SMALL COMPLETE CAPS FROM NODAL CUBICS

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

Abstract. Bicovering arcs in Galois affine planes of odd order are a powerful tool for constructing complete caps in spaces of higher dimensions. In this paper we investigate whether some arcs contained in nodal cubic curves are bicovering. For m_1, m_2 coprime divisors of $q-1$, bicovering arcs in $AG(2,q)$ of size $k \leq (q-1)\frac{m_1+m_2}{m_1m_2}$ are obtained, provided that $(m_1m_2, 6) = 1$ and $m_1m_2 < \sqrt[4]{q}/3.5$. Such arcs produce complete caps of size $kq^{(N-2)/2}$ in affine spaces of dimension $N \equiv 0 \pmod 4$. For infinitely many q's these caps are the smallest known complete caps in $AG(N,q)$, $N \equiv 0 \pmod 4$. Galois affine spaces and Bicovering arcs and Complete caps and Quasi-perfect codes and Cubic curves

1. Introduction

In a (projective or affine) space over the finite field with q elements $\mathbb{F}_q$, a *cap* is a set of points no three of which collinear; plane caps are usually called *arcs*. A cap is said to be *complete* if it is not contained in a larger cap. The problem of determining the spectrum of sizes of complete caps in a given space has been intensively investigated, also in connection with Coding Theory. In fact, complete caps of size k in the N-dimensional projective space $PG(N,q)$ with $k > N+1$ and linear quasi-perfect $[k, k-N-1, 4]$-codes over $\mathbb{F}_q$ are equivalent objects; see e.g. [8]. For fixed N and q, the smaller is a complete cap, the better are the covering properties of the corresponding code; see e.g. [12].

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

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

If q is even and N is odd, such bound is substantially sharp; see [18]. Otherwise, all known infinite families of complete caps have size far from (1); see the survey papers [14, 15] and the more recent works [1, 2, 3, 5, 10, 11, 12].

For q odd, a lifting method for constructing complete caps in higher dimensions was proposed in [10]. It is based on the notion of a bicovering arc in a Galois affine plane $AG(2,q)$; see Section 2.1 here. An arc A in $AG(2,q)$ is said to be bicovering

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

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

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

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

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

if 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. As first noticed in [10], if there exists a bicovering arc of size k in $AG(2,q)$, then a complete cap of size $kq^{(N-2)/2}$ can be constructed in $AG(N,q)$ for each positive $N \equiv 0 \pmod 4$.

Cubic curves have recently emerged as a useful tool to construct small bicovering arcs [1, 2, 6]. Let G denote the abelian group of the non-singular $\mathbb{F}_q$-rational points of an irreducible plane cubic $\mathcal{X}$ defined over $\mathbb{F}_q$. It was already noted by Zirilli [28] that no three points in a coset of a subgroup K of G can be collinear, provided that the index m of K in G is not divisible by 3. Since then, arcs in cubics have been thoroughly investigated; see e.g. [9, 17, 23, 24, 25, 26, 27]. It is easily seen that a necessary condition for the union of some cosets of K to be a bicovering arc is that they form a maximal 3-independent subset of the factor group G/K. The possibility of obtaining small bicovering arcs via this method was investigated in [1] for $\mathcal{X}$ singular with a cusp, and in [2] when $\mathcal{X}$ is a non-singular (elliptic) curve. As a result, general constructions of bicovering arcs of size less than $2pq^{7/8}$ [1] and $q/3$ [2] were provided.

In this paper we deal with cubics with an $\mathbb{F}_q$-rational node. We prove that if m is a divisor of $q-1$ coprime to 6 and such that $m \le \sqrt[4]{q}/3.5$, then the union of the cosets of K corresponding to a maximal 3-independent subset in G/K is a bicovering arc; see Theorem 2 in Section 4. A similar result for $\mathcal{X}$ elliptic was obtained in [2], under the further assumption that m is a prime; see [2, Theorem 1]. However, it should be remarked that allowing m to be a composite integer is a crucial improvement. In fact, for m a generic prime, the smallest known maximal 3-independent subsets in the cyclic group of order m have size approximately $m/3$ [27]; on the other hand, when $m = m_1m_2$ with $(m_1, m_2) = 1$ and $(m, 6) = 1$, maximal 3-independent subsets of size less than or equal to $m_1 + m_2$ can be easily constructed; see [24].

