\bar{u} - a/t) = \gamma_3 + \gamma_6 - \gamma_1 - \gamma_2.$$

This implies that in $\mathbb{K}(\bar{x}, \bar{y})$,

$$\operatorname{div}((a - t\bar{x}^m)(a - t\bar{y}^m)) = m \left(\sum_{i=1}^m (\bar{\gamma}_5^i + \bar{\gamma}_6^i - \bar{\gamma}_4^i - \bar{\gamma}_2^i) \right) \quad (13)$$

holds. As m is odd, this yields that $(a - t\bar{x}^m)(a - t\bar{y}^m)$ is not a square in $\mathbb{K}(\bar{x}, \bar{y})$. By Proposition 3 for each $c \in \mathbb{F}_q, c \neq 0$, the curve \mathcal{Y}_P has an irreducible component defined over \mathbb{F}_q with genus at most $6m^2 - 4m + 1$.

Case 3: $a = 0$. We keep the notation of Sect. 3.3. The curve \mathcal{C}_P is absolutely irreducible, and for each $i \in \{1, 2, 3\}$, the ramification index of γ_i in the extension $\mathbb{K}(\bar{x}, \bar{y})$ over $\mathbb{K}(\bar{u}, \bar{z})$ is equal to m . By Lemma 8, the divisor of $\bar{u}\bar{z}$ in $\mathbb{K}(\bar{u}, \bar{z})$ is $2\gamma_1 - \gamma_2 - \gamma_3$. Hence, in $\mathbb{K}(\bar{x}, \bar{y})$, the rational function $t^2\bar{x}^m\bar{y}^m = t^2\bar{u}\bar{z}$ has m zeros with multiplicity $2m$ (the places of $\mathbb{K}(\bar{x}, \bar{y})$ lying over γ_1) and $2m$ poles with multiplicity m (the places lying over γ_2 and γ_3). As m is odd and $a = 0$, this yields that $(a - t\bar{x}^m)(a - t\bar{y}^m)$ is not a square in $\mathbb{K}(\bar{x}, \bar{y})$. Also, by Proposition 3, for each $c \in \mathbb{F}_q, c \neq 0$, the curve \mathcal{Y}_P has an irreducible component defined over \mathbb{F}_q with genus at most $3m^2 - 2m + 1$. \square

4 Bicovery arcs from nodal cubics

Let \mathcal{X} be a singular plane cubic defined over \mathbb{F}_q with a node and at least one \mathbb{F}_q -rational inflection, and let G denote the set of non-singular \mathbb{F}_q -rational points of \mathcal{X} . Then, a

canonical equation for \mathcal{X} is $XY = (X-1)^3$. If the neutral element of the group (G, \oplus) is chosen to be the affine point $(1, 0)$, then (G, \oplus) is isomorphic to (\mathbb{F}_q^*, \cdot) via the map $v \mapsto (v, (v-1)^3/v)$.

Let K be the subgroup of G of index m with $(m, 6) = 1$, and let $P_t = (t, (t-1)^3/t)$ be a point in $G \setminus K$. Then, the coset $K_t = K \oplus P_t$ is an arc. In order to investigate the bicovering properties of the arc K_t it is useful to write K_t in an algebraically parametrized form:

$$K_t = \left\{ \left(tw^m, \frac{(tw^m - 1)^3}{tw^m} \right) \mid w \in \mathbb{F}_q^* \right\}.$$

For a point $P = (a, b)$ in $AG(2, q) \setminus \mathcal{X}$, let $f_{a,b,t,m}(X, Y)$ be as in (4).

Proposition 9 *An affine point $P = (a, b)$ in $AG(2, q) \setminus \mathcal{X}$ is collinear with two distinct points in K_t if and only if there exist $\tilde{x}, \tilde{y} \in \mathbb{F}_q^*$ with $\tilde{x}^m \neq \tilde{y}^m$ such that $f_{a,b,t,m}(\tilde{x}, \tilde{y}) = 0$.*

Proof The claim follows by straightforward computation. Details can be found in the preliminary version of the present paper ([2, Proposition 10]). \square

Proposition 10 *If*

$$q + 1 - (12m^2 - 8m + 2)\sqrt{q} \geq 8m^2 + 8m + 1, \quad (14)$$

then every point P in $AG(2, q)$ off \mathcal{X} is bicovered by K_t .

Proof We only deal with the case where $a \neq 0$ and either $a^3 \neq -1$ or $b \neq 1 - (a-1)^3$, the proofs for the other cases being analogous. Fix a non-zero element c in \mathbb{F}_q and let \mathcal{Y}_P be as in Proposition 8. Let $\mathbb{K}(\bar{x}, \bar{y}, \bar{w})$ be the function field of \mathcal{Y}_P , so that

$$\begin{cases} \bar{w}^2 = c(a - t\bar{x}^m)(a - t\bar{y}^m) \\ f_{a,b,t,m}(\bar{x}, \bar{y}) = 0 \end{cases}.$$

We argue as in the proof of Theorem 4.5 in [1]. Let E be the set of places γ of $\mathbb{K}(\bar{x}, \bar{y}, \bar{w})$ for which at least one of the following holds:

- (1) γ is either a zero or a pole of \bar{x} ;
- (2) γ is either a zero or a pole of \bar{y} ;
- (3) γ is either a zero or a pole of \bar{w} ;
- (4) γ is a zero of $\bar{x}^m - \bar{y}^m$.

