University of Trento

Department of Mathematics

Ph.D. in Mathematics
XVII Cycle

Complete Arcs and Caps in Galois Spaces

Irene Platoni

Supervisor: Prof. Massimo Giulietti

Head of PhD School: Prof. Francesco Serra Cassano

Academic Year 2014/2015

University of Trento

Department of Mathematics

Ph.D. in Mathematics
XVII Cycle

Complete Arcs and Caps in Galois Spaces

Ph.D.Thesis of: Irene Platoni

Supervisor: Prof. Massimo Giulietti

Head of PhD School: Prof. Francesco Serra Cassano

Academic Year 2014/2015

Contents

Preface

Galois spaces, that is affine and projective spaces of dimension $N \geq 2$ defined over a finite (Galois) field $\mathbb{F}_q$, are well known to be rich of nice geometric, combinatorial and group theoretic properties that have also found wide and relevant applications in several branches of Combinatorics, as well as in more practical areas, notably Coding Theory and Cryptography.

The systematic study of Galois spaces was initiated in the late 1950's by the pioneering work of B. Segre [**59**]. The trilogy [**34, 36, 42**] covers the general theory of Galois spaces including the study of objects which are linked to linear codes. Typical such objects are plane arcs and their generalizations - especially caps and arcs in higher dimensions - whose code theoretic counterparts are distinguished types of error-correcting and covering linear codes. Their investigation has received a great stimulus from Coding Theory, especially in the last decades; see the survey papers [**40, 41**].

An important issue in this context is *to ask for explicit constructions of small complete arcs and small complete caps.* A *cap* in a Galois space is a set of points no three of which are collinear. A cap is *complete* if its secants (lines through two points of the set) cover the whole space. An *arc* in a Galois space of dimension N is a set of points no $N+1$ of which lying on the same hyperplane. In analogy with caps, an arc which is maximal with respect to set-theoretical inclusion is said to be complete. Also, arcs coincide with caps in Galois planes. From these geometrical objects, there arise linear codes which turn out to have very good covering properties, provided that the size of the set is small with respect to the dimension N and the order q of the ambient space.

For the size $t(AG(N,q))$ of the smallest complete caps in a Galois affine space $AG(N,q)$ of dimension N over $\mathbb{F}_q$, the trivial lower bound is

$$\sqrt{2}q^{\frac{N-1}{2}}. \tag{0.1}$$

General constructions of complete caps whose size is close to this lower bound are only known for q even and N odd, see [**16, 19, 29, 52**]. When N is even, complete caps of size of the same order of magnitude as $cq^{N/2}$, with c a constant independent of q, are known to exist for both the odd and the even order case, see [**16, 18, 28, 29, 31**] (see also Section 2.2 and the references therein).

Whereas, few constructions of small complete arcs in Galois spaces of dimension $N > 2$ are known. In [**65, 66, 67**], small complete arcs having many points in common with the normal rational curve are investigated (see Section 4.2.3 for comparisons with our results).

In this thesis, new infinite families of complete arcs and caps in higher dimensional spaces are constructed from algebraic curves defined over a finite field. In most cases, no smallest complete caps/arcs were previously known in the literature. Although caps and arcs are rather combinatorial objects, constructions and proofs sometimes heavily rely on concepts and results from Algebraic Geometry in positive characteristic.

The thesis is organized as follows.

In Chapter 1 some preliminary notions and some of the material on algebraic curves and function fields, which is relevant to the proofs of the original results of the thesis, is summarized.

Chapter 2 surveys the state of the art of the research on small complete caps and arcs, with particular emphasis on recent developments. The first section is devoted to the general theory of caps in Galois spaces of dimension 2 and 3. In the plane case, the theory is well developed and quite rich of constructions. Also, small complete caps in three dimensional spaces are taken into account. The even order case was substantially settled by Segre's himself in 1959 [**58**], whereas the problem of constructing infinite families of complete caps of size close to the trivial lower bound is still wide open for odd q's. This explains why the problem of constructing finite families has received some attention. An original construction will be the object of Chapter 5. On the other hand, when the dimension is greater than 3, a number of new results have appeared in the last decade, and new notions have emerged as powerful tools in dealing with the covering problem, including that of a bicovering arc. The chapter is focused on recursive constructions of complete caps which will be used in the subsequent chapters.

Chapter 3, Chapter 4 and Chapter 5, describe the original results of the thesis, which are the objects of four publications [**1, 2, 5, 54**].

In Chapter 3, new infinite families of complete caps have been constructed in Galois spaces of order $q = p^h$, with $p > 3$. The method is based on some inductive constructions presented in Chapter 2 and on bicovering properties of certain plane arcs contained in singular cubic curves, previously investigated by T. Szőnyi in the eighties. For most pairs (N, p^h), with $h > 8$ and $N \equiv 0 \pmod 4$, complete caps of size at most $2pq^{\left(\frac{N}{2}-\frac{1}{8}\right)}$ in $AG(N, p^h)$ are described. Moreover, for suitable divisors m of $q+1$ or $q-1$, new complete plane caps of size roughtly q/m have been obtained, provided that $(m, 6) = 1$ and $m < \frac{1}{4}q^{1/4}$. When such a divisor m factors as a product $m_1 m_2$ with $(m_1, m_2) = 1$, new complete caps in $AG(N, q)$ with less than $\frac{m_1+m_2}{m}q^{N/2}$

points have been obtained. On the one hand, these results significantly widen the spectrum of prime powers q for which complete plane caps with approximately $q^{3/4}$ points can be constructed. On the other hand, complete caps of size roughly $q^{(\frac{N}{2}-\frac{1}{8})}$ are obtained in Galois spaces of dimension N. For infinitely many q's these turn out to be the smallest complete caps constructed so far in $AG(N,q)$, with $N \equiv 0 \pmod 4$.

The following table summarizes a number of existence results for complete caps constructed from plane cubic curves, including those obtained in this thesis.

Table 1. Small complete caps in Galois spaces from cubic curves

p	N	Size $\leq$	Conditions	Ref.
>2	2	$\frac{q-1}{m}+m$	$m \mid q-1$ $m \leq \frac{1}{C}\sqrt[4]{q}$, $C>1$	[**3, 68, 69**]
>3	2	$\frac{q+1}{m}+m$	$m \mid q+1$ $m \leq \frac{1}{\sqrt{6}}\sqrt[4]{q}$ $(m,6)=1$,$(m,\frac{q+1}{m})=1$	Thm. 3.63
>3	$\equiv_4 0$	$2p^{\beta}q^{7/8}q^{\frac{N-2}{2}}$	$q=p^h$, $h>8$ $\beta=\frac{\log_p q}{8}-\lfloor\frac{\lceil\frac{\log_p q}{4}\rceil-1}{2}\rfloor$	Thm. 3.20
>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, $7<m<\frac{1}{8}\sqrt[4]{q}$	[**3**]
>3	$\equiv_4 0$	$\frac{m_1+m_2}{m_1m_2}q^{N/2}$	$m_1m_2 \mid q-1$ $m_1m_2 \leq \frac{1}{3.5}\sqrt[4]{q}$ $(m_i,6)=1$,$(m_1,m_2)=1$	Thm. 3.42
>3	$\equiv_4 0$	$(\frac{m_1+m_2}{m_1m_2}(q+1)+3)q^{\frac{N-2}{2}}$	$m_1m_2 \mid q+1$ $m_1m_2 \leq \frac{1}{4}\sqrt[4]{q}$ $(m_i,6)=1$,$(m_1,m_2)=1$	Thm. 3.68
>3	$\equiv_4 0$	$\sim(\frac{m_2+(3/2)m_1}{m_1m_2})q^{N/2}$	m prime, $m \mid q^2-1$ $m_1m_2=m+5$ $m_1>7$ odd, $m_2>4$ $m \leq \frac{1}{4}\sqrt[4]{q}$	Sect. 3.4

A final section is also devoted to applications to Coding Theory, and the close relationship between linear codes with covering radius 2 and caps in Galois spaces is explained in details.

In Chapter 4, complete arcs arising from elliptic curves embedded in Galois spaces of higher dimensions are described. A key tool is the notion of a maximal k-independent subset of a finite group, which is of independent interest in additive combinatorics. For most pairs (N, q), with q odd and large enough, and N less than $\sqrt[12]{q}$, these arcs are the smallest complete arcs in the projective Galois space $PG(N, q)$ known in the literature. These results are of particular interest in Coding Theory, since complete arcs correspond to optimal codes (also known as MDS codes) whose covering radius is the smallest achievable.

In Chapter 5 we present a construction of small complete caps in three-dimensional affine spaces over finite fields of odd order from elliptic curves.

CHAPTER 1

Notation and Preliminaries

1.1. Algebraic function fields

In this section we recall some basic facts about the theory of function fields, extensions of function fields and a particular type of Galois extensions of function fields, namely Kummer extensions. For detailed proofs see [**64**]. We recall the definition of an algebraic function field over an arbitrary field K.

Definition 1.1. An *algebraic function field* over K is an extension field F of K such that F is a finite algebraic extension of $K(x)$, with $x \in F$ trascendental over K. If $F = K(x)$, then F is called the *rational function field over* K. The *full constant field* of F (also called the *field of constants* of F) is the finite extension K' of K, consisting of the elements in F that are algebraic over K.

We can equivalently say that K is algebraically closed in F or that K is the full constant field of F, that is $K = K'$.

From now on, we assume that K is an algebraically closed field. Now, we recall the definitions of valuation rings and places of a function field. Such definitions are motivated by the case of a rational function field, whose valuation rings are a useful tool in order to determine zeros and poles (with their multiplicity) of all the rational functions $f(x) \in K(x)$.

Definition 1.2. A *valuation ring* of F is a ring $\mathcal{O} \subseteq F$ with the following properties:

(1) $K \subsetneq \mathcal{O} \subsetneq F$,
(2) for every $z \in F$ we have that $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

The following proposition gives a useful characterization of the valuation rings of a rational function field.

Proposition 1.3. *Let $K(x)$ be a rational function field over K and $p(x) \in K(x)$ be an irreducible monic polynomial; then the set*

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x],\ p(x) \nmid g(x) \right\}$$

is a valuation ring of $K(x)$. Moreover, if $q(x)$ is another irreducible monic polynomial, then $\mathcal{O}_{p(x)} \neq \mathcal{O}_{q(x)}$.

Definition 1.4. Let A be a domain but not a field; A is said to be a *discrete valuation ring* if it is a local, noetherian ring whose only maximal ideal is principal.

Proposition 1.5. [**64**, Proposition 1.1.5. and Theorem 1.1.6.] *A valuation ring $\mathcal{O}$ of a function field F is a discrete valuation ring, whose maximal ideal consists of the non-invertible elements of $\mathcal{O}$.*

Definition 1.6. Let $\mathcal{O}$ be a valuation ring of F. A *place* of F is the maximal ideal of $\mathcal{O}$. A generator of a place γ, that is an element $t \in \gamma$ such that $\gamma = t\mathcal{O}$, is called a *local parameter* for γ.

We denote by $\mathbb{P}_F := \{\gamma \mid \gamma \text{ is a place of } F\}$ the set of places of F.

As a consequence of Proposition 1.5, $\mathcal{O}$ is uniquely determined by γ, namely $\mathcal{O} = \{z \in F \mid z^{-1} \notin \gamma\}$. Consequently $\mathcal{O}_\gamma := \mathcal{O}$ is called the *valuation ring of the place* γ.

Another equivalent description of the concept of a place is given in terms of discrete valuations, that is a place of a function field can be associated with a discrete valuation and conversely.

Proposition 1.7. *Let t be a local parameter of γ. Then, every $0 \neq x \in F$ has a unique representation $x = ut^n$, where $u \in \mathcal{O}_\gamma \setminus \gamma$ and $n \in \mathbb{Z}$.*

Definition 1.8. A *discrete valuation* of F in γ is a function

$$\begin{aligned} v_\gamma : F &\to \mathbb{Z} \cup \{\infty\} \\ x \mapsto v_\gamma(x) &:= \begin{cases} n & x \neq 0 \\ \infty & x = 0 \end{cases}, \end{aligned}$$

where n is defined as in Proposition 1.7, with the following properties:

(1) $v_\gamma(xy) = v_\gamma(x) + v_\gamma(y)$, for all $x, y \in F$,
(2) $v_\gamma(1/y) = -v_\gamma(y)$, for all $y \in F$,
(3) $v_\gamma(x + y) \geq \min\{v_\gamma(x), v_\gamma(y)\}$, for all $x, y \in F$; also, equality holds if $v_\gamma(x) \neq v_\gamma(y)$.

It makes sense to introduce the following terminology.

Definition 1.9. Let $z \in F$ and let γ be a place of F. We say that γ is a *zero* of z of order $v_\gamma(z)$ if $v_\gamma(z) > 0$, alternatively that γ is a *pole* of z of order $-v_\gamma(z)$ if $v_\gamma(z) < 0$.

Theorem 1.10. *For any place γ of F, we have*

$$\mathcal{O}_\gamma = \{z \in F \mid v_\gamma(z) \geq 0\},$$
$$\gamma = \{z \in F \mid v_\gamma(z) > 0\},$$

$$\mathcal{O}_\gamma \setminus \gamma = \{z \in F \mid v_\gamma(z) = 0\}.$$

An element $x \in F$ is a local parameter for γ if and only if $v_\gamma(x) = 1$.

Let F be a function field over K and let γ be a place of F.

Definition 1.11. The *residue class map* with respect to γ is the map

$$\begin{array}{rccc} \pi_\gamma : & F & \rightarrow & F_\gamma \cup \{\infty\} \\ & x & \mapsto & x(\gamma) := \begin{cases} x + \gamma & \text{if } x \in \mathcal{O}_\gamma \\ \infty & \text{if } x \in F \setminus \mathcal{O}_\gamma \end{cases} \end{array} \tag{1.1}$$

where

i) $F_\gamma := \mathcal{O}_\gamma/\gamma$ is the quotient field of $\mathcal{O}_\gamma$ over γ itself, called the *residue class field* of γ;
ii) an element $x(\gamma)$ of F_γ is called the *residue class field* of x modulo γ;

Remark 1.12. *By Definition* 1.2 *and Proposition* 1.5*, we know that $K \subsetneq \mathcal{O}_\gamma$ and $K \cap \gamma = \{0\}$, so the residue class map in* (1.1) *induces a canonical embedding of K into F_γ. As K is an algebraically closed field, we can read an element $z \in F$ as a function:*

$$\begin{array}{rccc} z : & \mathbb{P}_F & \rightarrow & K \cup \{\infty\} \\ & \gamma & \rightarrow & z(\gamma) \end{array} \tag{1.2}$$

This is why the extension field F over K is called a function field. The elements of K, interpreted as functions in the sense of (1.2)*, are constant functions.*

The divisor group $\text{div}(F)$ of F is the free (additive) abelian group generated by $\mathbb{P}_F$. For definitions and properties of divisors of a function field we refer to [**64**].