The main achievements of the present paper are summarized by the following result.

Theorem 1. *Let $q = p^h$ with $p > 3$, and let m be a proper divisor of $q-1$ such that $(m, 6) = 1$ and $m \le \frac{\sqrt[4]{q}}{3.5}$. Assume that $m = m_1m_2$ with $(m_1, m_2) = 1$. Then*

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

$$\frac{(m_1 + m_2)(q-1)}{m_1m_2};$$

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

$$\frac{(m_1 + m_2)(q-1)}{m_1m_2} q^{\frac{N-2}{2}}.$$

When p is large, the value $(m_1+m_2)/m_1m_2$, where m_1, m_2 are coprime divisors of $q-1$ with $(m_1m_2, 6) = 1$ and $m_1m_2 < \sqrt[4]{q}/3.5$, can be significantly smaller than both $2p/q^{1/8}$ and $1/3$. This certainly happens for infinite values of q; see Section 5.1. In this cases, Theorem 1 provides the smallest bicovering arcs known up to now, and hence the smallest known complete caps in $AG(N.q)$ with $N \equiv 0 \pmod 4$.

Our proofs heavily rely on concepts and results from both Algebraic Geometry in positive characteristic and Function Field Theory. In particular, a crucial role is played by the family of plane curves investigated in Section 3.

With regard to the problem of constructing bicovering arcs contained in singular cubics, it should be noted that the present paper together with [1] leave just one case open, namely that of a cubic with an isolated double point, which is currently under investigation by the same authors.

2. Preliminaries

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

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

For an arc A in $AG(2,q)$, let

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

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

$$(x - x_1)(x - x_2) \quad \text{is a non-zero square or a non-square in } \mathbb{F}_q, \tag{2}$$

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. 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_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.

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

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.** Let $\mathcal{C}$ be a projective absolutely irreducible algebraic curve, defined over the algebraic closure $\mathbb{K}$ of $\mathbb{F}_q$. An *algebraic function field F over* $\mathbb{K}$ is an extension F of $\mathbb{K}$ such that F is a finite algebraic extension of $\mathbb{K}(x)$, for some element $x \in F$ transcendental over $\mathbb{K}$. If $F = \mathbb{K}(x)$, then F is called the *rational function field over* $\mathbb{K}$. For basic definitions on function fields we refer to [22].

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

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

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

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

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

Proposition 2 (Proposition 3.7.3 in [22])**.** *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*

$$F' = F(y) \text{ with } y^m = u. \tag{3}$$

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*

$$r_\gamma := (m, v_\gamma(u)) > 0 \tag{4}$$

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 (4).

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 $\mathcal{C}$).

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

Proposition 4 (Hasse-Weil Bound - Theorem 5.2.3 in [22])**.** *The number N_q of $\mathbb{F}_q$-rational places of the function field $\mathbb{K}(\mathcal{C})$ of a curve $\mathcal{C}$ defined over $\mathbb{F}_q$ with genus g satisfies*

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

2.3. **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 $\mathbb{K}$, 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 following subset of $\mathrm{Div}(\mathbb{K}(\mathcal{C}))$:

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

where

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

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 [16]. 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

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

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 $\mathcal{C}$.