We are going to show that the size of E is at most $8m^2 + 8m$. It has already been noticed in the proof of Proposition 8, Case 2, that the only places of $\mathbb{K}(\bar{u}, \bar{z})$ that ramify in $\mathbb{K}(\bar{x}, \bar{y})$ are the places γ_j for $j = 1, \dots, 6$, and their common ramification index is m . Also, by (13), the degree-2 extension $\mathbb{K}(\bar{x}, \bar{y}, \bar{w})$ over $\mathbb{K}(\bar{x}, \bar{y})$ ramifies precisely at the places of $\mathbb{K}(\bar{x}, \bar{y})$ lying over $\gamma_2, \gamma_4, \gamma_5, \gamma_6$. Let Ω_j be the set of places

of $\mathbb{K}(\bar{x}, \bar{y}, \bar{w})$ lying over γ_j . Note that $|\Omega_1| = |\Omega_3| = 2m$ and $|\Omega_j| = m$ for each j in $\{2, 4, 5, 6\}$. From Lemma 4, we have that in $\mathbb{K}(\bar{x}, \bar{y}, \bar{w})$,

$$\begin{aligned}\operatorname{div}(\bar{x}) &= \sum_{\gamma \in \Omega_4 \cup \Omega_5} 2\gamma - \sum_{\gamma \in \Omega_2} 2\gamma - \sum_{\gamma \in \Omega_1} \gamma, \\ \operatorname{div}(\bar{y}) &= \sum_{\gamma \in \Omega_2 \cup \Omega_6} 2\gamma - \sum_{\gamma \in \Omega_4} 2\gamma - \sum_{\gamma \in \Omega_3} \gamma.\end{aligned}$$

Also, by (13),

$$\operatorname{div}(\bar{w}) = m \left(\sum_{\gamma \in \Omega_5 \cup \Omega_6} \gamma - \sum_{\gamma \in \Omega_2 \cup \Omega_4} \gamma \right).$$

As regards $\bar{x}^m - \bar{y}^m = \bar{u} - \bar{z}$, 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 E' of the zeros of $\bar{x}^m - \bar{y}^m$ in $\mathbb{K}(\bar{x}, \bar{y}, \bar{w})$ has size at most $8m^2$. Clearly, any place of E is contained either in E' or in Ω_j for some $j = 1, \dots, 6$, whence $|E| \leq 8m^2 + 8m$.

Our assumption on q and m , together with the Hasse-Weil bound, ensure the existence of at least $8m^2 + 8m + 1$ \mathbb{F}_q -rational places of $\mathbb{K}(\bar{x}, \bar{y}, \bar{w})$; hence, there exists at least one \mathbb{F}_q -rational place γ_c of $\mathbb{K}(\bar{x}, \bar{y}, \bar{w})$ not in E . Let

$$\tilde{x} = \bar{x}(\gamma_c), \quad \tilde{y} = \bar{y}(\gamma_c), \quad \tilde{w} = \bar{w}(\gamma_c).$$

Note that $P_c = (\tilde{x}, \tilde{y})$ is an \mathbb{F}_q -rational affine point of the curve with equation $f_{a,b,t,m}(X, Y) = 0$. Therefore, by Proposition 9, P is collinear with two distinct points

$$P_{1,c} = \left(t\tilde{x}^m, \frac{(t\tilde{x}^m - 1)^3}{t\tilde{x}^m} \right), \quad P_{2,c} = \left(t\tilde{y}^m, \frac{(t\tilde{y}^m - 1)^3}{t\tilde{y}^m} \right) \in K_t.$$

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

As $m > 2$, the coset K_t cannot bicover all the \mathbb{F}_q -rational affine points in \mathcal{X} . Therefore, unions of distinct cosets need to be considered.