Definition 1.13. The *genus* of F is defined by

$$g := \max\{\text{deg}A - \ell(A) + 1 \mid A \in \text{div}(F)\},$$

where $\text{deg}A$ is the degree of A and $\ell(A)$ is the dimension of the Riemann-Roch space $L(A)$ associated to A.

Now, we recall the definition and the main properties of extensions of function fields.

Definition 1.14. Let F be a function field over K. An algebraic function field F' over K is an *algebraic extension* of F if F' is an algebraic extension over F (or if F' is an extension field of F). Moreover, F' is a *finite algebraic extension* of F if the extension degree $[F' : F]$ is finite.

From now on, let F' be a finite algebraic extension of F and let γ' and γ be two places of F' and F respectively. Denote also by $\mathcal{O}'_\gamma$ and $\mathcal{O}_\gamma$, v_γ and $v_{\gamma'}$ their corresponding valuation rings and discrete valuations.

Definition 1.15. Under these assumptions:

i) the place γ' is said to be *lying over* (or to be an *extension* of) γ, and we write $\gamma'|\gamma$, if $\gamma \subseteq \gamma'$.
ii) the integer $e(\gamma'|\gamma) := e \geq 1$, such that

$$v_{\gamma'}(x) = e \cdot v_{\gamma}(x), \text{ for all } x \in F,$$

is called the *ramification index* of γ' over γ; moreover, the extension γ' of γ is *ramified* if $e(\gamma'|\gamma) > 1$, otherwise it is *unramified* if $e(\gamma'|\gamma) = 1$;

Remark 1.16. *The place γ' lies over γ when $\gamma = \gamma' \cap F$ and $\mathcal{O}_{\gamma} = \mathcal{O}_{\gamma'} \cap F$; this is the reason why γ is also called the restriction of γ' to F.*

Proposition 1.17. [**64**, Proposition 3.1.7] *For each place γ' of F' there is exactly one place γ of F, called the centre of γ' such that γ' is an extension of γ, namely $\gamma' = \gamma \cap F$. Conversely, every place γ of F has at least one, but only finitely many extensions γ' of F'.*

Definition 1.15-ii) naturally extends to finite extensions of function fields.

Definition 1.18. According to whether $e(\gamma'|\gamma) > 1$ or $e(\gamma'|\gamma) = 1$, for every γ' place of F' lying over a place γ of F and for every γ place of F, the algebraic extension F' over F is said to be *ramified* or *unramified.*

Transitivity of ramification index holds, as it is shown by the following proposition.

Proposition 1.19. *Let F'' be an algebraic extension of F'. If $\gamma' \in \mathbb{P}_{F'}$ is an extension of $\gamma \in \mathbb{P}_F$ and $\gamma'' \in \mathbb{P}_{F''}$ is an extension of $\gamma' \in \mathbb{P}_F$, then*

$$e(\gamma''|\gamma) = e(\gamma''|\gamma') \cdot e(\gamma'|\gamma).$$

Theorem 1.20. [**64**, Theorem 3.1.11] *If $\gamma_1, \ldots, \gamma_m$ are all the places of F' lying over a place γ of F, then*

$$\sum_{i=1}^{m} e_i = [F' : F],$$

where e_i denote the ramification indexes of γ_i over γ, for $i = 1, \ldots, m$.

As a consequence of Theorem 1.20, the number of places of F' lying over a place of F is less than or equal to the extension degree $[F' : F]$; also, $e_{\gamma'} \leq [F' : F]$ holds, for every place γ' lying over γ.

Definition 1.21. Under the assumptions of Theorem 1.20, if $[F' : F] = n$, then:

i) γ *splits completely* in F' if there are exactly n distinct places γ_i of F' lying over γ, with $e_{\gamma_i} = 1$, for $i = 1, \ldots, n$;

ii) alternatively, γ is *totally ramified* in F' if there is only one place γ' of F' lying over γ with $e_{\gamma'} = n$.

For a field extension F of K, we denote by

$$\mathrm{Aut}(F/K) = \{\sigma : F \to F \mid \sigma(a) = a, \forall\, a \in K\}$$

the group of automorphisms of F over K.

In general, if F is a finite extension, then $|\mathrm{Aut}(F/K)| \leq [F : K]$; also, F is said to be a *Galois extension* if equality holds. In this case, we denote by $\mathrm{Gal}(F/K) := \mathrm{Aut}(F/K)$ and say that it is the *Galois group* of F. A Galois extension F is said to be *cyclic* if its Galois group is cyclic.

An extension F' of a function field F is said to be Galois if F' is a Galois extension of finite degree over F. In addition, such an extension is said to be *cyclic* if F' is a cyclic extension over F.

Next theorem collects the definition and some properties of a special type of Galois extensions of a function field, that is Kummer extensions. An estimate of the genus of such extensions, which will be useful for our results is also included.

THEOREM 1.22 (Proposition 3.7.3 in [**64**]). *Let F be a function field over K and let $m > 1$ be an integer relatively prime to the characteristic of K. Suppose that $u \in F$ is an element satisfying*

$$u \neq \omega^e \textit{ for all } \omega \in F \textit{ and } e \mid m,\ e > 1. \tag{1.3}$$

Let

$$F' = F(y) \textit{ with } y^m = u,$$

then

i) *F' is a cyclic Galois extension of F of degree m;*

ii) *for a place γ' of F' lying over a place γ of F, we have*

$$e(\gamma'|\gamma) = \frac{m}{r_\gamma}, \qquad \textit{where } r_\gamma := (m, v_\gamma(u)) > 0 \tag{1.4}$$

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

iii) *if g (resp. g') denotes the genus of F (resp. F') as a function field over K, then*

$$g' = 1 + m(g-1) + \frac{1}{2} \sum_{\gamma \in \mathbb{P}_F} (m - r_\gamma),$$

where r_γ is defined as in (1.4).

An extension such as F' in Theorem 1.22 is said to be a *Kummer extension* of F.

1.2. Algebraic curves and function fields

Let q be an odd prime power, and let $\mathbb{F}_q$ denote the finite field with q elements. Throughout this chapter, $\mathbb{K}$ will denote the algebraic closure of $\mathbb{F}_q$. Also, by a curve we will mean a projective, absolutely irreducible, algebraic curve defined over $\mathbb{K}$.

It is well known that one can associate a rational function field $\mathbb{K}(\mathcal{C})$ over $\mathbb{K}$ to a generic curve $\mathcal{C}$, 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.

As a rule, 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. This corrispondence makes it possible to translate definitions and results from the language of algebraic function fields to the language of algebraic curves and vice versa. For example, the genus of F as a function field coincides with the genus of $\mathcal{C}$, it is possible to define divisors of a non-singular curve as formal sums of points, and formulate the Riemann-Roch Theorem with both the languages of algebraic curves and function fields.

Definition 1.23. 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 $\mathbb{F}_q$ and it is a rational function field over $\mathbb{F}_q$.

Definition 1.24. A place of $\mathbb{K}(\mathcal{C})$ is said to be $\mathbb{F}_q$*-rational* if it is fixed by the Frobenius map on $\mathbb{K}(\mathcal{C})$.

Proposition 1.25. [**37**, Theorem 8.29 and 8.31] *The centre 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.*

Here we report a Corollary of Theorem 1.22, which will be useful for our results.

Corollary 1.26. *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 $\mathbb{K}(\mathcal{C})(\omega)$, with $\omega^2 = u$, is the function field of some irreducible curve $\mathcal{C}'$ 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 $\mathbb{K}(\mathcal{C})(\omega)$ as in Corollary 1.26 is said to be a *double cover* of $\mathbb{K}(\mathcal{C})$ and similarly the corresponding irreducible curve $\mathcal{C}'$ defined over $\mathbb{F}_q$ is called a *double cover* of $\mathcal{C}$.

Remark 1.27. *Fix an affine coordinate system* (X, Y, Z) *in the three-dimensional space over* $\mathbb{K}$. *Under the assumptions of Corollary* 1.26 *note that, up to birational equivalence,* $\mathcal{C}'$ *is a component of the space curve with equation*

$$\begin{cases} f(X,Y) = 0 \\ h(X,Y) = Z^2 g(X,Y) \end{cases},$$

where $\mathcal{C} : f(X,Y) = 0$ *and* $u = h/g \in \mathbb{F}_q(\mathcal{C})$ *are as in Corollary* 1.26.

It is well known that every algebraic curve admits a non-singular model which is birationally equivalent to an algebraic plane curve. Thus, the following proposition give a useful tool to estimate the genus of a generic algebraic curve.

Proposition 1.28. *Let* $\mathcal{C}$ *be an algebraic plane curve of genus* g *and degree* n*; then*

$$g \leq \frac{1}{2}(n-1)(n-2) - \sum_{P \in \mathcal{C}} \frac{m_P(m_P - 1)}{2}, \tag{1.5}$$

where m_P *is the multiplicity of* $\mathcal{C}$ *in* P *and equality holds if* $\mathcal{C}$ *has at most ordinary singularities.*

The integer at the right hand side of (1.5) in Proposition 1.28 is called the *virtual genus* of the curve $\mathcal{C}$.

A criterion due to Segre to prove the absolute irreducibility of an algebraic plane curve is reported.

Proposition 1.29. [**60**][**63**, Lemma 8]*If a projective plane curve* $\mathcal{C}$ *of degree* δ *has a point* Q *and a tangent line* ℓ *at* Q *such that* ℓ *counts once among the tangents of* $\mathcal{C}$, $\mathrm{I}(Q, \mathcal{C} \cap \ell) = \delta$, *and* $\mathcal{C}$ *has no linear component through* Q, *then* $\mathcal{C}$ *is absolutely irreducible.*

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

Theorem 1.30 (Hasse–Weil Bound). *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*

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

1.3. Order and class of a place with respect to a plane model

Throughout this section, let $\mathcal{C}$ be an algebraic plane curve defined by the equation $f(X,Y) = 0$, where $f(X,Y)$ is an irreducible polynomial over $\mathbb{K}$. Let $\mathbb{K}(\mathcal{C})$ be the function field of $\mathcal{C}$ and 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 $f(\bar{x}, \bar{y}) = 0$.

For brevity, let $\mathbb{P}_{\mathcal{C}}$ denote the set of all places of $\mathbb{K}(\mathcal{C})$ and let $\mathcal{D}$ be the subset of $\mathrm{Div}(\mathbb{K}(\mathcal{C}))$ given by

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

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 [**37**]. 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 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

$$v_\gamma(D(\ell)) \in \{0, j_1(\gamma), j_2(\gamma)\}. \tag{1.6}$$

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

Theorem 1.31. *Let Q be a point of $\mathcal{C}$ and let 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 $v_\gamma(D(\ell))$ coincides with $j_1(\gamma)$ 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.

1.4. Classification of singular cubic curves with at least one rational inflection

The plane curves to be considered throughout this section are absolutely irreducible projective plane curves, i. e. curves of type $\mathcal{F} : F(X, Y, Z) = 0$, where $F(X, Y, Z)$ is an irreducible cubic form, that is a homogeneous polynomial of degree 3 in $\mathbb{F}_q[X, Y, Z]$, which does not factor in $\mathbb{K}[X, Y, Z]$.

From Proposition 1.28, it follows that the genus of a cubic curve is always less than or equal to 1; consequently, such curves can have at most one singularity. Also, this singular point can have 2, 1 or 0 distinct *rational tangents*, (that is tangents whose defining polynomials have coefficients in $\mathbb{F}_q$), according to the type of the singularity.

Actually, three types of singularities are possible accordingly to the three different types of non-degenerate singular cubics:

> **Type I** – Cubics with a node: having two distinct rational tangents at the singular point;
> **Type II** – Cubics with a cusp: having two coincident rational tangents at the singular point;
> **Type III** – Cubics with an isolated double point: having two distinct non-rational tangents at the singular point.

A non-singular point $P \in \mathcal{F}$ is a *point of inflection* if the tangent at P has triple contact with the curve, [**37**, Section 1.3]. Thus in particular, the tangent line at an inflection P of a cubic curve has no other point in common with the curve. These conditions are expressed algebraically by the requirement that

$$F(X,Y,Z) = f(X,Y,Z) \cdot g(X,Y,Z) + (aX + bY + cZ)^3$$

where

i) $f(X,Y,Z)$ is the linear form defining the tangent line at P,
ii) $g(X,Y,Z)$ is some form of degree 2,
iii) $aX + bY + cZ$ is some linear form vanishing at P.

In general a cubic curve can also have no $\mathbb{F}_q$-rational inflection points; however it can be proved that it is always isomorphic over $\mathbb{K}$, to another cubic containing at least one inflection point. One of the inflection points is usually chosen to be the neutral element of the abelian group that can be defined over the set

$$\mathcal{F}(\mathbb{F}_q) = \{P \in PG(2,q) \mid F(P) = 0 \text{ and } P \text{ is simple}\}$$

of the non-singular rational points of the cubic. For main properties and definition of the group structure on a cubic we refer to [**11**] or [**36**, Chapter 11].

Here we briefly report the classification of singular cubic curves with at least one rational inflection, on finite fields $\mathbb{F}_q$ of characteristic greater than 3. From tables 11.3, 11.4 and 11.6 of [**36**, Chapter 11], there exists only one cubic for each type, up to projective equivalence, as remarked in the following proposition.

PROPOSITION 1.32. *Let $q = p^h$ with $p > 3$ and let $\mathcal{F}$ be an irreducible singular cubic with at least one rational inflection;*

- *if $\mathcal{F}$ is of type I, then it has the following canonical form*
$$\mathcal{F} : XYZ - (X - Z)^3 = 0;$$
- *if $\mathcal{F}$ is of type II, then it has the following canonical form*
$$\mathcal{F} : YZ^2 - X^3 = 0;$$
- *if $\mathcal{F}$ is of type III, then it has the following canonical form*
$$\mathcal{F} : Y(X^2 - \beta^2 Z^2) - Z^3 = 0,$$
where $\beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ is such that $\beta^2 \in \mathbb{F}_q$.