Proposition 5. *Let Q be a point of $\mathcal{C}$ and ℓ be a line in $\mathbb{P}^2(\mathbb{K})$. Then the sum*

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

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. A family of curves defined over $\mathbb{F}_q$

Throughtout this section $q=p^h$ for some prime $p>3$, and m is 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 index m in the abelian group of the non-singular $\mathbb{F}_q$-rational points of a nodal cubic is played by the curve

$$\mathcal{C}_P: f_{a,b,t,m}(X,Y)=0, \tag{5}$$

where

$$\begin{aligned} f_{a,b,t,m}(X,Y) &= a(t^3X^{2m}Y^m + t^3X^mY^{2m} - 3t^2X^mY^m + 1) \\ &\quad -bt^2X^mY^m - t^4X^{2m}Y^{2m} + 3t^2X^mY^m - tX^m - tY^m. \end{aligned} \tag{6}$$

In [24, 25] 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 ([19]; see also [21, 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,

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

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 $a^2 + t^2X^mY^m - atX^m = 0$ is a generalized Fermat curve over $\mathbb{F}_q$ (see [7]). As proven in [7], such component is absolutely irreducible with genus less than m^2.

Proposition 6. *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 $a^2 + t^2X^mY^m - atX^m = 0$.*

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*

$$\begin{aligned} g_P(X,Y) &= a(t^3X^2Y + t^3XY^2 - 3t^2XY + 1) - bt^2XY \\ &\quad -t^4X^2Y^2 + 3t^2XY - tX - tY \end{aligned}$$

is absolutely irreducible.

Proof. Let X_∞ and Y_∞ be the ideal points of the X-axis and the Y-axis, respectively. It is straightforward to check that X_∞ and Y_∞ are the only ideal points of $\mathcal{Q}_P$, and that they are both ordinary double points. The tangent lines of $\mathcal{Q}_P$ at X_∞ are $Y = 0$ and $Y = a/t$; similarly, $X = 0$ and $X = a/t$ are the tangent lines at Y_∞. As $ab \neq (a-1)^3$, it is straightforward to check that none of such lines is a component of $\mathcal{Q}_P$; hence, $\mathcal{Q}_P$ has no linear component. Assume now that $\mathcal{Q}_P$ splits into two irreducible conics, say $\mathcal{C}_1$ and $\mathcal{C}_2$.

Without loss of generality we can assume that $X = 0$ and $X = a/t$ are the tangents of $\mathcal{C}_1$ and $\mathcal{C}_2$ at Y_∞, respectively.

We first consider the case where $Y = 0$ is the tangent of $\mathcal{C}_1$ at X_∞ and $Y = a/t$ is the tangent of $\mathcal{C}_2$ at X_∞. Then $\mathcal{C}_1 : XY + \epsilon = 0$ and $\mathcal{C}_2 : (X - a/t)(Y - a/t) + \bar{\epsilon} = 0$ for some $\epsilon, \bar{\epsilon} \in \mathbb{K}^*$. So for some $\rho \in \mathbb{K}^*$

$$\rho g_P(X,Y) = (XY + \epsilon)((X - a/t)(Y - a/t) + \bar{\epsilon}).$$

By comparing coefficients we obtain

$$\begin{cases} -\rho t^4 = 1 \\ -\rho t = -\epsilon \frac{a}{t} \\ \rho a = \epsilon \frac{a^2}{t^2} + \epsilon\bar{\epsilon} \end{cases} \Rightarrow \begin{cases} \frac{1}{t^3} = -\epsilon \frac{a}{t} \\ -\frac{a}{t^4} = \epsilon \frac{a^2}{t^2} + \epsilon\bar{\epsilon} \end{cases} \Rightarrow \epsilon\bar{\epsilon} = 0,$$

which is impossible.