Proposition 11 *Let $K_{t'}$ be a coset of K such that $K_t \cup K_{t'}$ is an arc. Let P_0 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 $K_{t'}$. If (14) holds, then P_0 is bicovered by $K_t \cup K_{t'}$.*

Proof Let $P_0 = (u_0, (u_0 - 1)^3/u_0)$ with $u_0 \neq 0$. Note that when P ranges over K_t , then the point $Q = \ominus(P_0 \oplus P)$ is collinear with P_0 and ranges over $K_{t'}$. Recall that P belongs to K_t if and only if

$$P = \left(tx^m, \frac{(tx^m - 1)^3}{tx^m} \right)$$

for some $x \in \mathbb{F}_q^*$. In this case,

$$Q = \left(\frac{1}{u_0 t x^m}, \frac{(1 - u_0 t x^m)^3}{(u_0 t x^m)^2} \right).$$

Let \bar{x} be a transcendental element over \mathbb{K} . In order to determine whether P_0 is bcovered by $K_t \cup K_{t'}$, we need to investigate whether the following rational function is a non-square in $\mathbb{K}(\bar{x})$:

$$\eta(\bar{x}) = (u_0 - t\bar{x}^m) \left(u_0 - \frac{1}{u_0 t \bar{x}^m} \right) = \frac{(u_0 - t\bar{x}^m)(u_0^2 t \bar{x}^m - 1)}{u_0 t \bar{x}^m}.$$

Let γ_0 and γ_∞ be the zero and the pole of \bar{x} in $\mathbb{K}(\bar{x})$, respectively. Note that both γ_0 and γ_∞ are poles of $\eta(\bar{x})$ of multiplicity m , since γ_∞ is a pole of order m of $(u_0 - t\bar{x}^m)$, $(u_0^2 t \bar{x}^m - 1)$, and $u_0 t \bar{x}^m$; hence, $v_{\gamma_\infty}(\eta(\bar{x})) = -m - m - (-m) = -m$. Also, γ_0 is a zero of $u_0 t \bar{x}^m$ of multiplicity m . As m is odd, $\eta(\bar{x})$ is not a square in $\mathbb{K}(\bar{x})$. Then Proposition 3 applies to $c\eta(\bar{x})$ for each $c \in \mathbb{F}_q^*$. Since $\eta(\bar{x})$ has exactly two poles, and the number of its zeros 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 m .

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 or a pole of \bar{w} . Let $\tilde{x} = \bar{x}(\gamma_c)$, $\tilde{w} = \bar{w}(\gamma_c)$. Therefore, P_0 is collinear with two distinct points

$$P(c) = \left(t\tilde{x}^m, \frac{(\tilde{x}^m - 1)^3}{t\tilde{x}^m} \right) \in K_t, \quad Q(c) = \left(\frac{1}{u_0 t \tilde{x}^m}, \frac{(1 - u_0 t \tilde{x}^m)^3}{(u_0 t \tilde{x}^m)^2} \right) \in K_{t'}.$$

If c is chosen to be a square, then P_0 is external to $P(c)Q(c)$; on the other hand, if c is not a square, then P_0 is internal to $P(c)Q(c)$. \square

In order to construct bicovering arcs contained in \mathcal{X} , the notion of a maximal-3-independent subset of a finite abelian group \mathcal{G} is needed, as given in [30]. 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*. Now, 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, \oplus) ; see [30, Lemma 1]. In geometrical terms, 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 . By Propositions 10 and 11, if K is large enough with respect to q , then S is a bicovering arc as well, and the following result holds.

Theorem 1 *Let m be a proper divisor of $q - 1$ such that $(m, 6) = 1$ and (14) holds. Let K be a subgroup of G of index m . For M a maximal 3-independent subset of the*

factor group G/K , the point set

$$S = \bigcup_{K_{t_i} \in M} K_{t_i}$$

is a bicovering arc in $AG(2, q)$ of size $\#M \cdot \frac{q-1}{m}$.

5 Complete caps from nodal cubics

We use Theorem 1, together with Proposition 1, in order to construct small complete caps in affine spaces $AG(N, q)$. Note that (14) holds when

$$\sqrt{q} \geq 6m^2 - 4m + 1 + \sqrt{36m^4 - 48m^3 + 36m^2 + 1},$$

which is clearly implied by $m \leq \frac{\sqrt[4]{q}}{3.5}$.

Corollary 1 *Let m be a proper divisor of $q - 1$ such that $(m, 6) = 1$ and $m \leq \frac{\sqrt[4]{q}}{3.5}$. Assume that the cyclic group of order m admits a maximal 3-independent subset of size s . Then,*

- (i) *there exists a bicovering arc in $AG(2, q)$ of size $\frac{s(q-1)}{m}$;*
- (ii) *for $N \equiv 0 \pmod{4}$, $N \geq 4$, there exists a complete cap in $AG(N, q)$ of size*

$$\frac{s(q-1)}{m} q^{\frac{N-2}{2}}.$$

In the case where a group \mathcal{G} is the direct product of two groups $\mathcal{G}_1, \mathcal{G}_2$ of order at least 4, neither of which elementary 3-abelian, there exists a maximal 3-independent subset of \mathcal{G} of size less than or equal to $(\#\mathcal{G}_1) + (\#\mathcal{G}_2)$; see [27]. Then, Theorem 2 below follows at once from Corollary 1.