1.5. Covering density of quasi-perfect and MDS codes

Let $\mathbb{F}_q$ be the finite field with q elements. A q-ary linear code C of lenght n and dimension k is a k-dimensional linear subspace of $\mathbb{F}_q^n$. The number of non-zero positions in a vector $v \in \mathbb{F}_q^n$ is called the Hamming weight $\omega(v)$ of v. For v_1, $v_2 \in \mathbb{F}_q^n$ the Hamming distance $d(v_1, v_2)$ is the weight $\omega(v_1 - v_2)$. The minimum distance of C is
$$d(C) := \min\{\omega(x) \mid x \in C, x \neq 0\}$$
and a q-ary linear code of lenght n, dimension k and minimum distance d is called an $[n, k, d]_q$-code. Such a code is said to be t-error correcting, where t is the integer part of $(d - 1)/2$. The covering radius of C is the minimum integer $R(C)$ such that for any vector $v \in \mathbb{F}_q^n$ there exists $x \in C$ with $d(v, x) \leq R(C)$. An $[n, k, d]_q$-code with covering radius ρ is denoted by $[n, k, d]_q\rho$. Clearly, $R(C) \geq t$ holds and when equality is attained the code C is said to be perfect. As there are only finitely many classes of linear perfect codes, of particular interest are those codes C with $R(C) = t + 1$, called quasi-perfect codes (see [**9, 12, 13**]).

Another relevant class of codes are the MDS (Maximum Distance Separable) codes, that is codes meeting the Singleton Bound. A number of properties of an MDS code, including its Hamming weight distribution, only depend on its length and dimension. This is not the case for the covering radius. For an MDS code the covering radius $R(C)$ is either s or $s - 1$, s beeing the codimension of the code; see e.g. [**20**]. It is worth noticing that when $r = 4$, MDS codes with covering radius 3 are quasi-perfect codes.

One of the parameters characterizing the covering quality of an $[n, k, d]_q\rho$-code C is its covering density $\mu(C)$, first introduced in [**14**] as the average number of codewords at distance less than or equal to ρ from a vector in $\mathbb{F}_q^n$:
$$\mu(C) = \frac{V_q(n, \rho)}{q^{n-k}},$$

where

$$V_q(n,j) = \sum_{i=0}^{j} \binom{n}{i} (q-1)^i$$

is the size of a sphere of radius j in $\mathbb{F}_q^n$. The covering density $\mu(C)$ is always greater than or equal to 1, and equality holds precisely when C is perfect. Among codes with the same codimension s and covering radius ρ, the shortest ones have the best covering density. This motivates the following notation:

$l(s,\rho,q)_d$ is the the minimal length n for which there exists an $[n, n-s, d]_q\rho$-code with given s, q, d and ρ.

The problem of estimating $l(s,\rho,q)_d$ has been broadly investigated (see the seminal paper [**10**], as well as the recent survey [**17**] and the references therein).

In sections 3.5 and 4.3 we will determine some upper-bounds on $l(s+1,2,q)_4$ and $l(s,s-1,q)_{s+1}$, based on our geometrical results.

CHAPTER 2

Complete arcs and caps in Galois spaces

Let $\Sigma = \Sigma(N,q)$ be a Galois space of dimension N, over the finite field with q elements.

Definition 2.1. A *k-arc* of Σ is a set of k points no $N+1$ of which are contained in the same hyperplane. A *k-cap* of Σ is a set of k points no three of which are collinear. A k-cap/k-arc is said to be *complete* if it is maximal with respect to set theoretical inclusion, that is, if it is not contained in a $(k+1)$-cap/$(k+1)$-arc.

Clearly, a plane k-cap is a k-arc.

Definition 2.2. Let A be an arc and let C be a cap of Σ. A point $P \notin C$ is said to be *covered* by C if it is collinear with two distinct points of C, while a point $P \notin A$ is said to be *covered* by A if it is contained in a hyperplane generated by N points of A.

2.1. Complete arcs and caps in Galois spaces of dimension 2 and 3

Since the seminal work by B. Segre, complete arcs in Galois planes have played a prominent role in Finite Geometry. The theory of plane arcs is well developed and quite rich of constructions (see [**35, 40, 41, 69, 70**] and the references therein, as well as the monograph [**36**] for a deeper treatment).

The maximum value of k for a plane k-arc to exist is denoted by $m(2,q)$, and a plane k-arc with this number of points is said to be an *oval* or a *hyperoval* according to whether q is odd or even. For arcs in $PG(2,q)$ the main results are summarized in the following table.

Table 1. Values of $m(2,q)$

q	$m(2,q)$
q odd	$q+1$
q even	$q+2$

A complete classification for ovals in $PG(2,q)$ is known when q is odd; otherwise, when q is even, there are a number of infinite families of hyperovals and there is as yet no classification. In fact, from a classical result due to Segre, it is well known that $m(2,q)$-arcs coincides with the rational points of a conic, when q is odd, while Bose showed that, when q is even, a conic plus its nucleus is an $m(2,q)$-arc. A hyperoval of this type is called *regular* and Segre [**62**] showed that every hyperoval is regular for $q = 2,4,8$. Otherwise, for $q = 2^h$, $h \geq 4$, there exist *irregular* hyperovals, that is hyperovals which are not the union of a conic plus its nucleus. Several infinite classes of irregular hyperovals are known. For a detailed description we refer to [**41**].

In order to generalize his famous theorem to higher dimensions, Segre proved the incompleteness of q-arcs of $PG(2,q)$, q odd, that is a plane q-arc is always contained or can be completed to an oval. A similar assertion for Galois planes of even order was proved by Tallini. These results initiated the study of upper-bounds for the size of non-oval and non-hyperoval complete arcs.

In fact, finding values of k for which a k-arc is always contained in an $m(2,q)$-arc is equivalent to that of determining an upper bound for the second largest size $m'(2,q)$ of a complete arc which is not an oval nor a hyperoval. Consequently, any k-arc with $k > m'(2,q)$ is contained in an $m(2,q)$-arc.

The following table surveys the known results on this problem. In particular, for q satisfying the conditions in the first column, the second column gives an upper bound on $m'(2,q)$, the third column indicates when this upper bound is sharp, the fourth column contains the references for such results.

Table 2. Upper bounds for $m'(2,q)$

	q	$m'(2,q)$	Sharp	Ref.
(1)	$q = p^{2e}$, $p > 2, e \geq 1$	$\leq q - \sqrt{q}/4 + 25/16$		[**73**]
(2)	$q = p^{2e+1}$, $p > 2, e \geq 1$	$\leq q - \sqrt{pq}/4$ $+29p/16 + 1$		[**76**]
(3)	q prime, $q > 2$	$\leq 44q/45 + 8/9$		[**74**]
(4)	$q = p^h, p \geq 5$	$\leq q - \sqrt{q}/2 + 5$		[**37**]
(5)	$q = p^h, p \geq 3$ $q \geq 23^2, q \neq 5^5, 3^6,$ h even for $p = 3$	$\leq q - \sqrt{q}/2 + 3$		[**38, 39**]
(6)	$q = 2^{2e}, e > 1$	$= q - \sqrt{q} + 1$		[**8, 25, 44**]
(7)	$q = 2^{2e+1}, e \geq 1$	$\leq q - 2\sqrt{q} + 2$	$q = 8$	[**76**]

The sharpness of (6) was shown independently by Boros and Szőnyi [**8**], Fisher, Hirschfeld and Thas [**25**], and Kestenband [**44**]. Details of the constructions can also be found in [**69**].

Another natural question is about the uniqueness of a complete arc contaning a given k-arc. That the arcs considered in (6) are unique follows from Hirschfeld [**36**, Section 8.7], Lisonek, Chao and Kaneta. Also, the following result holds.

Theorem 2.3. *For $q = p^{2e}$, $q > 4$, a complete $(q - \sqrt{q} + 1)$-arc exists in $PG(2, q)$ and it is projectively unique for $q = 9, 16, 25$.*

Conjecture 2.4. $m'(2, q) = q - \sqrt{q} + 1$ for $q = p^{2e}$, $q > 9$.

Better results for $q = 2^{2e}$, with $e > 2$ are obtained by Hirschfeld and Korchmáros.

Theorem 2.5. [**37**] *A complete arc of $PG(2, q)$ has size either $q + 2$, $q - \sqrt{q} + 1$ or at most $q - 2\sqrt{q} + 6$. For $q = 16$, the list of sizes of complete arcs in $PG(2, q)$ is* $9, 10, 11, 12, 13, 18$.

General lower and upper bounds on the smallest size $t(2, q)$ of a complete arc in $PG(2, q)$ are given in the following table. The trivial lower bound is obtained by Segre in [**57**], whereas an improvement on the lower bound is obtained by Blokhuis [**7**], Ball [**4**] and Polverino [**55**], for $q = p, p^2$ and p^3 respectively. The upper bound of Kim and Vu [**46**] is obtained via the probabilistic method, and d and c are absolute constants.

Table 3. Lower and upper bounds for $t(2, q)$

q	$t(2, q)$	Ref.
q	$> \sqrt{2q} + 1$	[**57**]
$q = p^h, p$ prime, $h = 1, 2, 3$	$> \sqrt{3q} + 1/2$	[**7, 4, 55**]
q	$\leq d\sqrt{q}\log^c q$	[**46**]

A remarkable idea in order to obtain complete plane arcs is that of properly choosing some algebraically parametrized subsets of points contained in conic or cubic curves, in such a way that they are arcs. Then, to prove the completeness of such arcs, a typical method due to Segre [**60**] and Lombardo Radice [**48**] (see also [**70**]), is applied.

Let $\mathcal{X}$ be a conic or a cubic curve and let S be a subset of $\mathcal{X}$ which is also an arc. Write S in an algebraically parametrized form; i.e. consider rational functions over $\mathbb{F}_q$, say $u(T), v(T)$, in such a way that

$$S = \{(u(t), v(t)) \mid t \in A\}, \tag{2.1}$$

where A can be either $\mathbb{F}_q$ or $\mathbb{F}_q^*$. In the case of cubic curves, this can be easily done when $\mathcal{X}$ is singular.

Method 1

For a point $P = (a, b)$ off $\mathcal{X}$:

C1) Construct an algebraic curve

$$\mathcal{C}_P : f_P(X, Y) = 0, \tag{2.2}$$

defined over $\mathbb{F}_q$, where

$$f_P(X, Y) = \begin{pmatrix} a & b & 1 \\ u(X) & v(X) & 1 \\ u(Y) & v(Y) & 1 \end{pmatrix}$$

As $u(X)$ and $u(Y)$ are rational functions describing the first coordinate of two distinct points in S, such a curve clearly describes the collinearity of two distinct points of S with P.

C2) Show that $\mathcal{C}_P$ is absolutely irreducible or has at least an absolutely irreducible component defined over $\mathbb{F}_q$; also, compute an upper bound $\bar{g}$ for the genus of $\mathcal{C}_P$ (or of its irreducible $\mathbb{F}_q$-rational component).

C3) Apply the Hasse–Weil bound (see Theorem 1.30). Then, if q is large enough with respect to $\bar{g}$, the existence of a suitable $\mathbb{F}_q$-rational affine point (x_0, y_0) of $\mathcal{C}_P$ is guaranteed. This is sufficient to deduce the collinearity between P and the points $(u(x_0), v(x_0))$ and $(u(y_0), v(y_0))$ of S.

C4) It is possible that for a few points P the curve $\mathcal{C}_P$ is reducible and does not admit an $\mathbb{F}_q$-rational component. In this case, P may not be covered by the secants of S. In order to obtain the completeness, it is necessary to extend the arc S with some of such points.

Whereas, some extrapoints on $\mathcal{X}(\mathbb{F}_q)$ need to be added to S in order to obtain a complete arc. In this context, the notion of a maximal 3-independent subset, which will be given in Section 2.4, is relevant.

To conclude this section, we recall some results about complete caps in $PG(3, q)$.

In $PG(3, q)$, the trivial lower bound (0.1) on the size of a complete cap reads $\sqrt{2}q$ and, if q is even, it is substantially sharp. In fact, the existence of a complete cap of size $3q + 2$ was showed by Segre [**58**]. Also, Segre's construction was generalized by Pambianco and Storme [**51**], who obtained complete caps of size $2q + n$ for each n such that there exists a complete arc with n points in $PG(2, q)$ (see also [**15**]). When q is odd, the size of the smallest complete caps are known for $q \leq 5$ and, for generic values of q, the smallest known complete caps have size of the same order of magnitude as q^2. In particular, infinite families of complete caps of size approximately $q^2/2$ [**34**] and $q^2/3$ [**21, 22**] sharing many points with an elliptic quadric have been obtained by generalizing the classical method by Segre and Lombardo Radice. Segre's construction for q even consists of three conics, plus two points. In 1998, Pellegrino tried to extend this idea to the odd order case; see [**53**]. He claimed that it is possible to choose s conics with $\binom{s-1}{2} \leq \frac{q+1}{4}$ in such a way that their union, together with few extra points, is a complete cap of size less than or equal to $\frac{\sqrt{q}}{2}q + 2$. A major gap in Pellegrino's completeness proof has recently emerged; see [**6**]. Nonetheless, his idea turned out to be useful to construct small complete caps by computer.

THEOREM 2.6. [**6**] *Assume that* $19 \leq q \leq 30000$*,* q *odd. Then there exists a complete cap in* $AG(3,q)$ *with size at most* $a_q(q+1)+2$*, where*

$$a_q = \begin{cases} 4 & if 19 \leq q \leq 37, \\ 5 & if 41 \leq q \leq 121, \\ 6 & if 127 \leq q \leq 509, \\ 7 & if 521 \leq q \leq 2347, \\ 8 & if 2351 \leq q \leq 5227, \\ 9 & if 5231 \leq q \leq 29989, \end{cases}$$

with the only exceptions of $q = 10531, 18493, 18973, 23677, 24077, 24121, 25163, 25639$*,* 26227*,* 28643*, where* $a_q = 10$*.*

It is worth noticing that for $q \leq 97$, smaller complete caps were obtained in [**15, 50**], while for $100 < q < 350$, smaller complete caps which turn out to be the smallest complete caps known in literature, were obtained from elliptic curves in Chapter 5.

2.2. Recursive constructions for complete caps

Since the theory of caps in small dimensional spaces is well developed and quite rich of constructions, to obtain complete caps in higher dimension a natural idea is to try to use some kind of lifting methods. We recall two well-known recursive constructions for caps in affine spaces.

- **Blow-up construction**
  For a positive integer r, fix a basis of $\mathbb{F}_{q^r}$ as a linear space over $\mathbb{F}_q$. Let

$$\begin{aligned} \pi_s : & AG(s,q^r) \to AG(rs,q) \\ & (x_1,\ldots,x_r) \mapsto (x_1^1,\ldots,x_1^s,\ldots,x_r^1,\ldots,x_r^s) \end{aligned}$$

  be the identification of $AG(s,q^r)$ with $AG(rs,q)$, which maps every coordinate $x_j \in \mathbb{F}_{q^r}$ into its expansion $x_j^1,\ldots,x_j^s$ with respect to the fixed basis of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$.