We now assume that $Y = a/t$ is the tangent of $\mathcal{C}_1$ at X_∞ and $Y = 0$ is the tangent of $\mathcal{C}_2$ at X_∞. Then for some $\epsilon, \bar{\epsilon}, \rho \in \mathbb{K}^*$

$$\rho g_P(X,Y) = \left(X\left(Y - \frac{a}{t}\right) + \epsilon\right)\left(\left(X - \frac{a}{t}\right)Y + \bar{\epsilon}\right).$$

By comparing coefficients we have

$$\begin{cases} -\rho t^4 = 1 \\ \rho a t^3 = -\frac{a}{t} \\ \rho\left(3t^2 - 3at^2 - bt^2\right) = \frac{a^2}{t^2} + \epsilon + \bar{\epsilon} \\ -\rho t = -\epsilon\frac{a}{t} \\ -\rho t = -\bar{\epsilon}\frac{a}{t} \\ \rho a = \epsilon\bar{\epsilon} \end{cases} \Rightarrow \begin{cases} \rho = -\frac{1}{t^4} \\ 3a + b - 3 = a^2 + \bar{\epsilon}t^2 + \epsilon t^2 \\ \frac{1}{t^3} = -\epsilon\frac{a}{t} \\ \frac{1}{t^3} = -\bar{\epsilon}\frac{a}{t} \\ -\frac{a}{t^4} = \epsilon\bar{\epsilon} \end{cases}$$

$$\Rightarrow \begin{cases} \epsilon t^2 = \bar{\epsilon}t^2 = -1/a \\ -\frac{a}{t^4} = \frac{1}{a^2t^4} \\ 3a + b - 3 = a^2 - \frac{1}{a} - \frac{1}{a} \end{cases} \Rightarrow \begin{cases} a^3 = -1 \\ ab = (a-1)^3 - 1 \end{cases},$$

which implies that both $a^3 = -1$ and $b = 1 - (a-1)^3$ hold, a contradiction.

□

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

$$a(t^3\bar{u}^2\bar{z} + t^3\bar{u}\bar{z}^2 - 3t^2\bar{u}\bar{z} + 1) - bt^2\bar{u}\bar{z} - t^4\bar{u}^2\bar{z}^2 + 3t^2\bar{u}\bar{z} - t\bar{u} - t\bar{z} = 0. \tag{7}$$

By the proof of Lemma 1 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*

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

and

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

Proof. We keep the notation of Section 2.3. Here, the role of $\bar{x}$ and $\bar{y}$ is played by $\bar{u}$ and $\bar{z}$, respectively. Then

$$v_{\gamma_1}(\bar{z} - a/t) + e_{\gamma_1} = j_2(\gamma_1), \tag{8}$$

$$v_{\gamma_1}(\bar{u}) + e_{\gamma_1} = 0, \tag{9}$$

$$v_{\gamma_1}(\bar{z}) + e_{\gamma_1} = 1. \tag{10}$$

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, (10) 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, (8) and (10) yield that $j_2(\gamma_1) = 1$, a contradiction. From (10) it follows that $e_{\gamma_1} = 1$; then $v_{\gamma_1}(\bar{u}) = -1$ is obtained from (9).

As far as γ_2 is concerned, note that

$$v_{\gamma_2}(\bar{z} - a/t) + e_{\gamma_2} = 1, \tag{11}$$

$$v_{\gamma_2}(\bar{u}) + e_{\gamma_2} = 0, \tag{12}$$

$$v_{\gamma_2}(\bar{z}) + e_{\gamma_2} = j_2(\gamma_2). \tag{13}$$

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

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*

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

and

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

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*

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

and

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

Proof. Clearly, γ_5 is a zero of $\bar{u}$, whereas γ_6 is a zero of $\bar{z}$. From (7), the number of zeros (and poles) of either $\bar{u}$ or $\bar{z}$ is 2. Then the assertion follows from Lemmas 2 and 3. □

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 $\mathbb{K}(\bar{u},\bar{y}) : K(\bar{u},\bar{z})$ 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 $\bar{\gamma}_1^1,\ldots,\bar{\gamma}_1^m$ be the places of $\mathbb{K}(\bar{u},\bar{y})$ lying over γ_1 and let $\bar{\gamma}_5^1,\ldots,\bar{\gamma}_5^m$ 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 $\mathbb{K}(\bar{u},\bar{y})$,*