Theorem 2 *Let $q = p^h$ with $p > 3$ a prime, and let m be a proper divisor of $q - 1$ such that $(m, 6) = 1$ and $m \leq \frac{\sqrt[4]{q}}{3.5}$. Assume that $m = m_1 m_2$ with $(m_1, m_2) = 1$. Then,*

- (i) *there exists a bicovering arc in $AG(2, q)$ of size less than or equal to*

$$\frac{(m_1 + m_2)(q - 1)}{m_1 m_2};$$

- (ii) *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*

$$\frac{(m_1 + m_2)(q - 1)}{m_1 m_2} q^{\frac{N-2}{2}}.$$

5.1 Comparison with previous results

We distinguish two possibilities for the integer h such that $q = p^h$.

5.1.1 $h \leq 8$

The best previously known general construction of complete caps in $AG(N, q)$ is that given in [4], providing complete caps of size approximately $q^{N/2}/3$. It is often possible to choose m_1 and m_2 as in Theorem 2 in such a way that the value $(m_1 + m_2)/m_1m_2$ is significantly smaller than $1/3$.

This happens for instance for all $q = p^h$ such that $p - 1$ has a composite divisor $m < \sqrt[4]{p}/3.5$ with $(m, 6) = 1$.

For $p > 3$ generic, when $h = 8$ a possible choice for m is $m = (p^2 - 1)/(2^s 3^k)$, where $2^s \geq 4$ is the highest power of 2 which divides $p^2 - 1$, and similarly $3^k \geq 3$ is the highest power of 3 which divides $p^2 - 1$.

Assume first that 3 divides $p - 1$, so that $(3, p + 1) = 1$. Then $m = m_1 m_2$, where $m_1 = (p - 1)/(2^{s_1} 3^k)$ and $m_2 = (p + 1)/2^{s_2}$ with $s_1 + s_2 = s$. Then, Theorem 2 provides complete caps in $AG(N, q)$ of size approximately at most

$$(2^{s_2} + 2^{s_1} 3^k) q^{\frac{N}{2} - \frac{1}{8}}.$$

If 3 divides $p + 1$, then a similar bound can be obtained.

5.1.2 $h > 8$

The smallest known complete caps in $AG(N, q)$ have size approximately

$$2q^{N/2}/p^{\lfloor (\lceil h/4 \rceil - 1)/2 \rfloor},$$

see [1, Theorem 6.2]. Theorem 2 provides an improvement on such bound whenever it is possible to choose m_1 and m_2 so that

$$(m_1 + m_2)/m_1 m_2 < 2/p^{\lfloor (\lceil h/4 \rceil - 1)/2 \rfloor}. \quad (15)$$

This certainly happens for instance when $h \equiv 0 \pmod{8}$ and p is large enough. Let $2^s \geq 4$ be the highest power of 2 which divides $\sqrt[4]{q} - 1$, and similarly $3^k \geq 3$ the highest power of 3 which divides $\sqrt[4]{q} - 1$. Then, it is easy to see that one can choose m_1 and m_2 so that

$$\frac{m_1 + m_2}{m_1 m_2} \sim (2^{s_2} + 2^{s_1} 3^k) q^{-\frac{1}{8}},$$

with $s_1 + s_2 = s$. On the other hand, $2/p^{\lfloor (\lceil h/4 \rceil - 1)/2 \rfloor} = 2pq^{-\frac{1}{8}}$.

Another family of qs for which (15) happens is $q = p^{12}$, with $p \equiv 1 \pmod{12}$ and $(p^2 + 1)/2$ a composite integer. Assume that $(p^2 + 1)/2 = v_1 v_2$ with $v_1, v_2 >$

1 and $v_1 < v_2$. Then, choosing $m_1 = v_1(p + 1)/2$ and $m_2 = v_2$, we have that $(m_1 + m_2)/m_1m_2 < 2/p$.

6 Cubics with an isolated double point

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} .

6.1 Further properties of the algebraic curves of Sect. 3

Assume that 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 $A, B \in \mathbb{F}_{q^2}$ be such that

$$AB \neq (A - 1)^3, \quad A \neq 0, \quad \text{either } A^3 \neq -1 \text{ or } B \neq 1 - (A - 1)^3. \quad (16)$$

From the results of Sect. 3, the curve with equation $f_{A,B,\bar{t},m}(X, Y) = 0$ is absolutely irreducible of genus $g \leq 3m^2 - 3m + 1$. Also, the following results hold for its function field $\mathbb{K}(\bar{x}, \bar{y})$ and for the subfield $\mathbb{K}(\bar{u}, \bar{z})$, where $\bar{u} = \bar{x}^m$ and $\bar{z} = \bar{y}^m$.