PROPOSITION 2.7. *If C is a cap in $AG(s, q^r)$, then $\pi_s(C)$ is a cap in $AG(rs, q)$, called the blow-up of C.*

- **Product construction**
  For two positive integers r, s, let

$$\begin{aligned}\pi_{r,s} :&AG(r,q) \times AG(s,q) \to AG(r+s,q)\\ &((x_1,\dots,x_r),(y_1,\dots,y_s)) \mapsto (x_1,\dots,x_r,y_1,\dots,y_s)\end{aligned}$$

  be the identification of $AG(r,q) \times AG(s,q)$ with $AG(r+s,q)$.

PROPOSITION 2.8. *If C_1 is a cap in $AG(r,q)$ and C_2 is a cap in $AG(r+s,q)$, then $\pi_{r,s}(C_1 \times C_2)$ is a cap in $AG(r+s,q)$.*

Now, let $\mathcal{P}(q) = \{(a, a^2) \mid a \in \mathbb{F}_q\}$ be the complete cap in $AG(2,q)$ consisting of the $\mathbb{F}_q$-rational points of the parabola. Recursive contructions applied to such a point-set, give interesting results on the sizes of the smallest complete caps in Galois spaces of higher dimensions. Here we report such constructions both in the even and in the odd order case.

First, we assume that q is even.

THEOREM 2.9. [**52**] *Let q be even. Then the blow-up of $\mathcal{P}(q^r)$ is a complete cap of size q^r in $AG(2r,q)$.*

THEOREM 2.10. [**16**] *Let q be even. Then the product of the blow-up of $\mathcal{P}(q^r)$ by any complete cap of size k in $AG(s,q)$ is a complete cap of size kq^r in $AG(2r+s,q)$.*

By Theorem 2.10 for $s = 1$, a complete cap of size $2q^r$ in $AG(2r+1,q)$ is obtained, as the product of the blow-up of $\mathcal{P}(q^r)$ by the trivial cap of the line $AG(1,q)$, consisting of two points $\{0,1\}$. This implies that, when the dimension $N = 2r+s$ is odd, the trivial lower bound (0.1) is substantially sharp, otherwise we get un upper bound of the order of $q^{\frac{N}{2}}$ on $t(N,q)$ by Theorem 2.9, with $N = 2r$.

In [**52**], it was also proved that

$$t(N,q) \leq \begin{cases} q^{\frac{N}{2}} + s_{N,q}, & N \text{ even},\\ (2+1)q^{\frac{N-1}{2}} + s_{N,q}, & N \text{ odd},\end{cases} \tag{2.3}$$

where

$$s_{N,q} := 3\left(q^{\lfloor\frac{N-2}{2}\rfloor} + q^{\lfloor\frac{N-2}{2}\rfloor-1} + \ldots + q\right) + 2.$$

For about a decade, (2.3) was the best known upper bound on $t(N,q)$, for $q > 2$

and $N > 3$, with the exception of few small values of both N and q. Inequality (2.3) was improved in [**29**]:

$$t(N,q) \leq \begin{cases} \frac{1}{2}q^{\frac{N}{2}} + s_{N,q}, & N \text{ even}, \\ (2+\frac{1}{2})q^{\frac{N-1}{2}} + s_{N,q}, & N \text{ odd}, \end{cases} \tag{2.4}$$

where $s_{N,q}$ is previously defined.
Better upper bounds were obtained for specific values of $q \leq 2^{15}$, see [**31**]. Also in [**31**] it was proved that

$$t(N,q) \leq \frac{1}{3}q^{\frac{N}{2}} + \frac{5}{3}q^{\frac{(N-2)}{2}} + s_{N,q} - 2 \quad q \geq 2^8 \text{ square}, N \geq 4 \text{ even}.$$

From now on, we assume that q is odd.

THEOREM 2.11. [**18**] *Let q be odd. Then the blow-up of $\mathcal{P}(q^r)$ is a complete cap in $AG(2r,q)$ if and only if r is odd.*

By theorem 2.11, for q odd and the dimension $N \equiv 2 \pmod 4$, we get un upper bound of the order of $q^{\frac{N}{2}}$ on $t(N,q)$.

In the following table we survey the more recent upper bounds for $t(N,q)$, for large values of q, with the respective references.

TABLE 4. Upper bounds for $t(N,q)$

N	q	$t(N,q)$	Ref.
even > 4	even ≥ 32 $\geq 2^6$ square	$\leq \frac{1}{2}q^{\frac{N}{2}} + \frac{5}{6}s_{N,q} + \frac{1}{3}$ $\leq \frac{1}{3}q^{\frac{N}{2}} + s_{N,q} + \frac{2}{3}$	[**16**]
odd > 5	even ≥ 32 $\geq 2^6$ square	$\leq \left(2+\frac{1}{2}\right)q^{\frac{N-1}{2}} + \frac{5}{6}s_{N,q} + \frac{1}{3}$ $\leq \left(2+\frac{1}{3}\right)q^{\frac{N-1}{2}} + s_{N,q} + \frac{2}{3}$	[**16**]
$\equiv_4 2$	odd, ≥ 5	$\leq q^{N/2} + t\left(\frac{N}{2}-1, q\right)$	[**18**]

A natural question to ask in order to obtain small complete caps in spaces of odd order and dimension $N \not\equiv 2 \pmod 4$, is whether the product of the blow-up of $\mathcal{P}(q^r)$, r odd, and a complete arc in $AG(2,q)$ is complete. In this context the notion of a bicovering and almost bicovering arc is useful.

2.3. Small complete caps from bicovering and almost bicovering arcs

According to Segre [**61**], 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

$$(x-x_1)(x-x_2) \text{ is a non-zero square in } \mathbb{F}_q \text{ or not,}$$

where x, x_1 and x_2 are the coordinates of P, P_1 and P_2 with respect to any affine frame of ℓ. Definition 13 in [**61**] extends as follows.

DEFINITION 2.12. Let A be a complete arc in $AG(2,q)$. A point $P \in AG(2,q) \setminus A$ is *regular (pseudo-regular)* with respect to A if it is external (internal) to any segment P_1P_2, with $P_1, P_2 \in A$ collinear with P. A point $P \in AG(2,q) \setminus A$ is *bicovered* by A if it is neither regular nor pseudo-regular.
If every point $P \in AG(2,q) \setminus A$ 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 an arc A in $AG(2,q)$ and an odd integer r, let

$$C_A = \{(\alpha, \alpha^2, u, v) \mid \alpha \in \mathbb{F}_{q^r}, (u,v) \in A\} \subseteq AG(2r+2,q)$$

denote the product of the blow-up of $\mathcal{P}(q^r)$ and A. As noticed in [**28**], the set C_A is a cap whose completeness in $AG(2r+2,q)$ depends on the bicovering properties of A in $AG(2,q)$.

The following results from [**28**] are a key tool in our construction.

PROPOSITION 2.13. [**28**, Proposition 4.2] *Let q be odd, and let A be a bicovering k-arc in $AG(2,q)$; then C_A is a complete cap in $AG(2r+2,q)$ of size kq^r, for every odd integer r.*

By a slight modification of the product construction it is possible to obtain complete caps from almost bicovering arcs. For an element $c \in \mathbb{F}_q$, let

$$\mathcal{P}_c(q) = \{(a, a^2 - c) \mid a \in \mathbb{F}_q\} \subseteq AG(2,q).$$

For a point $(x_0, y_0) \in AG(2,q)$, let

$$C_{(c,x_0,y_0)} = \{(\alpha, \alpha^2 - c, x_0, y_0) \mid \alpha \in \mathbb{F}_{q^r}\}$$

be the product of the blow-up of $\mathcal{P}_c(q^r)$ and the trivial cap of $AG(2,q)$ consisting of the simple point (x_0, y_0).

PROPOSITION 2.14. [**28**, Proposition 4.3] *Let q be odd and let c be a non square in $\mathbb{F}_q$. Also, let A be an almost bicovering k-arc admitting exactly one regular point (x_0, y_0). Then*

$$C = C_A \cup C_{(c,x_0,y_0)}$$

is a complete cap in $AG(2r+2,q)$ of size $(k+1)q^r$, for every odd integer r.

Proposition 2.15. [**28**, Proposition 4.4] *Let q be odd and let c be a non-zero square in $\mathbb{F}_q$. Also, let A be an almost bicovering k-arc admitting exactly one pseudo-regular point (x_0, y_0). Then*

$$C = C_A \cup C_{(c,x_0,y_0)}$$

is a complete cap in $AG(2r+2, q)$ of size $(k+1)q^r$, for every odd integer r.

We summarize Propositions 2.13, 2.14 and 2.15 in the next theorem.

Theorem 2.16. [**28**, Proposition 4.2, 4.3 and 4.4] *Let q be odd and let c be a non square in $\mathbb{F}_q$.*

i) *If A is a bicovering k-arc, then C_A is a complete cap in $AG(2r+2, q)$ of size $k \cdot q^r$, for every odd integer r;*
i) *If A is an almost bicovering k-arc with center $Q = (x_0, y_0)$, then either*

$$C = C_A \cup \{(\alpha, \alpha^2 - c, x_0, y_0) \mid \alpha \in \mathbb{F}_{q^r}\}$$

or

$$C = C_A \cup \{(\alpha, \alpha^2 - c^2, x_0, y_0) \mid \alpha \in \mathbb{F}_{q^r}\}$$

is a complete cap in $AG(2r+2, q)$ of size $(k+1)q^r$, for every odd integer r, according to whether Q is a regular or a pseudo-regular point.

Remark 2.17. *Since r is an odd integer, the dimension $N = 2r + 2$ of the affine spaces in which the complete caps of Theorem 2.16 are contained, is congruent to zero modulo 4.*

By Theorem 2.16, bicovering and almost bicovering plane arcs are a powerful tool to construct small complete caps in $AG(N, q)$, with q odd and $N \equiv 0 \pmod 4$. However, to establish whether a complete arc is bicovering or almost bicovering can be a difficult task. From previous results by B. Segre [**61**] if the arc A consists of the affine points of an ellipse or a hyperbola $\mathcal{C}$, it is almost bicovering, provided that $q > 13$. Note that, by appling Theorem 2.16 to these type of almost bicovering arcs, an upper bound of $q^{\frac{N}{2}}$ for $t(N, q)$ is obtained when the dimension N is congruent to zero modulo 4. In particular, such a bound is attained when the arc A is a hyperbola. Smaller complete arcs A in $AG(2, q)$ can be obtained by choosing some points on $\mathcal{C}$ and adding few extra-points (see e.g. [**45, 59, 72**]); in this case a point $Q \in \mathcal{C} \setminus A$ can hardly be bicovered, as there are few secants of A through Q. No such problem arises when complete arcs contained in cubic curves are considered.

In Sections 3.1.3, 3.2.2 and 3.3.4, we deal with the problem of determine bicovering and almost bicovering arcs contained in singular cubics. A remarkable idea in order to obtain such arcs consists of a generalization of the method due to Segre [**60**] and Lombardo Radice [**48**] (see also in Section 2.1), which is shown below.

Let $\mathcal{X}$ be a cubic curve and let S be the arc (2.1) contained in $\mathcal{X}$.

Method 2

For a point $P = (a, b)$ off $\mathcal{X}$ and a non-zero element $c \in \mathbb{F}_q$:

BC1) Construct a space curve

$$\mathcal{Y}_{P,c} : \begin{cases} f_P(X,Y) = 0 \\ (a - u(X))(a - u(Y)) = cZ^2 \end{cases} . \tag{2.5}$$

where $f_P(X,Y) = 0$ is the plane curve of Method 1 and $u(X)$ and $u(Y)$ are rational functions describing the first coordinate of two distinct points in S.

BC2) Apply C2)-C3) of Method 1 to $\mathcal{Y}_{P,c}$.
If q is large enough with respect to $\bar{g}$, the existence of a suitable $\mathbb{F}_q$-rational affine point (x_0, y_0, z_0) of $\mathcal{Y}_{P,c}$ is guaranteed. This is sufficient to deduce the collinearity between P and the points

$$P_{1,c} = (u(x_0), v(x_0)) \quad P_{2,c} = (u(y_0), v(y_0))$$

of S. Also, according to whether c is a non-zero square in $\mathbb{F}_q$ or not, the point P will be external or internal to the segment $P_{1,c}P_{2,c}$.

In order to bicover the points in $\mathcal{X}(\mathbb{F}_q)$, the notion of a maximal-3-independent subset of an abelian group is essential. As we will see in the next sections, it is possible to extend the arc S to an arc contained in $\mathcal{X}(\mathbb{F}_q)$ of size less than $2|S|$, and covering all the points in $\mathcal{X}(\mathbb{F}_q)$. However, in order to such points being bicovered, it seems that larger arcs are needed. As it turned out, a suitable choice is the union of some cosets of a subgroup K of $\mathcal{X}(\mathbb{F}_q)$, corresponding to a maximal 3-independent subset of the factor group $\mathcal{X}(\mathbb{F}_q)/K$.

2.4. Maximal 3-independent subsets of abelian groups

In this section we introduce the notion of a maximal 3-independent subset of an abelian group, which will be an essential tool to obtain complete and bicovering arcs contained in cubic curves.

Definition 2.18. Let $\mathcal{G}$ be an abelian group. A subset X of $\mathcal{G}$ is said to be *maximal 3-independent* if

(1) $x_1 + x_2 + x_3 \neq 0$ for all $x_1, x_2, x_3 \in X$;
(2) for any $y \in \mathcal{G} \setminus X$, there exist $x_1, x_2 \in X$ with $y + x_1 + x_2 = 0$. Furthermore, X is said to be *good* if $x_1 \neq x_2$ can be assumed.

We recall the following results from [**71, 78**].

Theorem 2.19 (Theorem 1 in [**71**]). *Let $\mathcal{G}$ be an elementary abelian p-group of order $q = p^r$, with $r \geq 2$ and p a prime greater than 3. Then there exists a maximal 3-independent subset X of $\mathcal{G}$ of size*

$$\begin{cases} 2p^{r/2} - 3 & \textit{if } r \textit{ is even,} \\ p^{\frac{r-1}{2}} + p^{\frac{r+1}{2}} - 3 & \textit{if } r \textit{ is odd;} \end{cases}$$

Proof. We distinguish two cases according to whether r is an even or odd integer.

- $r = 2n$, with $n \geq 1$;
  Let $q' = p^n$ and fix a basis of $\mathbb{F}_q$ as a linear space over $\mathbb{F}_{q'}$; then $\mathcal{G}$ is isomorphic to $\mathbb{F}_{q'} \times \mathbb{F}_{q'}$. For any $\gamma \in \mathbb{F}_{q'}$, $\gamma \neq 0$, put

  $$X_1 = \{(\gamma, \nu) \mid \nu \neq -2\gamma,\ \nu \in \mathbb{F}_{q'}\}$$
  $$X_2 = \{(\xi, \gamma) \mid \xi \neq -2\gamma,\ \xi \in \mathbb{F}_{q'}\}$$

  and consider $X = X_1 \cup X_2$. We shall prove that X is a maximal 3-independent subset of $\mathcal{G}$ up to isomorphisms.