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

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

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

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 7. *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 $i_0\in\{1,\ldots,s\}$ 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

$$\begin{tikzcd}
 & & \mathbb{K}(\bar{x},\bar{y}) \arrow[ddll, dash] \arrow[ddd, dash] \arrow[drr, dash, "m"] & & \\
 & & & & \mathbb{K}(\bar{u},\bar{z},\bar{y})=\mathbb{K}(\bar{u},\bar{y}) \arrow[ddll, dash, "m"] \arrow[d, dash] \\
\mathbb{K}(\bar{x}) \arrow[dd, dash, "m"'] & & & & \mathbb{K}(\bar{y}) \arrow[dd, dash, "m"] \\
 & & \mathbb{K}(\bar{u},\bar{z}) \arrow[dll, dash, "2"'] \arrow[drr, dash, "2"] & & \\
\mathbb{K}(\bar{u}) & & & & \mathbb{K}(\bar{z})
\end{tikzcd}$$

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. □

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. It is easily seen that $\mathcal{Q}_P$ does not admit any linear component. Note that both X_∞ and Y_∞ are cuspidal double points of $\mathcal{Q}_P$. The tangent line at X_∞ is $Y=0$, and the intersection multiplicity of $\mathcal{Q}_P$ and $Y=0$ at X_∞ is equal to 3; similarly, $X=0$ is the tangent line at Y_∞ and $\mathrm{I}(Y_\infty,\mathcal{Q}_P\cap\{X=0\})=3$. Therefore, precisely one irreducible component $\mathcal{C}$ of $\mathcal{Q}_P$ passes through Y_∞; also, Y_∞ is a double point of $\mathcal{C}$ and there is only one place of $\mathbb{K}(\mathcal{C})$ centered at Y_∞. Then $\mathcal{C}$ is a curve of degree greater than 2. Since $\mathcal{Q}_P$ does not have any linear component, the only possibility is that the degree of $\mathcal{C}$ is four, that is, $\mathcal{C}=\mathcal{Q}_P$. This shows that $\mathcal{Q}_P$ is absolutely irreducible. As $\mathcal{Q}_P$ is a quartic with at least two singular points, its genus g is less than or equal to 1. □

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

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

In order to prove that $\mathcal{C}_P$ is absolutely irreducible, the same arguments as in Section 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

$$g' = m(g-1) + \frac{3m-1}{2}, \tag{14}$$

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

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

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

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

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

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

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

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

by (14) this can only happen when both $e = 3$ and $g' = (m-1)/2$ hold. But this is impossible as $(m, 6) = 1$ is assumed. □

Arguing as in the proofs of Lemma 6 and Proposition 7, the following result is obtained.

Proposition 8. *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

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

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 Section 4.

Proposition 9. *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 Section 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 [7], the genus of $\mathcal{C}$ is $(m^2 - 3m + 2)/2$; also there are m places, say $\gamma_1^1, \ldots, \gamma_1^m$ of $\mathbb{K}(\bar{x}, \bar{y})$ centered at X_∞, and m places, say $\gamma_2^1, \ldots, \gamma_2^m$ of $\mathbb{K}(\bar{x}, \bar{y})$ centered at Y_∞. Let $\gamma_3^1, \ldots, \gamma_3^m$ denote the places centered at the m simple affine points of $\mathcal{C}$ with coordinates $(v, 0)$ with $v^m = a/t$. We have

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

Then it is easy to see that

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

whence

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

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

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

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 Section 3.2. By Lemma 5, the only places of $\mathbb{K}(\bar{u},\bar{y})$ which ramify in the extension $\mathbb{K}(\bar{x},\bar{y}) : K(\bar{u},\bar{y})$ are $\bar{\gamma}_1^1,\ldots,\bar{\gamma}_1^m$ and $\bar{\gamma}_5^1,\ldots,\bar{\gamma}_5^m$; their common ramification index is m. Therefore, for each $j = 1,\ldots,6$, 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 $j = 1,\ldots,6$, let $\bar{\bar{\gamma}}_j^1,\ldots,\bar{\bar{\gamma}}_j^m$ denote the places of $\mathbb{K}(\bar{x},\bar{y})$ lying over the place γ_j of $\mathbb{K}(\bar{u},\bar{z})$.