Proposition 12 *In $\mathbb{K}(\bar{u}, \bar{z})$, there exist six places γ_j , $j = 1, \dots, 6$, such that*

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

Proposition 13 *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.*

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 14 *In $\mathbb{K}(\bar{x}, \bar{y})$,*

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

In order to investigate the bicovering properties of a coset of index m in the abelian group of the non-singular \mathbb{F}_q -rational points of \mathcal{X} , 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 15 Assume that A and B satisfy conditions (16). 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

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

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 Proposition 12, 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,

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

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

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

where D is a divisor of degree 4 whose support is disjoint from $\{\gamma_i \mid i = 1, \dots, 6\}$. Therefore, by Proposition 13,

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

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 14, 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 2 yields (iii). \square

6.2 Covering properties of certain subsets 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 $v, w \in \mathbb{K}^*$,

$$Q_v \oplus Q_w = Q_{vw}. \quad (17)$$

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 (17),

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

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

$$K_{\bar{t}} = \{Q_{\bar{t}(\frac{u+\beta}{u-\beta})^m} \mid u \in \mathbb{F}_q\} \cup \{Q_{\bar{t}}\}. \quad (18)$$

Throughout this section, a and b are fixed 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 The proof is a straightforward computation. For the details, see the preliminary version of the present paper ([3, Lemma 11]). \square

The curve with equation $L_{a,b,\bar{t},m}(X, Y) = 0$ actually belongs to the family described in Sect. 6.1.

Lemma 12 *Let*

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

Then

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

where $f_{A,B,\bar{i},m}$ is defined as in (4).

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*

$$(a, b) \notin \left\{ \left(0, -\frac{9}{8\beta^2} \right), \left(\beta\sqrt{-3}, 0 \right), \left(-\beta\sqrt{-3}, 0 \right) \right\}, \quad (19)$$

then $L_{a,b,\bar{i},m}(X, Y) = 0$ 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 $\mathcal{C}_{A,B,\bar{i},m}$ be as in (3). By Lemma 12, the curve $L_{a,b,\bar{i},m}(X, Y) = 0$ is actually $\mathcal{C}_{A,B,\bar{i},m}$. Note that m divides $q^2 - 1$ and that each coefficient of $f_{A,B,\bar{i},m}(X, Y)$ lies in \mathbb{F}_{q^2} . Then, the curve $\mathcal{C}_{A,B,\bar{i},m}$ 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 1 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. [11, Lemma 4.5].

In order to show that if (19) holds, then P is collinear with two points in $K_{\bar{i}}$, we need to ensure the existence of a point (x, y) of the curve with equation $L_{a,b,\bar{i},m}(X, Y) = 0$ such that $Q_{\bar{i}x^m}$ and $Q_{\bar{i}y^m}$ are distinct points in $K_{\bar{i}}$. To this end, it is useful to consider a curve which is birationally equivalent to $L_{a,b,\bar{i},m}(X, Y) = 0$ but 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 14 *If (19) 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 the curve $L_{a,b,\bar{t},m}(X, Y) = 0$, 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 15 *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 $\mathbb{F}_q[Z]$:

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

Let

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

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

$$h(Z) = t\theta_1(Z) + \beta^2\theta_2(Z), \quad l(Z) = \theta_1(Z) + t\theta_2(Z) \quad (20)$$

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

$$\bar{t} \left(\frac{Z + \beta}{Z - \beta} \right)^m = \frac{\frac{h(Z)}{l(Z)} + \beta}{\frac{h(Z)}{l(Z)} - \beta}. \quad (21)$$

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 2 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 (21), $u = \frac{h(z)}{l(z)}$ holds, with $h(Z)$ and $l(Z)$ as in (20).

Remark 3 If (r, v) is an \mathbb{F}_q -rational affine point of the curve with equation $M_{a,b,\bar{t},m}(R, V) = 0$, such that

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

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 $K_{\bar{t}}$ by (18).

Proposition 16 Let $P = (a, b)$ be a point in $AG(2, q)$ off \mathcal{X} . Assume that (19) holds. If

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

then P is collinear with two distinct points of $K_{\bar{t}}$.

Proof Let $\mathbb{K}(\bar{r}, \bar{v})$ be the function field of the curve $M_{a,b,\bar{t},m}(R, V) = 0$, 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 14, we have that

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

satisfy $f_{A,B,\bar{r},m}(\bar{x}, \bar{y}) = 0$. Therefore, by Propositions 12 and 13 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, ensure 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 3, $P = (a, b)$ is collinear with $Q_{\bar{r}(\frac{\bar{r}+\beta}{\bar{r}-\beta})^m}$ and $Q_{\bar{v}(\frac{\bar{v}+\beta}{\bar{v}-\beta})^m}$, which are two distinct points in $K_{\bar{r}}$. \square

The following technical variant of Proposition 16 will also be needed.

Proposition 17 *Let $P = (a, b)$ be a point in $AG(2, q)$ off \mathcal{X} . Assume that (19) holds. If*

$$q + 1 - (6m^2 - 6m + 2)\sqrt{q} \geq 8m^2 + 8m + 1, \quad (22)$$

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

Proof One can argue as in the proof of Proposition 16. We need to ensure that neither $Q_{\bar{r}(\frac{\bar{r}+\beta}{\bar{r}-\beta})^m}$ or $Q_{\bar{v}(\frac{\bar{v}+\beta}{\bar{v}-\beta})^m}$ coincides with T . As $T = Q_{\bar{r}}$, 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 12, 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 that need to be ruled out. \square

If (19) is not satisfied, then P is not collinear with any two points of $K_{\bar{r}}$. Actually, a stronger statement holds.