  In order to verify (1) of Definition 2.18 it suffices to consider the following two cases:
  (1a) $x_1, x_2, x_3 \in X_1$,
  (1b) $x_1, x_2 \in X_1, x_3 \in X_2$,
  the proofs of the other cases being analogous. In the former case, if $x_i = (\gamma, \nu_i)$, for $i = 1, 2, 3$, then $x_1 + x_2 + x_3 = (3\gamma, \nu_1 + \nu_2 + \nu_3) \neq (0, 0)$ as $p > 3$ by assumption; in the latter case, if $x_i = (\gamma, \nu_i)$, for $i = 1, 2$ and $x_3 = (\xi_3, \gamma)$, then $x_1 + x_2 + x_3 = (2\gamma + \xi_3, \nu_1 + \nu_2 + \gamma) \neq (0, 0)$ as $\xi_3 \neq -2\gamma$.

  To prove (2) of Definition 2.18 we take $y = (\xi, \nu) \in \mathcal{G} \setminus X$ and consider the cases:
  (2a) $(\xi, \nu) = (-2\gamma, \gamma)$ or $(\xi, \nu) = (\gamma, -2\gamma)$,
  (2b) $\xi \neq \gamma \neq \nu$.
  In the former case, if $x_i = (\gamma, \nu_i)$, for $i = 1, 2$, then $y + x_1 + x_2 = (0, \gamma + \nu_1 + \nu_2) = (0, 0)$ if and only if the equation $-\gamma = \nu_1 + \nu_2$ admits a solution in $\mathbb{F}_q$ with $\nu_i \neq -2\gamma$, for $i = 1, 2$, but this is trivial for $q \geq 4$. In the latter case, if $x_1 = (-\gamma - \xi, \gamma)$ and $x_2 = (\gamma, -\gamma - \nu)$, then $y + x_1 + x_2 = (0, 0)$. Also, as $X_1 \cap X_2 = \{(\gamma, \gamma) \mid \gamma \in \mathbb{F}_{q'}\}$, then

  $$|X| = |X_1| + |X_2| - 1 = 2(p^n - 1) - 1 = 2p^n - 3$$

  and the assertion holds as $r = 2n$.
- $r = 2n + 1$, with $n \geq 1$;
  Let $q' = p^n$; in this case $\mathcal{G}$ is isomorphic to $\mathbb{F}_{q'} \times \mathbb{F}_{pq'}$. For any $\gamma_1 \in \mathbb{F}_{q'}$ and $\gamma_2 \in \mathbb{F}_{pq'}$, with $\gamma_i \neq 0$, for $i = 1, 2$, let

  $$X_1 = \{(\gamma_1, \nu) \mid \nu \neq -2\gamma_2, \nu \in \mathbb{F}_{pq'}\}$$

$$X_2 = \{(\xi, \gamma_2) \mid \xi \neq -2\gamma_1, \nu \in \mathbb{F}_{q'}\}$$

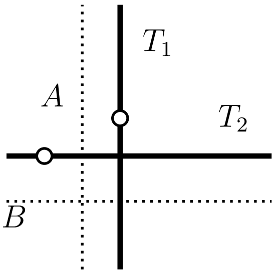
and consider $X = X_1 \cup X_2$. The proof of the first case shows that X satisfies the properties (1)–(2) of Definition 2.18 and $|X| \leq |X_1| + |X_2| - 1 = p^n + p^{n+1} - 3$ so the assertion on the size of X follows as $r = 2n + 1$. □

In a similar way, an explicit construction of good maximal 3-independent subsets was provided by Szőnyi, for direct products of abelian groups of order at least 4.

Theorem 2.20. [**68**, Example 1.2] *Let $\mathcal{G} = A \times B$ be an abelian group with A and B not-elementary 3-abelian. Choose two elements $a \in A$, $b \in B$ and consider the sets (see also Figure 1)*

$$T_1 = \{(a, x) \mid x \neq -2b,\ b \in B\}, \qquad T_2 = \{(y, b) \mid y \neq -2a,\ a \in A\}.$$

Figure 1. Maximal 3-independent subset in $\mathcal{G} = A \times B$



Then, the set $\overline{T} = T_1 \cup T_2$ is a maximal 3-independent subset of $\mathcal{G}$ of size $|A| + |B| - 3$.

Proposition 2.21 (Lemma 1 in [**78**]). *Let $f : \mathcal{G}_1 \to \mathcal{G}_2$ be a surjective homomorphism of finite abelian groups. Let X be a maximal 3-independent subset of $\mathcal{G}_2$. Then $f^{-1}(\mathcal{X})$ is a maximal 3-independent subset of $\mathcal{G}_1$. Also, if $|\mathcal{G}_1| \geq |\mathcal{G}_2| \cdot s(\mathcal{G}_1)$, where $s(\mathcal{G}_1) = \{x \in \mathcal{G}_1 \mid 2x = 0\}$, then $f^{-1}(X)$ is good.*

2.5. Some results on bicovering plane arcs from elliptic curves

To conclude this chapter, we recall some results about arcs in $AG(2, q)$, arising from elliptic curves.

In particular, arcs arising from cosets of the abelian group $G = (\mathcal{E}(\mathbb{F}_q), \oplus)$ of the set of $\mathbb{F}_q$-rational points of a non-singular cubic curve $\mathcal{E}$ defined over $\mathbb{F}_q$, were introduced by Voloch in [**78**], and were the main ingredient of some constructions of small complete arcs due to Szőnyi [**68, 69**]. Recently, Giulietti and Anbar deal with the investigation of the bicovering properties of such arcs (see [**3**]). Here we state some of their results, which will be relevant to our proofs.

Theorem 2.22. *Let $q = p^h$, with $p > 3$ and $G = \mathbb{Z}_m \times K$, for $m > 3$ a prime divisor of $q-1$, with $7 < m < \frac{1}{8}\sqrt[4]{q}$. Assume that the finite group of order m admits a maximal 3-independent subset of size s. Then there exists a bicovering k-arc in $AG(2,q)$ with*

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

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

It has been shown in [**78**] that if $m > 7$ is a prime, then there always exists a maximal 3-independent subset of size $s \leq (m+1)/3$ in the finite group of order m. Then, bicovering k- arcs in $AG(2,q)$ of size $k \leq q/3$ are obtained, under the assumptions of Theorem 2.22. Also, by applying Theorem 2.16 to the bicovering arcs of Theorem 2.22, small complete caps attaining the correspondent bound of Table 1 in the Preface, are obtained in affine spaces of dimension $N \equiv 0 \pmod 4$.

The following result is a consequence of Theorem 4 in [**3**].

Proposition 2.23. *Let S be a non-trivial coset of K in G defined as in Theorem 2.22, and let P be a point in S. Assume that the j-invariant of $\mathcal{E}$ is different from 0. If m divides $q-1$ and*

$$m \leq \frac{\sqrt[4]{q}}{8}, \tag{2.6}$$

then every point in $PG(2,q) \setminus \mathcal{E}(\mathbb{F}_q)$ is collinear with two points in $S \setminus \{P\}$.

Remark 2.24. *Arguing as in the proof of Theorem* 4 *in* [**3**], *condition* (2.6) *can be relaxed to $m \leq \frac{\sqrt[4]{q}}{4}$.*

Remark 2.25. *Proposition* 2.23 *was previously stated in* [**78**] *in a more general form. However, the proof given in* [**78**] *contains a gap which has not been filled yet; see* [**3**, Remark 4].

Also, for $q \leq 127$ some computational results were presented in [**23**].

Theorem 2.26. [**23**] *There exists a bicovering arc in $AG(2,q)$ of size n_q contained in an elliptic curve defined over $\mathbb{F}_q$, with (q, n_q) as follows:*

q	67	73	81	83	89	97	101	103	107	109	113	121	127
n_q	42	45	49	50	54	55	61	60	63	65	66	71	74

Also, there exists an almost bicovering arc in $AG(2,53)$ of size 34 *contained in an elliptic curve.*

CHAPTER 3

Small complete caps from singular cubics

Although the theory of complete arcs contained in plane cubic curves was well established in the late 80's, such structures are the base for some recent constructions of complete caps in higher dimension, which are the object of this chapter. Our constructions rely on the bicovering properties of certain plane arcs contained in cubic curves. In particular, we examine irreducible singular cubics with at least one rational inflection (see Section 1.4 for the classification). Section 3.1 is devoted to cubics with an $\mathbb{F}_q$-rational cusp, Section 3.2 is about cubics with an $\mathbb{F}_q$-rational node, and finally Section 3.3 deals with cubics with an isolated double point. Also, a construction by Szőnyi of complete arcs contained in cuspidal cubics [**71**] is generalized in the former section, while new complete plane arcs are obtained in the last section.

Throughout this chapter we assume that the characteristic of $\mathbb{F}_q$ is $p > 3$ and let $\mathbb{K}$ be the algebraic closure of $\mathbb{F}_q$. Let $\mathcal{X}$ be an irreducible singular plane cubic curve defined over $\mathbb{F}_q$ and let G be the set of its non-singular rational points. It is a classical result from algebraic geometry that it is possible to define a group law $\oplus$ on G in such a way that three distinct points in G are collinear if and only if their sum is the neutral element. This provides arcs contained in G in a rather easy way.

Proposition 3.1. *Let K be a subgroup of G of index m with $(3, m) = 1$, and let Q be a point in $G \setminus K$. Then the coset $S = K \oplus Q$ is an arc.*

Proof. By the previous assertion, three distinct points in S are collinear if and only if $3Q = 0$ in the factor group G/K, i.e. $3Q \in K$. Taking into account that $(3, m) = 1$, this implies $Q \in K$, a contradiction. □

In order to investigate the covering and the bicovering properties of S, a useful tool is the algebraic method due to Segre and Lombardo Radice (see Section 2.1), together with its generalization (see Section 2.3).

To apply the aforementioned methods, it would be useful to write the arc S in an algebraically parametrized form, where the rational functions describing the coordinates of the points of S are defined over $\mathbb{F}_q$; in fact, such methods require that the algebraic curves $\mathcal{C}_P$ and $\mathcal{Y}_{P,c}$ defined as in (2.2) and (2.5), to test if a point P off $\mathcal{X}$ is covered or bicovered by two points in S, are defined over $\mathbb{F}_q$. This can be easily done when $\mathcal{X}$ is a singular cubic with a cusp or with a node, by using explicit isomorphisms of the group $(G, \oplus)$ with $(\mathbb{F}_q, +)$ or $(\mathbb{F}_q^*, \cdot)$. Otherwise, when $\mathcal{X}$ is the cubic with an isolated double point, the standard parametrization of the points of S, arising from the natural isomorphism between $(G, \oplus)$ and the subgroup of order $q+1$ of the multiplicative group of $\mathbb{F}_{q^2}$, involves rational functions defined over $\mathbb{F}_{q^2}$ but not over $\mathbb{F}_q$. Consequently, a straightforward application of the methods is not possible in this case. A key point to overcome such a difficulty was to find a curve which is birationally equivalent to $\mathcal{C}_P$, but is defined over $\mathbb{F}_q$ (see Section 3.3.2).

Sections 3.1, 3.2 and 3.3 are organized as follows. The first paragraphs are devoted to the proofs of the absolute irreducibility of the algebraic curves $\mathcal{C}_P$ and $\mathcal{Y}_{P,c}$ (or at least of one of their component); then complete and bicovering plane arcs are obtained, by using the aforementioned methods in order to cover or bicover the points outside the cubics and by enlarging S in a proper way in order to cover or bicover also the points in $\mathcal{X}$. Finally, small complete caps are obtained by applying Theorem 2.16 to the bicovering and almost bicovering arcs of the previous sections.

3.1. Cuspidal case

3.1.1. A family of curves defined over $\mathbb{F}_q$. Throughout this section $q = p^h$ for some prime $p > 3$, and h' is an integer with $1 \leq h' < h$. Let M be an additive subgroup of $\mathbb{F}_q$ of order $\sigma = p^{h'}$; also, let

$$L_M(X) = \prod_{m \in M} (X - m) \in \mathbb{F}_q[X].$$

Then L_M is a linearized polynomial, that is, there exist $\beta_0, \ldots, \beta_{h'-1} \in \mathbb{F}_q$, with $\beta_0 \neq 0$, such that

$$L_M(X) = X^\sigma + \sum_{i=0}^{h'-1} \beta_i X^{p^i};$$

see for example [**47**, Theorem 3.52]. Let $\eta : \mathbb{F}_q \to \mathbb{F}_q$ be the additive homomorphism defined by $\eta(a) = L_M(a)$ for any $a \in \mathbb{F}_q$. Clearly, $\mathrm{Ker}(\eta)$ coincides with M, and $\mathrm{Im}(\eta)$ is an additive subgroup of $\mathbb{F}_q$ of index σ.

For $a, b \in \mathbb{F}_q$ with $a \neq b^3$, let $P = (b, a) \in AG(2, q)$ and let t be an element of $\mathbb{F}_q \setminus \mathrm{Im}(\eta)$. A crucial role for the investigation of the bicovering properties of a coset of index σ in the abelian group associated to a singular cuspidal cubic is played by the curve

$$\mathcal{C}_P : f_{a,b,t,M}(X, Y) = 0, \tag{3.1}$$

where

$$\begin{aligned} f_{a,b,t,M}(X,Y) \;=\; & a + (L_M(X)+t)(L_M(Y)+t)^2 + (L_M(X)+t)^2(L_M(Y)+t) + \\ & -b((L_M(X)+t)^2 + (L_M(X)+t)(L_M(Y)+t) + (L_M(Y)+t)^2). \end{aligned} \tag{3.2}$$

Denote by $M_{b,t}$ and $M'_{b,t}$ the sets of the roots of the polynomials $b - L_M(X) - t$ and $L_M(X) + 2t + b \in \mathbb{F}_q[X]$ respectively.

Remark 3.2. *As the formal derivatives of the polynomials $b - L_M(X) - t$ and $L_M(X) + 2t + b$ are equal to*

$$(b - L_M(X) - t)' = -\sigma x^{\sigma-1} - \sum_{i=1}^{h'-1} \beta_i p^i X^{p^i-1} - \beta_0 = -\beta_0 \neq 0,$$

$$(L_M(X) + 2t + b)' = \sigma x^{\sigma-1} + \sum_{i=1}^{h'-1} \beta_i p^i X^{p^i-1} + \beta_0 = \beta_0 \neq 0,$$

the sizes of $M_{b,t}$ and $M'_{b,t}$ are equal to σ.