From Equations (8)–(13), together with Lemma 4, we deduce that in $\mathbb{K}(\bar{u},\bar{z})$

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

holds; similarly,

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

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

$$\mathrm{div}\big((a - t\bar{x}^m)(a - t\bar{y}^m)\big) = m\Big(\sum_{i=1}^{m}(\bar{\bar{\gamma}}_5^i + \bar{\bar{\gamma}}_6^i - \bar{\bar{\gamma}}_4^i - \bar{\bar{\gamma}}_2^i)\Big) \tag{15}$$

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 Section 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 $3m^2 - 2m + 1$.

□

4. Bicovering arcs from nodal cubics

If $\mathcal{X}$ is a singular plane cubic defined over $\mathbb{F}_q$ with a node and at least one $\mathbb{F}_q$-rational inflection, then a canonical equation for $\mathcal{X}$ is $XY = (X-1)^3$. If the neutral element of $(G,\oplus)$ 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 write K_t in an algebraically parametrized form:

$$K_t = \Big\{\big(tw^m, \frac{(tw^m - 1)^3}{tw^m}\big) \mid w \in \mathbb{F}_q^*\Big\}. \tag{16}$$

For a point $P = (a,b)$ in $AG(2,q) \setminus \mathcal{X}$, let $f_{a,b,t,m}(X,Y)$ be as in (6).

Proposition 10. *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. Two distinct points $P_1 = \Big(v_1, \frac{(v_1-1)^3}{v_1}\Big)$, $P_2 = \Big(v_2, \frac{(v_2-1)^3}{v_2}\Big)$ in $\mathcal{X}$ are collinear with P if and only if

$$\begin{vmatrix} v_1 & \frac{(v_1-1)^3}{v_1} & 1 \\ v_2 & \frac{(v_2-1)^3}{v_2} & 1 \\ a & b & 1 \end{vmatrix} = 0.$$

As $P_1 \neq P_2$, this is equivalent to

$$a(v_1^2v_2 + v_1v_2^2 - 3v_1v_2 + 1) - bv_1v_2 - v_1v_2(v_1v_2 - 3) - (v_1 + v_2) = 0.$$

When P_1, P_2 are elements of K_t, both $v_1 = t\tilde{x}^m$ and $v_2 = t\tilde{y}^m$ hold for some $\tilde{x}, \tilde{y} \in \mathbb{F}_q^*$, whence the assertion. □

Proposition 11. *If*

$$q + 1 - (12m^2 - 8m + 2)\sqrt{q} \geq 8m^2 + 8m + 1 \tag{17}$$

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 proof 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 9. 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 4.4 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 9, Case 2, that the only places of $\mathbb{K}(\bar{u}, \bar{z})$ that ramifies in $\mathbb{K}(\bar{x}, \bar{y})$ are the places γ_j for $j = 1, \ldots, 6$, and their common ramification index is m. Also, by (15), 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 $\mathbb{K}(\bar{x}, \bar{y}, \bar{w})$

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

Also, by (15),

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

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 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 $j = 1 \ldots, 6$, whence $|E| \leq 8m^2 + 8m$.

Our assumption on q and m, together with Proposition 4, ensures 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 10, P is collinear with two distinct points

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

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. □

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 12. *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* (17) *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

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

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

$$Q=\Big(\frac{1}{u_0tx^m},\frac{(1-u_0tx^m)^3}{(u_0tx^m)^2}\Big).$$

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

$$\eta(\bar{x})=(u_0-t\bar{x}^m)\Big(u_0-\frac{1}{u_0tx^m}\Big)=\frac{(u_0-t\bar{x}^m)(u_0^2t\bar{x}^m-1)}{u_0t\bar{x}^m}.$$