Proposition 18 *Let $a, b \in \mathbb{F}_q$ be such that*

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

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

Proof The claim follows by standard arguments. For the details, see the preliminary version of the present paper ([3, Proposition 21]). \square

In order to investigate the bicovering properties of the arc $K_{\tilde{r}}$, according to Remarks 2 and 3, we need to consider the rational function $(a - \frac{h(\tilde{r})}{l(\tilde{r})})(a - \frac{h(\tilde{v})}{l(\tilde{v})})$ in the function field of $M_{a,b,\tilde{r},m}(R, V) = 0$.

Lemma 16 *Let $P = (a, b)$ be a point in $AG(2, q)$ off \mathcal{X} satisfying (19). Let $\mathbb{K}(\tilde{r}, \tilde{v})$ be the function field of the curve $M_{a,b,\tilde{r},m}(R, V) = 0$, so that $M_{a,b,\tilde{r},m}(\tilde{r}, \tilde{v}) = 0$. Then, the rational function $(a - \frac{h(\tilde{r})}{l(\tilde{r})})(a - \frac{h(\tilde{v})}{l(\tilde{v})})$ is not a square in $\mathbb{K}(\tilde{r}, \tilde{v})$.*

Proof Let \bar{x} and \bar{y} be as in the proof of Proposition 16, so that $\mathbb{K}(\tilde{r}, \tilde{v}) = \mathbb{K}(\bar{x}, \bar{y})$ with $f_{A,B,\tilde{r},m}(\bar{x}, \bar{y}) = 0$. By straightforward computation,

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

Then, the assertion follows from Proposition 15. \square

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

$$q + 1 - (16m^2 - 8m + 2)\sqrt{q} \geq 16m^2 + 24m + 1, \quad (23)$$

then P is bicovered by the points of $K_{\tilde{r}}$.

Proof Let $\mathbb{K}(\tilde{r}, \tilde{v})$ be the function field of the curve $M_{a,b,\tilde{r},m}(R, V) = 0$, so that $M_{a,b,\tilde{r},m}(\tilde{r}, \tilde{v}) = 0$. By Proposition 15 and Lemma 16, for every $c \in \mathbb{F}_q^*$ the equation

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

defines a Kummer extension $\mathbb{K}(\tilde{r}, \tilde{v}, \tilde{w})$ of $\mathbb{K}(\tilde{r}, \tilde{v})$ with genus less than or equal to $8m^2 - 4m + 1$. Let E be as in the proof of Proposition 16, and let E' be the set of places of $\mathbb{K}(\tilde{r}, \tilde{v}, \tilde{w})$ that either lie over a place in E or over a zero or a pole of $(a - \frac{h(\tilde{r})}{l(\tilde{r})})(a - \frac{h(\tilde{v})}{l(\tilde{v})})$. By Proposition 15, together with the proof of Proposition 16, an upper bound for the size of E' is $16m^2 + 24m$. Our assumption on q and m , together with the Hasse-Weil bound, ensure the existence of at least $16m^2 + 24m + 1$ \mathbb{F}_q -rational places of $\mathbb{K}(\tilde{r}, \tilde{v}, \tilde{w})$; hence, there exists at least one \mathbb{F}_q -rational place γ_c of $\mathbb{K}(\tilde{r}, \tilde{v}, \tilde{w})$ 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 $M_{a,b,\tilde{r},m}(R, V) = 0$. Therefore, by Remark 3, P is collinear with two distinct points

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

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 20 *Let $K_{\bar{\tau}}$ be a coset of K such that $K_{\bar{\tau}} \cup K_{\bar{\tau}'}$ 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 $K_{\bar{\tau}} \cup K_{\bar{\tau}'}$ but collinear with a point of $K_{\bar{\tau}}$ and a point of $K_{\bar{\tau}'}$.*

- (i) *If $u \neq 0$ and (23) holds, then P_u is bicovert by $K_{\bar{\tau}} \cup K_{\bar{\tau}'}$.*
- (ii) *The point $P_0 = (0, -\frac{1}{\beta^2})$ is not bicovert by $K_{\bar{\tau}} \cup K_{\bar{\tau}'}$. It is internal (resp. external) to every segment cut out on $K_{\bar{\tau}} \cup K_{\bar{\tau}'}$ 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 $K_{\bar{\tau}}$, then the point $Q = \Theta(P_u \oplus P)$ ranges over $K_{\bar{\tau}'}$ and is collinear with P_u and P . Recall that P belongs to $K_{\bar{\tau}}$ if and only if $P = (e, \frac{1}{e^2 - \beta^2})$ with

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

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

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

Note that $e(\bar{x})$ is defined over \mathbb{F}_q . In order to determine whether P_u is bicovert by $K_{\bar{\tau}} \cup K_{\bar{\tau}'}$, 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 $\bar{t} \left(\frac{\bar{x}+\beta}{\bar{x}-\beta} \right)^m - 1$ 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 3 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 $\tilde{x} = \bar{x}(\gamma_c)$, $\tilde{w} = \bar{w}(\gamma_c)$,

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

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

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

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

7 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 $K_{\tilde{t}}$ are as in Sect. 6. 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. [27, Example 1.2]. If m and $(q + 1)/m$ are coprime, such a construction applies to G .