Lemma 3.3. *The curve $\mathcal{C}_P$ satisfies the following properties:*

i) *the ideal points of $\mathcal{C}_P$ are the ideal points of the axes, together with the ideal point of the line $X + Y = 0$;*
ii) *the ideal points of $\mathcal{C}_P$ are ordinary singularities of $\mathcal{C}_P$ of multiplicity σ;*
iii) *the tangent lines at the ideal point X_∞ of the X-axis are the lines ℓ_d^X of equation $Y = d$, with $d \in M_{b,t}$; similarly, the tangent lines at the ideal point Y_∞ of the Y-axis are the lines ℓ_d^Y of equation $X = d$, with $d \in M_{b,t}$; also, the tangent lines at the ideal point R_∞ of the line $X + Y = 0$ are the lines ℓ_e^R of equation $X + Y = e$, with $e \in M'_{b,t}$;*
iv) *for each $d \in M_{b,t}$ and for each $e \in M'_{b,t}$, we have that*

$$I(X_\infty, \mathcal{C}_P \cap \ell_d^X) = I(Y_\infty, \mathcal{C}_P \cap \ell_d^Y) = I(R_\infty, \mathcal{C}_P \cap \ell_e^R) = 3\sigma.$$

Proof. The sum of the monomials of highest degree in $f_{a,b,t,M}(X,Y)$ is

$$X^\sigma Y^\sigma (X^\sigma + Y^\sigma) = X^\sigma Y^\sigma (X+Y)^\sigma,$$

which proves i) and that the multiplicity of each ideal point of $\mathcal{C}_P$ is at most σ.

Also, it is easily seen that the lines ℓ_d^X of affine equation $Y = d$, with $d \in M_{b,t}$ have no affine point in common with $\mathcal{C}_P$, thus they are the tangent lines to $\mathcal{C}_P$ at X_∞. In fact, by intersecting ℓ_d^X with $\mathcal{C}_P$ we get

$$\begin{aligned} f_{a,b,t,M}(X,d) &= a + (L_M(X)+t)b^2 + (L_M(X)+t)^2 b - (L_M(X)+t)^2 b + \\ &\quad -(L_M(X)+t)b^2 - b^3 = a - b^3, \end{aligned}$$

which is different from 0 by the previous assumptions on $a, b \in \mathbb{F}_q$. As $\mathcal{C}_P$ is left invariant by the transformation $X \mapsto Y$, $Y \mapsto X$, the lines ℓ_d^Y of affine equation $X = d$, with $d \in M_{b,t}$ are the tangent lines to $\mathcal{C}_P$ at Y_∞.

In a similar way it can be proved that the lines ℓ_e^R of affine equation $X + Y = e$, where $e \in M'_{b,t}$ are the tangent lines at R_∞; in fact, for $A(X) = L_M(X) + t$, we have

$L_M(e-X)+t=-A(X)-b$ and

$$f_{a,b,t,M}(X,e-X)=a+A(X)(A(X)+b)^2-A(X)^2(A(X)+b)+$$

$$-bA(X)^2+bA(X)(A(X)+b)-b(A(X)+b)^2=$$

$$=a+A(X)(A(X)+b)[(A(X)+b)-A(X)+b]-bA(X)^2-b(A(X)+b)^2=$$

$$=a+2bA(X)(A(X)+b)-bA(X)^2-b(A(X)+b)^2=$$

$$=a-b(A(X)-(A(X)+b))^2=a-b^3\neq 0,$$

by the previous assumptions on $a,b\in\mathbb{F}_q$. Therefore, iii) and iv) are proved and this, together with Remark 3.2, implies ii). □

The absolute irreducibility of the curve $\mathcal{C}_P$ is proved in the proposition below, by using Segre's irreducibility criterion (see Proposition 1.29). Also, an estimate of the genus of the curve is given.

Proposition 3.4 (Lemma 1 and Lemma 2 in [**71**]). *The curve $\mathcal{C}_P$ is absolutely irreducible of genus less than or equal to $3\sigma^2-3\sigma+1$.*

Proof. By Lemma 3.3, Segre's irreducibility criterion is met by $\mathcal{C}=\mathcal{C}_P$, $Q=X_\infty$ and a generic tangent line $\ell=\ell_d^X$ at X_∞. Thus $\mathcal{C}_P$ is an absolutely irreducible curve. Taking into account ii) of Lemma 3.3, the curve $\mathcal{C}_P$ has three distinct ordinary singularities of multiplicity σ. Then its virtual genus is at most

$$\frac{1}{2}(3\sigma-1)(3\sigma-2)-3\frac{1}{2}\sigma(\sigma-1)=3\sigma^2-3\sigma+1.$$

The assertion then follows, as the virtual genus is an upper bound for the actual genus of a plane curve (see Proposition 1.28). □

Now, let $\mathbb{K}(\mathcal{C}_P)$ be the function field of $\mathcal{C}_P$ (see Section 1.2) and let $\bar{x}$ and $\bar{y}$ denote the rational functions of $\mathbb{K}(\mathcal{C}_P)$ associated to the affine coordinates X and Y, respectively. Clearly $\mathbb{K}(\mathcal{C}_P)=\mathbb{K}(\bar{x},\bar{y})$ and $f_{a,b,t,M}(\bar{x},\bar{y})=0$ holds. By ii) of Lemma 3.3, there are precisely σ linear places of $\mathbb{K}(\bar{x},\bar{y})$ centered at each ideal point of $\mathcal{C}_P$.

Lemma 3.5. *Let $\gamma_1^X,\dots,\gamma_\sigma^X$ be the σ linear places of $\mathbb{K}(\bar{x},\bar{y})$ centered at X_∞ with tangents ℓ_d^X of equation $Y=d$, with $d\in M_{b,t}$. Then, for each $d\in M_{b,t}$, there is an index i_d such that*

$$v_{\gamma_{i_d}^X}(\bar{y}-d)=2\sigma,\quad v_{\gamma_{i_d}^X}(\bar{x}-d)=-1;$$

for any other $1\le i\le\sigma$, $i\neq i_d$

$$v_{\gamma_i^X}(\bar{y}-d)=0,\qquad v_{\gamma_i^X}(\bar{x}-d)=-1.$$

Proof. We keep the notation of Section 1.3. For the sake of simplicity, let $\gamma := \gamma_i^X$ be a linear place centered at X_∞ with tangent $\ell^X_{d_\gamma}$. Then for every $d \in M_{b,t}$

$$v_\gamma(\bar{y} - d_\gamma) + e_\gamma = j_2(\gamma), \tag{3.3}$$

$$v_\gamma(\bar{y} - d) + e_\gamma = 1, \text{ for } d \neq d_\gamma \tag{3.4}$$

$$v_\gamma(\bar{x} - d) + e_\gamma = 0, \tag{3.5}$$

hold. From here one can easily deduce that $v_\gamma(\bar{y} - d) = 0$. In fact, if $v_\gamma(\bar{y} - d) > 0$, then $v_\gamma(\bar{y} - d_\gamma) = 0$ and hence $e_\gamma = j_2(\gamma) > 1$ implies $v_\gamma(\bar{y} - d) < 0$ by (3.4), a contradiction; on the other hand, if $v_\gamma(\bar{y} - d) < 0$, then $v_\gamma(\bar{y} - d_\gamma) = v_\gamma(\bar{y} - d)$; hence $j_2(\gamma) = 1$ a contradiction. Consequently, from (3.4) it follows that $e_\gamma = 1$; then $v_\gamma(\bar{x} - d) = -1$ is obtained from (3.5). It follows that, for each $d \in M_{b,t}$, there is an index i_d such that for all $i \neq i_d$

$$v_{\gamma_i^X}(\bar{y} - d) = 0, \qquad v_{\gamma_i^X}(\bar{x} - d) = -1 \qquad v_{\gamma_{i_d}^X}(\bar{x} - d) = -1$$

hold. By Theorem 1.31, together with iv) of Proposition 3.3, we have that

$$\sum_{i=1}^{\sigma} v_{\gamma_i^X}(\bar{y} - d) + \sigma = 3\sigma,$$

which implies $v_{\gamma_{i_d}^X}(\bar{y} - d) = 2\sigma$ from the assertions above. □

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

Lemma 3.6. *Let $\gamma_1^Y, \ldots, \gamma_\sigma^Y$ be the σ linear places of $\mathbb{K}(\bar{x}, \bar{y})$ centered at Y_∞ with tangents ℓ_d^Y of equation $X = d$, with $d \in M_{b,t}$. Then, for each $d \in M_{b,t}$, there is an index j_d such that*

$$v_{\gamma_{j_d}^Y}(\bar{x} - d) = 2\sigma, \quad v_{\gamma_{j_d}^Y}(\bar{y} - d) = -1;$$

for any other $1 \leq j \leq \sigma$, $j \neq j_d$

$$v_{\gamma_j^Y}(\bar{x} - d) = 0, \qquad v_{\gamma_j^Y}(\bar{y} - d) = -1.$$

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

$$\mathcal{Y}_{P,c} : \begin{cases} f_{a,b,t,M}(X, Y) = 0 \\ c(b - L_M(X) - t)(b - L_M(Y) - t) = Z^2 \end{cases}. \tag{3.6}$$

The existence of a suitable $\mathbb{F}_q$-rational point of $\mathcal{Y}_{P,c}$ will guarantee that P is bicovered by the arc comprising the points of a coset of index σ in the abelian group of the non-singular $\mathbb{F}_q$-rational points of a cuspidal cubic; see Section 3.1.3. Here we prove the existence of an absolutely irreducible component of the curve $\mathcal{Y}_{P,c}$, in order to apply the Hasse–Weil bound to guarantee the existence of such a point.

The following lemma plays a key role in this section.

LEMMA 3.7. *For any non-zero element $c \in \mathbb{F}_q$, the rational function*

$$\alpha = c(b - L_M(\bar{x}) - t)(b - L_M(\bar{y}) - t)$$

is not a square in $\mathbb{K}(\bar{x}, \bar{y})$.

PROOF. By the definition of $M_{b,t}$, note that α can be written as

$$\alpha = c \prod_{d \in M_{b,t}} (\bar{x} - d)(\bar{y} - d).$$

Therefore, for any place γ_i^X centered at X_∞ we have

$$v_{\gamma_i^X}(\alpha) = \sum_{d \in M_{b,t}} \big(v_{\gamma_i^X}(\bar{y} - d) + v_{\gamma_i^X}(\bar{x} - d)\big) = 2\sigma + \sum_{d \in M_{b,t}} -1 = \sigma,$$

by Lemma 3.5. Similarly $v_{\gamma_i^Y}(\alpha) = \sigma$ holds for each $i = 1, \ldots, \sigma$ by Lemma 3.6. Note that σ is an odd integer, as $p > 3$ is assumed. This implies that α cannot be a square in $\mathbb{K}(\bar{x}, \bar{y})$, which proves the assertion. □

PROPOSITION 3.8. *Let $a, b \in \mathbb{F}_q$ be such that $a \neq b^3$. For each $c \in \mathbb{F}_q$, $c \neq 0$, the space curve $\mathcal{Y}_{P,c}$ has an irreducible component defined over $\mathbb{F}_q$ with genus less than or equal to $6\sigma^2 - 5\sigma + 1$.*

PROOF. The hypothesis of Corollary 1.26 are satisfied by the curve $\mathcal{C}_P$ and by the rational function α, defined as in Lemma 3.7. Consequently, $\omega^2 = \alpha$ defines a Kummer extension of $\mathbb{K}(\bar{x}, \bar{y})$ which is the function field of some irreducible curve. Such a curve is contained in $\mathcal{Y}_{P,c}$ as well, by Remark 1.27. Thus, the first part of the assertion is proved.

By iii) and iv) of Lemma 3.3, the only places of $\mathbb{K}(\bar{x}, \bar{y})$ that can be either a zero or a pole of α are those centered at ideal points of $\mathcal{C}_P$. If γ is a place centered at the ideal point of the line with equation $X + Y = 0$ then

$$v_\gamma(\alpha) = \sum_{d \in M_{b,t}} \big(v_\gamma(\bar{y} - d) + v_\gamma(\bar{x} - d)\big) = -2\sigma.$$

On the other hand, in the proof of Lemma 3.7 it is shown that the valuation of α at any place centered at X_∞ or Y_∞ is equal to σ. Therefore, the number of places of $\mathbb{K}(\bar{x}, \bar{y})$ such that the valuation of α is odd is equal to 2σ. Then the assertion on the genus follows from Corollary 1.26 together with Proposition 3.4. □

3.1.2. A generalization of Szőnyi's construction of complete plane arcs. If $\mathcal{X}$ is singular with a cusp, we can assume that the affine equation of $\mathcal{X}$ is $Y = X^3$, (see Proposition 1.32 in Section 1.4). As $Y_\infty = (0, 1, 0)$ is the singular point of $\mathcal{X}$, the group G coincides with the set of the $\mathbb{F}_q$-rational affine points of $\mathcal{X}$. If the neutral element of G is chosen to be the affine point $(0, 0)$, then the group G is isomorphic to $\mathbb{F}_q$ via the map $\phi : (\mathbb{F}_q, +) \to (G, \oplus), \phi(v) = (v, v^3)$.

REMARK 3.9. *It is easy to see that three distinct points (v_i, v_i^3) in G, $(i = 1, 2, 3)$ are collinear if and only if the sum $v_1 + v_2 + v_3$ of their first coordinates v_i is equal to zero. In fact, by imposing the collinearity condition*

$$\det \begin{pmatrix} v_1 & v_1^3 & 1 \\ v_2 & v_2^3 & 1 \\ v_3 & v_3^3 & 1 \end{pmatrix} = 0,$$

this is equivalent to

$$(v_1 - v_2)[-v_3^3 + v_3(v_1^2 + v_1v_2 + v_2^2) - v_1v_2(v_1 + v_2)] = 0.$$

After some computation and as $v_i \neq v_j$ for $i, j = 1, 2, 3$, $i \neq j$, we get

$$(v_1 + v_2 + v_3)[v_3(v_1 + v_2 - v_3) - v_1v_2] = 0$$

and the required condition is proven.

Let η be defined as in Section 3.1.1, then $\mathrm{Im}(\eta)$ is an additive subgroup of $\mathbb{F}_q$ of index σ. Let $K = \{(v, v^3) \mid v \in \mathrm{Im}(\eta)\}$ be the corresponding subgroup of G and let $Q = (t, t^3)$ be a point in $G \setminus K$. Then the coset of K in G, defined as

$$K_t = K \oplus Q = \{(v, v^3) \mid v \in \mathrm{Im}(\eta) + t\}, \tag{3.7}$$

or equivalently

$$K_t = \{(L_M(x) + t, (L_M(x) + t)^3) \mid x \in \mathbb{F}_q\}, \tag{3.8}$$

is an arc by Proposition 3.1.