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 $(u_0-t\bar{x}^m)$, $(u_0^2t\bar{x}^m-1)$, and $u_0t\bar{x}^m$; hence, $v_{\gamma_\infty}(\eta(\bar{x}))=-m-m-(-m)=-m$. Also, γ_0 is a zero of $u_0t\bar{x}^m$ 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 nor 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

$$P(c)=\left(t\tilde{x}^m,\frac{(\tilde{x}^m-1)^3)}{t\tilde{x}^m}\right)\in K_t,\qquad Q(c)=\left(\frac{1}{u_0t\tilde{x}^m},\frac{(1-u_0t\tilde{x}^m)^3}{(u_0t\tilde{x}^m)^2}\right)\in K_{t'}.$$

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 $P(c)Q(c)$. □

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 [27]. 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 [27], Lemma 1, together with Remark 5(5). 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 11 and 12, if K is large enough with respect to q then S is a bicovering arc as well, and the following result holds.

Theorem 2. *Let m be a proper divisor of $q-1$ such that $(m, 6) = 1$ and (17) 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. Conclusions

We use Theorem 2, together with the results in Section 2.1 in order to construct small complete caps in affine spaces $AG(N, q)$. Note that (17) 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 [24]. Then Theorem 1 follows at once from Corollary 1.

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 [2], providing complete caps of size approximately $q^{N/2}/3$. It is often possible to choose m_1, m_2 as in Theorem 1 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 $m=(p^2-1)/(2^s3^k)$, 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 $m=m_1m_2$ 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 1 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 $p+1$ 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 1 provides an improvement on such bound whenever it is possible to choose m_1, m_2 so that

$$(m_1+m_2)/m_1m_2 < 2/p^{\lfloor(\lceil h/4\rceil-1)/2\rfloor}. \tag{18}$$

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 arguing as in Case (i) it is easy to see that one can choose m_1, m_2 so that

$$\frac{m_1+m_2}{m_1m_2} \sim (2^{s_2}+2^{s_1}3^k)q^{-\frac{1}{8}},$$

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 q's for which (18) happens is $q=p^{12}$, with $p\equiv 1 \pmod{12}$ and $(p^2+1)/2$ a composite integer. Assume that $(p^2+1)/2=v_1v_2$ with $v_1,v_2>1$ and $v_1<v_2$. Then choosing $m_1=v_1(p+1)/2$ and $m_2=v_2$ gives $(m_1+m_2)/m_1m_2 < 2/p$.

References

[1] Nurdagül Anbar, Daniele Bartoli, Massimo Giulietti, and Irene Platoni. Small complete caps from singular cubics. Submitted, 2013.

[2] Nurdagül Anbar and Massimo Giulietti. Bicovering arcs and small complete caps from elliptic curves. *J. Algebraic Combin.*. In press. Published online October 2012. DOI: 10.1007/s10801-012-0407-8.

[3] Daniele Bartoli, Giorgio Faina, and Massimo Giulietti. Small complete caps in three-dimensional Galois spaces. Submitted, 2013.

[4] Aiden A. Bruen, James W. P. Hirschfeld, and David L. Wehlau. Cubic curves, finite geometry and cryptography. *Acta Appl. Math.*, 115(3):265–278, 2011.

[5] Alexander A. Davydov, Massimo Giulietti, Stefano Marcugini, and Fernanda Pambianco. New inductive constructions of complete caps in PG(N,q), q even. *J. Combin. Des.*, 18(3):177–201, 2010.

[6] Giorgio Faina, Fabio Pasticci, and Lorenzo Schmidt. Small complete caps in Galois spaces. *Ars Combin.*, 105:299–303, 2012.

[7] Stefania Fanali and Massimo Giulietti. On the number of rational points of generalized fermat curves over finite fields. *Int. J. Number Theory*, 8(4):1087–1097, 2012.

[8] Ernst M. Gabidulin, Alexander A. Davydov, and Leonid M. Tombak. Linear codes with covering radius 2 and other new covering codes. *IEEE Trans. Inform. Theory*, 37(1):219–224, 1991.