Proposition 21 *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*

$$\mathcal{A} = K_{\tilde{t}} \setminus \{T\} \cup (H \oplus R) \setminus \{\oplus 2R' \oplus R\}$$

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 (19). By Remark 1, 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 $(0, -\frac{9}{8\beta^2})$.

7.1 Small complete arcs in $AG(2, q)$

Let \mathcal{A} be as in Proposition 21. We use Propositions 17, 18, and 21 in order to construct small complete arcs in Galois planes. Note that (22) is implied by $m \leq \frac{\sqrt[4]{q}}{\sqrt{6}}$.

Theorem 3 *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 $m + \frac{q+1}{m}$.*

7.2 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 $K_{\bar{i}}$. Then, the union S of the cosets of K corresponding to M is a good maximal 3-independent subset of G ; see [30, Lemma 1]. 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 18, 19, and 20, 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 4 *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 (23) 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*

$$\mathcal{B} = \left(\bigcup_{K_{\bar{i}} \in M} K_{\bar{i}} \right) \cup \mathcal{E} \quad (24)$$

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 (24) is an almost bicovering arc. Note that by Proposition 18, there is precisely one point in G collinear with any two points in \mathcal{E} .

Theorem 5 *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 (23) 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*

$$\mathcal{B} = \left(\bigcup_{K_{\bar{i}} \in M} K_{\bar{i}} \right) \cup \mathcal{E}$$

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 4 and 5, together with Proposition 1, 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 [27, 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 (23) is implied by $m \leq \frac{\sqrt[4]{q}}{4}$, the following result holds.

Theorem 6 *Let $q = p^h$ with $p > 3$ a prime, 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*

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

8 The case where m is a prime

By Corollary 1, Theorem 4, and Theorem 5, when q is large enough with respect to m , bicoxing arcs of size roughly sq/m can be constructed provided that a maximal-3-independent subset of size s in the cyclic group C_m of order m exists. In both Theorems 2 and 6, m is assumed to be a composite integer in order to apply the explicit construction of maximal 3-independent subsets provided by Szőnyi [27, Example 1.2]. As to the prime case, it was shown in [30] that if $m > 7$ is a prime, then there exists a maximal 3-independent subset of size $s \leq (m + 1)/3$ in C_m ; this gives rise to bicoxing arcs of size less than $q/3$ and complete caps of size less than $\frac{1}{3}q^{N/2}$. In [15], maximal sets M in C_m with the property that $x_1 + x_2 + x_3 \neq 0$ for pairwise distinct $x_1, x_2, x_3 \in M$ are constructed. The following result based on [15, Theorem 3.4] can be proved by straightforward computation.

Proposition 22 *Let $m > 3$ be a prime. For an odd divisor $m' \geq 7$ of $m + 5$, let $k = (m + 5)/m' > 4$. Then*

$$\{1, \dots, k - 2\} \cup \{lk - 2 \mid l = 2, \dots, m' - 2\} \cup \{lk - 3 \mid l = 2, \dots, \frac{m' - 1}{2}\}$$

is a maximal-3-independent subset of the cyclic group $\mathbb{Z}/(m)$.

Now let $m > 3$ be a prime divisor of $q^2 - 1$ such that $m \leq \frac{\sqrt[4]{q}}{4}$, and assume that $m + 5 = m_1 m_2$ for $m_1 \geq 7$ odd and $m_2 > 4$. Then, by Proposition 22, together with Corollary 1, Theorem 4, and Theorem 5, complete caps in $AG(N, q)$ with approximately

$$\left(\frac{m_2 + (3/2)m_1}{m_1 m_2} \right) q^{N/2}$$

points can be constructed. This shows that, apart from the constant $3/2$, Theorems 2 and 6 remain valid for m a prime, and m_1, m_2 suitable divisors of $m + 5$.