For a point $P = (b, a)$ in $AG(2, q) \setminus \mathcal{X}$, let $f_{a,b,t,M}(X, Y)$ be as in (3.2).

Arguing as in the proof of [**71**, Lemma 3 and Theorem 2], the following results can be easily obtained.

PROPOSITION 3.10. *The point P is collinear with two distinct points in K_t if and only if there exist $x, y \in \mathbb{F}_q$ with $L_M(x) \neq L_M(y)$ such that $f_{a,b,t,M}(x, y) = 0$.*

PROOF. Two distinct points $P_1 = (v_1, v_1^3)$, $P_2 = (v_2, v_2^3)$ in $\mathcal{X}$ are collinear with P if and only if

$$\det \begin{pmatrix} v_1 & v_1^3 & 1 \\ v_2 & v_2^3 & 1 \\ b & a & 1 \end{pmatrix} = 0.$$

Then, as $P_1 \neq P_2$ and

$$\det\begin{pmatrix} v_1 & v_1^3 & 1 \\ v_2 & v_2^3 & 1 \\ b & a & 1 \end{pmatrix} = (v_1v_2^3 - v_2v_1^3) - a(v_1 - v_2) + b(v_1^3 - v_2^3) =$$

$$= (v_1 - v_2)[-a + b(v_1^2 + v_1v_2 + v_2^2) - v_1v_2(v_2 + v_1)],$$

the collinearity condition is equivalent to

$$-a + b(v_1^2 + v_1v_2 + v_2^2) - v_1v_2(v_2 + v_1) = 0. \tag{3.9}$$

When P_1, P_2 are elements of K_t, both $v_1 = L_M(x) + t$ and $v_2 = L_M(y) + t$ hold for some $x, y \in \mathbb{F}_q$, by (3.8). Then the assertion follows, as (3.9) is exactly $f_{a,b,t,M}(x, y) = 0$. □

Proposition 3.11. *If*

$$q + 1 - (6\sigma^2 - 6\sigma + 2)\sqrt{q} \geq 3\sigma^2 + 3\sigma + 1, \tag{3.10}$$

then P is collinear with two distinct points of K_t.

Proof. Let $\mathbb{K}(\bar{x}, \bar{y})$ be the function field of $\mathcal{C}_P$, so that $f_{a,b,t,M}(\bar{x}, \bar{y}) = 0$ holds. Let E be the set of places γ of $\mathbb{K}(\bar{x}, \bar{y})$ for which at least one of the following holds:

(1) γ is a pole of either $\bar{x}$ or $\bar{y}$;
(2) $L_M(\bar{x})(\gamma) = L_M(\bar{y})(\gamma)$.

We are going to show that the size of E is at most $3\sigma^2 + 3\sigma$. Poles of $\bar{x}$ or $\bar{y}$ in $\mathbb{K}(\bar{x}, \bar{y})$ are places centered at ideal points of $\mathcal{C}_P$. By Bézout's Theorem their number is at most 3σ. Also, it is easily seen that the number of places of $\mathbb{K}(\bar{x}, \bar{y})$ such that (2) holds is $3\sigma^2$. Our assumption on q and σ, together with the Hasse–Weil bound, ensures the existence of at least $3\sigma^2 + 3\sigma + 1$ $\mathbb{F}_q$-rational places of $\mathbb{K}(\bar{x}, \bar{y})$; hence, there exists at least one $\mathbb{F}_q$-rational place γ of $\mathbb{K}(\bar{x}, \bar{y})$ not in E. Let

$$x = \bar{x}(\gamma), \quad y = \bar{y}(\gamma).$$

be the images of $\bar{x}$ and $\bar{y}$ by the residue class map with respect to γ (see Definition 1.11 in Section 1.1). Note that (x, y) is an $\mathbb{F}_q$-rational affine point of the curve $\mathcal{C}_P$. Therefore, by Proposition 3.10, P is collinear with two distinct points

$$P_1 = (L_M(x) + t, (L_M(x) + t)^3),\ P_2 = (L_M(y) + t, (L_M(y) + t)^3) \in K_t.$$

This proves the assertion. □

In order to cover the points on $\mathcal{X}$, union of distinct cosets need to be considered. By applying the construction of Theorem 2.19 to the additive subgroup $\mathbb{F}_q/\mathrm{Im}(\eta)$ of $(\mathbb{F}_q, +)$ of order σ, the following extension of Theorem 3 in [**71**] can be obtained. Note that (3.10) holds when

$$\sqrt{q} \geq 3\sigma^2 - 3\sigma + 1 + \sqrt{9\sigma^4 - 18\sigma^3 + 18\sigma^2 - 3\sigma + 1},$$

which is implied by $q \geq 36\sigma^4$.

THEOREM 3.12. *Let $q = p^h$ with $p > 3$ a prime. For an integer h' with $1 < h' < h$, let $\sigma = p^{h'}$ and let $\mathbb{F}_q/\mathrm{Im}(\eta)$ be the additive subgroup of $\mathbb{F}_q$ of order σ. Assume that $q \geq 36\sigma^4$ and let T be a maximal 3-independent subset of $\mathbb{F}_q/\mathrm{Im}(\eta)$. Then*

$$A = \bigcup_{t \in T} K_t$$

is a complete k-arc in $AG(2,q)$ with

$$k = \begin{cases} (2\sqrt{\sigma} - 3)\dfrac{q}{\sigma}, & \text{if } h' \text{ is even,} \\ \\ (\sqrt{\sigma/p} + \sqrt{\sigma p} - 3)\dfrac{q}{\sigma}, & \text{if } h' \text{ is odd.} \end{cases}$$

PROOF. As $\mathbb{F}_q/\mathrm{Im}(\eta)$ is isomorphic to G/K, by applying Proposition 2.21 to the canonical projection $\pi : G \to G/K$, the set A is a good maximal 3-indipendent subset of G. Taking into account Definition 2.18 and Remark 3.9, stating that three distinct points $(v_i, v_i^3, 1)$ in G, $(i = 1, 2, 3)$ are collinear if and only if the sum $v_1 + v_2 + v_3$ of their first coordinates v_i is equal to zero, the set A is an arc by (1) of Definition 2.18. Also, A is complete, as it covers all the points in $G \setminus A$ by (2) of Definition 2.18 and the points off $\mathcal{X}$ are covered too, as (3.10) in Proposition 3.11 holds for $q \geq 36\sigma^4$. The assertions on the cardinality of A directly follow from Theorem 2.19 and $|K_t| = |\mathrm{Im}(\eta)| = q/\sigma$. □

COROLLARY 3.13. *Let $q = p^h$ with $p > 3$ a prime and $h > 8$. Let v_h be the integer in $\{1, \ldots, 8\}$ such that $v_h \equiv h \pmod 8$, and let t_h be the integer in $\{1, \ldots, 4\}$ such that $t_h \equiv h \pmod 4$. Assume that $p^{t_h} > 36$. Then there exists a complete k-arc in $AG(2,q)$ with*

$$k < 2p^{h - \lfloor (\lceil h/4 \rceil - 1)/2 \rfloor} \leq 2p^{\frac{v_h}{8}} q^{7/8} \leq 2pq^{7/8}.$$

PROOF. Let $h' = \left\lceil \frac{h}{4} \right\rceil - 1$, and let $\sigma = p^{h'}$. Note that $h > 8$ implies $h' > 1$, and that $t_h = 4 - 4\lceil h/4 \rceil + h$ holds for any positive integer h. Therefore, $p^{4 - 4\lceil h/4 \rceil + h} > 36$. Whence, $q = p^h > 36p^{4(\lceil h/4 \rceil - 1)} = 36\sigma^4$. By Theorem 3.12, there exists a complete k-arc in $AG(2,q)$ with

$$k = \begin{cases} \left(2p^{\frac{1}{2}(\left\lceil \frac{h}{4} \right\rceil - 1)} - 3\right)p^{h - \left\lceil \frac{h}{4} \right\rceil + 1}, & \text{if } \left\lceil \frac{h}{4} \right\rceil - 1 \text{ is even,} \\ \\ \left(p^{\frac{1}{2}(\left\lceil \frac{h}{4} \right\rceil - 2)} + p^{\frac{1}{2}\left\lceil \frac{h}{4} \right\rceil} - 3\right)p^{h - \left\lceil \frac{h}{4} \right\rceil + 1}, & \text{if } \left\lceil \frac{h}{4} \right\rceil - 1 \text{ is odd.} \end{cases}$$

Note that $k < 2p^{h - \lfloor (\lceil h/4 \rceil - 1)/2 \rfloor}$ holds. It is easily seen by straightforward computation that $p^{h - \lfloor (\lceil h/4 \rceil - 1)/2 \rfloor} \leq p^{\frac{7}{8}h + \frac{v_h}{8}}$, whence the assertion. □

3.1.3. Bicovering arcs from cuspidal cubics. As in Section 3.1.2, let $\mathcal{X}$ be the singular cubic with a cusp, having canonical equation $Y = X^3$. Let K_t denote the arc defined by (3.7) for t in $\mathbb{F}_q \setminus \mathrm{Im}(\eta)$. In order to prove that any point $P = (b, a) \in AG(2, q) \setminus \mathcal{X}$ is bicovered by K_t, it is necessary to require the existence of an $\mathbb{F}_q$-rational affine point $(\tilde{x}, \tilde{y}, \tilde{z})$ of the curve $\mathcal{Y}_{P,c}$ defined as in (3.6) such that $L_M(\tilde{x}) \neq L_M(\tilde{y})$; then, taking into account Proposition 3.10, by $f_{a,b,t,M}(\tilde{x}, \tilde{y}) = 0$ the point P is collinear with

$$P_{1,c} = (L_M(\tilde{x}) + t, (L_M(\tilde{x}) + t)^3),\ P_{2,c} = (L_M(\tilde{y}) + t, (L_M(\tilde{y}) + t)^3) \in K_t.$$

Also, if c is a square in $\mathbb{F}_q$, 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 $P_{1,c}P_{2,c}$.

Proposition 3.14. *If*

$$q + 1 - 2(6\sigma^2 - 5\sigma + 1)\sqrt{q} \geq 6\sigma^2 + 6\sigma + 1, \tag{3.11}$$

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

Proof. Fix a non-zero element c in $\mathbb{F}_q$ and let $\mathcal{Y}_{P,c}$ be as in (3.6). Let $\mathbb{K}(\mathcal{C}_P)(\bar{z}) = \mathbb{K}(\bar{x}, \bar{y}, \bar{z})$ be the function field of $\mathcal{Y}_{P,c}$, so that

$$\begin{cases} f_{a,b,t,M}(\bar{x}, \bar{y}) = 0 \\ c(b - L_M(\bar{x}) - t)(b - L_M(\bar{y}) - t) = \bar{z}^2 \end{cases}. \tag{3.12}$$

Let E be the set of places γ of $\mathbb{K}(\bar{x}, \bar{y}, \bar{z})$ for which at least one of the following holds:

(1) γ is a pole of either $\bar{x}$ or $\bar{y}$;
(2) $L_M(\bar{x})(\gamma) = L_M(\bar{y})(\gamma)$;
(3) γ is either a zero or a pole of $\bar{z}$.

We are going to show that the size of E is at most $6(\sigma^2 + \sigma)$. This follows from the proof of Proposition 3.11 together with the fact that $\mathbb{K}(\bar{x}, \bar{y}, \bar{z})$ is a double cover of $\mathbb{K}(\bar{x}, \bar{y})$. Also, note that zeros and poles of $\bar{z}$ are places of $\mathbb{K}(\bar{x}, \bar{y}, \bar{z})$ lying over zeros and poles of $\alpha = c(b - L_M(\bar{x}) - t)(b - L_M(\bar{y}) - t)$ in $\mathbb{K}(\bar{x}, \bar{y})$. By the proof of Proposition 3.8, zeros and poles of α are places centered at ideal points of $\mathcal{C}_P$. These places have already been considered in (1).

Our assumption on q and σ, together with the Hasse–Weil bound, ensures the existence of at least $6\sigma^2 + 6\sigma + 1$ $\mathbb{F}_q$-rational places of $\mathbb{K}(\bar{x}, \bar{y}, \bar{z})$; hence, there exists at least one $\mathbb{F}_q$-rational place γ_c of $\mathbb{K}(\bar{x}, \bar{y}, \bar{z})$ not in E. Let

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

be the image of $\bar{x}$, $\bar{y}$, and $\bar{z}$ by the residue class map with respect to γ_c (see Definition 1.11 in Section 1.1). As (3.12) holds in $\mathbb{K}(\bar{x}, \bar{y}, \bar{z})$, the point $P_c = (\tilde{x}, \tilde{y}, \tilde{z})$ is an affine point of $\mathcal{Y}_{P,c}$. Therefore, by Proposition 3.10, P is collinear with two distinct points

$$P_{1,c} = (L_M(\tilde{x}) + t, (L_M(\tilde{x}) + t)^3),\ P_{2,c} = (L_M(\tilde{y}) + t, (L_M(\tilde{y}) + t)^3) \in K_t.$$

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 $\sigma > 2$ the coset K_t cannot bicover all the $\mathbb{F}_q$-rational affine points in $\mathcal{X}$. Therefore, the union A of distinct cosets of K as defined in Theorem 3.12 need to be considered.