[9] Massimo Giulietti. On plane arcs contained in cubic curves. *Finite Fields Appl.*, 8:69–90, 2002.

[10] Massimo Giulietti. Small complete caps in Galois affine spaces. *J. Algebraic Combin.*, 25(2):149–168, 2007.

[11] Massimo Giulietti. Small complete caps in PG(N, q), q even. *J. Combin. Des.*, 15(5):420–436, 2007.

[12] Massimo Giulietti and Fabio Pasticci. Quasi-Perfect Linear Codes With Minimum Distance 4. *IEEE Trans. Inform. Theory*, 53(5): 1928-1935, 2007.

[13] James W. P. Hirschfeld. *Projective geometries over finite fields.* Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, second edition, 1998.

[14] James W. P. Hirschfeld and Leo Storme. The packing problem in statistics, coding theory and finite projective spaces. *J. Statist. Plann. Inference*, 72(1-2):355–380, 1998. R. C. Bose Memorial Conference (Fort Collins, CO, 1995).

[15] James W. P. Hirschfeld and Leo Storme, *The packing problem in statistics, coding theory, and finite projective spaces*: update 2001, in: Finite Geometries, Proceedings of the Fourth Isle of Thorns Conference, A. Blokhuis, J. W. P. Hirschfeld, D. Jungnickel and J. A. Thas, Eds., Developments in Mathematics 3, Kluwer Academic Publishers, Boston, (2000), 201-246.

[16] James W. P. Hirschfeld, Gábor Korchmáros, and Fernando Torres. *Algebraic curves over a finite field.* Princeton University Press, Princeton and Oxford, 2008.

[17] James W. P. Hirschfeld and José Felipe Voloch. The characterisation of elliptic curves over finite fields. *J. Austral. Math. Soc. Ser. A*, 45: 275–286, 1988.

[18] Fernanda Pambianco and Leo Storme. Small complete caps in spaces of even characteristic. *J. Combin. Theory Ser. A*, 75(1):70–84, 1996.

[19] Beniamino Segre. Ovali e curve σ nei piani di Galois di caratteristica due. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. (8)*, 32:785–790, 1962.

[20] Beniamino Segre. Proprietà elementari relative ai segmenti ed alle coniche sopra un campo qualsiasi ed una congettura di Seppo Ilkka per il caso dei campi di Galois. *Ann. Mat. Pura Appl. (4)*, 96:289–337, 1972.

[21] Beniamino Segre and Umberto Bartocci. Ovali ed altre curve nei piani di Galois di caratteristica due. *Acta Arith.*, 18:423–449, 1971.

[22] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[23] Tamás Szőnyi. Small complete arcs in Galois planes. *Geom. Dedicata*, 18(2):161–172, 1985.

[24] Tamás Szőnyi. Arcs in cubic curves and 3-independent subsets of abelian groups. In *Combinatorics (Eger, 1987)*, volume 52 of *Colloq. Math. Soc. János Bolyai*, pages 499–508. North-Holland, Amsterdam, 1988.

[25] Tamás Szőnyi. Complete arcs in Galois planes: a survey. Quaderni del Seminario di Geometrie Combinatorie 94, Dipartimento di Matematica "G. Castelnuovo", Università degli Studi di Roma "La Sapienza", Roma, January 1989.

[26] José Felipe Voloch. On the completeness of certain plane arcs, *European J. Combin.*, 8:453-456, 1987.

[27] José Felipe Voloch. On the completeness of certain plane arcs. II. *European J. Combin.*, 11(5):491–496, 1990.

[28] Francesco Zirilli. Su una classe di k-archi di un piano di Galois, *Atti Accad. Naz. Lincei Rend.* 54:393-397, 1973.

E-mail address: nurdagul@su.sabanciuniv.edu
E-mail address: bartoli@dmi.unipg.it
E-mail address: irene.platoni@unitn.it
E-mail address: giuliet@dmi.unipg.it