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

References

1. Anbar, N., Bartoli, D., Giulietti, M., Platoni, I.: Small complete caps from singular cubics. *J. Combin. Des.* (2013). doi:[10.1002/jcd.21366](https://doi.org/10.1002/jcd.21366).
2. Anbar, N., Bartoli, D., Giulietti, M., Platoni, I.: Small complete caps from nodal cubics. [Arxiv:1305.3019](https://arxiv.org/abs/1305.3019)
3. Anbar, N., Bartoli, D., Giulietti, M., Platoni, I.: Complete arcs and complete caps from cubics with an isolated double point. [Arxiv:1305.3420](https://arxiv.org/abs/1305.3420)
4. Anbar, N., Giulietti, M.: Bicovery arcs and small complete caps from elliptic curves. *J. Algebraic Combin.* **38**, 371–392 (2013)
5. Bartoli, D., Faina, G., Giulietti, M.: Small complete caps in three-dimensional Galois spaces. *Finite Fields Appl.* **24**, 184–191 (2013)
6. Bruen, A.A., Hirschfeld, J.W.P., Wehlau, D.L.: Cubic curves, finite geometry and cryptography. *Acta Appl. Math.* **115**(3), 265–278 (2011)
7. Davydov, A.A., Giulietti, M., Marcugini, S., Pambianco, F.: New inductive constructions of complete caps in $PG(N, q)$, q even. *J. Combin. Des.* **18**(3), 177–201 (2010)
8. Davydov, A.A., Östergård, P.R.J.: 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.
9. Faina, G., Pasticci, F., Schmidt, L.: Small complete caps in Galois spaces. *Ars Combin.* **105**, 299–303 (2012)
10. Fanali, S., Giulietti, M.: On the number of rational points of generalized fermat curves over finite fields. *Int. J. Number Theory* **8**(4), 1087–1097 (2012)
11. Giulietti, M.: On plane arcs contained in cubic curves. *Finite Fields Appl.* **8**, 69–90 (2002)
12. Giulietti, M.: Small complete caps in Galois affine spaces. *J. Algebraic Combin.* **25**(2), 149–168 (2007)
13. Giulietti, M.: Small complete caps in $PG(N, q)$, q even. *J. Combin. Des.* **15**(5), 420–436 (2007)
14. Giulietti, M., Pasticci, F.: Quasi-Perfect Linear Codes With Minimum Distance 4. *IEEE Trans. Inform. Theory* **53**(5), 1928–1935 (2007)
15. Hadnagy, É.: Small Complete Arcs in $PG(2, p)$. *Finite Fields Appl.* **5**, 1–12 (1999)
16. Hirschfeld, J.W.P.: *Projective Geometries Over Finite Fields*. Oxford Mathematical Monographs, 2nd edn. The Clarendon Press Oxford University Press, New York (1998)
17. Hirschfeld, J.W.P., Storme, L.: 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)
18. Hirschfeld, J.W.P., Storme, L.: The packing problem in statistics, coding theory, and finite projective spaces: update 2001, in: *Proceedings of the Fourth Isle of Thorns Conference Finite Geometries (Developments in Mathematics 3)*, Blokhuis, A., Hirschfeld, J.W.P., Jungnickel, D., Thas, J.A. (eds.) pp. 201–246. Kluwer Academic Publishers, Boston (2000)
19. Hirschfeld, J.W.P., Voloch, J.F.: The characterisation of elliptic curves over finite fields. *J. Austral. Math. Soc. Ser. A* **45**, 275–286 (1988)
20. Lombardo-Radice, L.: Sul problema dei k -archi completi in $S_{2,q}$. ($q = p^f$, p primo dispari.). *Boll. Un. Mat. Ital.* (3) **11**, 178–181 (1956)
21. Pambianco, F., Storme, L.: Small complete caps in spaces of even characteristic. *J. Combin. Theory Ser. A* **75**(1), 70–84 (1996)
22. Segre, B.: 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)
23. Segre, B.: Introduction to Galois geometries. *Atti Accad. Naz. Lincei Mem. Cl. Sci. Fis. Mat. Natur. Sez. I* (8) **8**, 133–236 (1967)
24. Segre, B., Bartocci, U.: Ovali ed altre curve nei piani di Galois di caratteristica due. *Acta Arith.* **18**, 423–449 (1971)
25. Stichtenoth, H.: *Algebraic Function Fields and Codes*, Volume 254 of Graduate Texts in Mathematics, 2nd edn. Springer, Berlin (2009)
26. Szőnyi, T.: Small complete arcs in Galois planes. *Geom. Dedicata.* **18**(2), 161–172 (1985)
27. Szőnyi, T.: Arcs in cubic curves and 3-independent subsets of abelian groups. In: *Combinatorics (Eger, 1987)*, Colloq. Math. Soc. János Bolyai, vol 52, pp. 499–508. North-Holland, Amsterdam (1988)
28. Szőnyi, T.: Complete arcs in Galois planes: a survey. In: *Quaderni del Seminario di Geometrie Combinatorie 94*, Dipartimento di Matematica “G. Castelnuovo”, Università degli Studi di Roma “La Sapienza”, Roma (1989)

29. Voloch, J.F.: On the completeness of certain plane arcs. *European J. Combin.* **8**, 453–456 (1987)
30. Voloch, J.F.: On the completeness of certain plane arcs. II. *European J. Combin.* **11**(5), 491–496 (1990)
31. Zirilli, F.: Su una classe di k -archi di un piano di Galois. *Atti Accad. Naz. Lincei Rend.* **54**, 393–397 (1973)