REMARK 3.15. *Let t_1 and t_2 be two distinct elements in $\mathbb{F}_q$. If P_1, P_2, P_3 are collinear points in $\mathcal{X}$ with $P_1 \in K_{t_1}$ and $P_2 \in K_{t_2}$, then $P_3 \in K_{-(t_1+t_2)}$.*

PROOF. Let $P_i = (u_i, u_i^3)$, $i = 1, 2, 3$ be distinct affine points of $\mathcal{X}$. Recall that collinearity of P_1, P_2, P_3 is equivalent to $u_1 + u_2 + u_3 = 0$. If $P_1 \in K_{t_1}$ and $P_2 \in K_{t_2}$, then $u_1 = L_M(x_1) + t_1$ and $u_2 = L_M(x_2) + t_2$ for some $x_1, x_2 \in \mathbb{F}_q$. Therefore,

$$u_3 = -u_1 - u_2 = L_M(-(x_1 + x_2)) - (t_1 + t_2),$$

which shows that $P_3 \in K_{-(t_1+t_2)}$. □

PROPOSITION 3.16. *Let K_{t_1}, K_{t_2} be cosets of K such that $K_{t_1} \cup K_{t_2}$ is an arc. Let P_0 be an $\mathbb{F}_q$-rational affine point of $\mathcal{X} \setminus \{(0,0)\}$ not belonging to $K_{t_1} \cup K_{t_2}$ but collinear with a point of K_{t_1} and a point of K_{t_2}. If* (3.11) *holds, then P_0 is bicovered by $K_{t_1} \cup K_{t_2}$.*

PROOF. Let $P_0 = (u_0, u_0^3)$ be a point of $\mathcal{X} \setminus A$ with $u_0 \neq 0$, and let $t \in \mathbb{F}_q$ be such that $P_0 \in K_t$. By Theorem 3.12 there exist $t_1, t_2 \in T$ such that P_0 is collinear with $P_1 \in K_{t_1}$ and $P_2 \in K_{t_2}$. Note that Remark 3.15 yields that for each point $P_1 = (v, v^3) \in K_{t_1}$, the point $P_2 = (-u_0 - v, (-u_0 - v)^3)$ must belong to K_{t_2}, where $t_2 = -(t_1 + t)$, since P_2 is a point of $\mathcal{X}$ collinear with P_0 and P_1. We are going to show that P_0 is bicovered by $K_{t_1} \cup K_{t_2}$. That is, P_0 is external to P_1P_2 for some choice of v, and internal to P_1P_2 for some other. Let S be the set of non-zero squares in $\mathbb{F}_q$ and N be the set of non-squares in $\mathbb{F}_q$. We need to prove the existence of an element $v \in \mathbb{F}_q$, $v = L_M(x) + t_1$ for some $x \in \mathbb{F}_q$, such that

$$(u_0 - v)(u_0 - (-u_0 - v)) = (u_0 - v)(2u_0 + v) \in S,$$

and of an element $\tilde{v} \in \mathbb{F}_q$, $\tilde{v} = L_M(\tilde{x}) + t_1$ for some $\tilde{x} \in \mathbb{F}_q$, such that

$$(u_0 - \tilde{v})(u_0 - (-u_0 - \tilde{v})) = (u_0 - \tilde{v})(2u_0 + \tilde{v}) \in N.$$

Let $\bar{x}$ be a trascendental element over $\mathbb{K}$. To this end, for a non-zero element c in $\mathbb{F}_q$ we need to investigate whether the following rational function

$$\beta(\bar{x}) = \frac{1}{c}(u_0 - L_M(\bar{x}) - t_1)(2u_0 + L_M(\bar{x}) + t_1)$$

is a non-square in $\mathbb{K}(\bar{x})$. Let a be a root of $2u_0 + L_M(X) + t_1$ in $\mathbb{K}$. Let γ_a be the only place of $\mathbb{K}(\bar{x})$ such that $\bar{x}(\gamma_a) = a$. As $2u_0 + L_M(X) + t_1$ is a separable polynomial, we have $v_{\gamma_a}(2u_0 + L_M(\bar{x}) + t_1) = 1$. Also, $u_0 \neq 0$, together with $p > 3$, implies that γ_a is not a zero nor a pole of $(u_0 - L_M(\bar{x}) - t_1)$. Then $v_{\gamma_a}(\beta(\bar{x})) = 1$. This proves that $\beta(\bar{x})$ is not a square in $\mathbb{K}(\bar{x})$. Then Proposition 1.26 applies to $c\beta(\bar{x})$ for each $c \in \mathbb{F}_q$. By the argument above it is easy to deduce that $v_\gamma(\beta(\bar{x})) = 1$ for any place γ such that $\bar{x}(\gamma)$ is a root of $(u_0 - L_M(X) - t_1)(L_M(X) + t_1)$. The valuation of $\beta(\bar{x})$ at the only pole of $\bar{x}$ in $\mathbb{K}(\bar{x})$ is 2σ. For any other place of $\mathbb{K}(\bar{x})$, the valuation of $\beta(\bar{x})$ is equal to 0. Then the genus of the Kummer extension $\mathbb{K}(\bar{x}, \bar{z})$ of $\mathbb{K}(\bar{x})$ with $\bar{z}^2 = c\beta(\bar{x})$ is $\sigma - 1$.

Our assumption on q, together with the Hasse–Weil bound, yield the existence of an $\mathbb{F}_q$-rational place γ_c of $\mathbb{K}(\bar{x}, \bar{z})$ which is not a zero nor a pole of $\bar{z}$. Let $\tilde{x} = \bar{x}(\gamma_c)$, $\tilde{z} = \bar{z}(\gamma_c)$. Therefore, P_0 is collinear with two distinct points

$$P_{1,c} = (L_M(\tilde{x}) + t_1, (L_M(\tilde{x}) + t_1)^3) \in K_{t_1}$$

and

$$P_{2,c} = (-u_0 - L_M(\tilde{x}) - t_1, (-u_0 - L_M(\tilde{x}) - t_1)^3) \in K_{t_2}.$$

If c is chosen to be a square, then P_0 is external to $P_{1,c}P_{2,c}$; on the other hand, if c is not a square, then P_0 is internal to $P_{1,c}P_{2,c}$. □

Remark 3.17. *The point $(0, 0)$ is either external or internal to all the secants of $K_{t_1} \cup K_{t_2}$ containing it, according to whether $q \equiv 1 \pmod 4$ or $q \equiv 3 \pmod 4$.*

Proof. If $P_0 = (0, 0)$, then for any v we have that $(u_0 - v)(u_0 - (-u_0 - v)) = -v^2$ belongs to S if -1 is a square in $\mathbb{F}_q$, and is an element of N if -1 is not a square in $\mathbb{F}_q$. By the discussion in the proof of Proposition 3.16, it follows that the point $(0, 0)$ is either external or internal to all the secants of A containing it, according to whether $q \equiv 1 \pmod 4$ or $q \equiv 3 \pmod 4$. □

Now, it is easy to deduce that the complete arcs constructed in Section 3.1.2 are almost bicovering, provided that (3.11) holds, which is clearly implied by $q \geq 144\sigma^4$.

Theorem 3.18. *Let $q = p^h$ with $p > 3$ a prime. For an integer h' with $1 < h' < h$, let $\sigma = p^{h'}$ and let $\mathbb{F}_q/\mathrm{Im}(\eta)$ be the additive subgroup of $\mathbb{F}_q$ of order σ. Assume that $q \geq 144\sigma^4$ and let T be a maximal 3-independent subset of $\mathbb{F}_q/\mathrm{Im}(\eta)$. Then*

$$A = \bigcup_{K_t \in T} K_t$$

is an almost bicovering k-arc in $AG(2, q)$ with

$$k = \begin{cases} (2\sqrt{\sigma} - 3)\dfrac{q}{\sigma}, & \text{if } h' \text{ is even,} \\ \\ (\sqrt{\sigma/p} + \sqrt{\sigma p} - 3)\dfrac{q}{\sigma}, & \text{if } h' \text{ is odd.} \end{cases}$$

The center of A is $Q = (0, 0)$, which is either external or internal to all the secants of A containing it, according to whether $q \equiv 1 \pmod 4$ or $q \equiv 3 \pmod 4$.

PROOF. The set A is a complete arc in $AG(2,q)$ of size k by Theorem 3.12. Proposition 3.14 yields that any point off $\mathcal{X}$ is bicovered by A. The assertion for the points on $\mathcal{X}$ follows from Proposition 3.16 and Remark 3.17. □

An analogous result to that of Corollary 3.13 holds.

COROLLARY 3.19. *Let $q = p^h$ with $p > 3$ a prime and $h > 8$. Let v_h be the integer in $\{1, \dots, 8\}$ such that $v_h \equiv h \pmod 8$, and let t_h be the integer in $\{1, \dots, 4\}$ such that $t_h \equiv h \pmod 4$. Assume that $p^{t_h} > 144$. Then there exists an almost bicovering k-arc in $AG(2,q)$ with*

$$k < 2p^{h-\lfloor(\lceil h/4\rceil-1)/2\rfloor} \leq 2p^{\frac{v_h}{8}}q^{7/8} \leq 2pq^{7/8}.$$

PROOF. Let $h' = \left\lceil \frac{h}{4} \right\rceil - 1$, and let $\sigma = p^{h'}$. Note that $h' > 1$, and that $t_h = 4 - 4\lceil h/4\rceil + h$. Therefore, $p^{4-4\lceil h/4\rceil+h} > 144$ holds. Whence,

$$q = p^h > 144p^{4(\lceil h/4\rceil-1)} = 144\sigma^4.$$

By Theorem 3.18, there exists an almost bicovering k-arc in $AG(2,q)$ with

$$k = \begin{cases} \left(2p^{\frac{1}{2}(\left\lceil \frac{h}{4}\right\rceil-1)} - 3\right)p^{h-\left\lceil\frac{h}{4}\right\rceil+1}, & \text{if } \left\lceil \frac{h}{4}\right\rceil - 1 \text{ is even,} \\ \\ \left(p^{\frac{1}{2}(\left\lceil \frac{h}{4}\right\rceil-2)} + p^{\frac{1}{2}\left\lceil \frac{h}{4}\right\rceil} - 3\right)p^{h-\left\lceil\frac{h}{4}\right\rceil+1}, & \text{if } \left\lceil \frac{h}{4}\right\rceil - 1 \text{ is odd.} \end{cases}$$

Note that $k < 2p^{h-\lfloor(\lceil h/4\rceil-1)/2\rfloor}$ holds. It is easily seen by straightforward computation that $p^{h-\lfloor(\lceil h/4\rceil-1)/2\rfloor} \leq p^{\frac{7}{8}h+\frac{v_h}{8}}$, whence the assertion. □

3.1.4. Small complete caps from cuspidal cubics. We use Corollary 3.19, together with Theorem 2.16 in Section 2.3 in order to construct small complete caps in affine Galois spaces $AG(N,q)$, where $N \equiv 0 \pmod 4$. The following theorem holds.

THEOREM 3.20. *Let $q = p^h$ with $p > 3$ a prime, $h > 8$. Let v_h be the integer in $\{1, \dots, 8\}$ such that $v_h \equiv h \pmod 8$, and let t_h be the integer in $\{1, \dots, 4\}$ such that $t_h \equiv h \pmod 4$. Assume that $p^{t_h} > 144$. Then there exists a complete k-cap in $AG(N,q)$ with*

$$k < \left(2p^{h-\lfloor(\lceil h/4\rceil-1)/2\rfloor}\right)q^{\frac{N-2}{2}} \leq 2p^{\frac{v_h}{8}}q^{\frac{N}{2}-\frac{1}{8}} \leq 2pq^{\frac{N}{2}-\frac{1}{8}}. \tag{3.13}$$

PROOF. Let $q' = q^{(N-2)/2}$ and let A be as in Theorem 3.18. If $q \equiv 1 \pmod 4$, then by Proposition 2.16, together with Theorem 3.18, the set

$$C = C_A \cup \{(\alpha, \alpha^2 - c, x_0, y_0) \mid \alpha \in \mathbb{F}_{q'}\}$$

defined as in Theorem 2.16 is a complete cap in $AG(N,q)$. If $q \equiv 3 \pmod 4$, the same holds for

$$C = C_A \cup \{(\alpha, \alpha^2 - c^2, x_0, y_0) \mid \alpha \in \mathbb{F}_{q'}\}$$

Note that the size of C is less than $2p^{h-\lfloor(\lceil h/4\rceil-1)/2\rfloor}q^{(N-2)/2}$, by Corollary 3.19. Also, $p^{h-\lfloor(\lceil h/4\rceil-1)/2\rfloor} \leq p^{\frac{7}{8}h+\frac{v_h}{8}}$ holds. Whence, (3.13) follows. □

3.2. Nodal case

3.2.1. A family of curves defined over $\mathbb{F}_q$. Throughout this section $q = p^h$ for some prime $p > 3$, and m is a proper divisor of $q-1$ with $(m, 6) = 1$. Also, 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

$$\mathcal{C}_P : f_{a,b,t,m}(X, Y) = 0, \tag{3.14}$$

where

$$\begin{aligned} f_{a,b,t,m}(X,Y) &= a(t^3X^{2m}Y^m + t^3X^mY^{2m} - 3t^2X^mY^m + 1) \\ &\quad -bt^2X^mY^m - t^4X^{2m}Y^{2m} + 3t^2X^mY^m - tX^m - tY^m. \end{aligned} \tag{3.15}$$

In [**68, 69**] 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 (see Proposition 1.29) 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.

3.2.1.1. *$a^3 = -1$ 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 [**24**]). As proved in [**24**], such component is absolutely irreducible with genus less than m^2.

Proposition 3.21. *Assume that $a^3 = -1$ and $b = 1-(a-1)^3$. Then the curve $\mathcal{C}_P$ has an irreducible $\mathbb{F}_q$-rational component of genus less than m^2, with equation $a^2 + t^2X^mY^m - atX^m = 0$.*

3.2.1.2. *$a \neq 0$ and either $a^3 \neq -1$ or $b \neq 1-(a-1)^3$.*

Lemma 3.22. *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. A plane quartic curve can admit irreducible components defined over $\mathbb{F}_q$ having at most degree 2. Here we prove that this cannot happen, thus the assertion. 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_∞.
It is straightforward to check that none of such lines is a component of $\mathcal{Q}_P$, as neither $X - a/t$ and $Y - a/t$ nor X and Y divide $g_P(X, Y)$. In fact, $X - a/t$ divides $g_P(X, Y)$ if and only if $g_P(a/t, Y) = 0$ and

$$g_P(a/t, Y) = a(ta^2Y + t^2aY^2 - 3taY + 1) - btaY - t^2a^2Y^2 + 3taY - a - tY =$$

$$= tY(a^3 - 1) - 3taY(a - 1) - btaY = tY(a - 1)[(a^2 + a + 1) - 3a] - btaY =$$

$$= tY(a - 1)^3 - tYab \neq 0,$$

as $ab \neq (a - 1)^3$ by assumptions. As $\mathcal{Q}_P$ is left invariant by the transformation $X \mapsto Y$, $Y \mapsto X$, also $Y - a/t$ does not divide $g_P(X, Y)$. Neither X nor Y divide $g_P(X, Y)$, as it is not possible that $g_P(0, Y) = a - tY$ and $g_P(X, 0) = a - tX$ are components of $g_P(X, Y)$ by the previous assertions. 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 $\mathcal{C}_1 : X\left(Y - \frac{a}{t}\right) + \epsilon = 0$ and $\mathcal{C}_2 : \left(X - \frac{a}{t}\right)Y + \bar{\epsilon} = 0$ for some $\epsilon, \bar{\epsilon}, \rho \in \mathbb{K}^*$. So

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

By comparing coefficients we have

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

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

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. Clearly $\mathbb{K}(\mathcal{Q}_P) = \mathbb{K}(\bar u, \bar z)$ and $g_P(\bar u, \bar z) = 0$ holds in $\mathbb{K}(\bar u, \bar z)$, that is

$$a(t^3\bar u^2\bar z + t^3\bar u\bar z^2 - 3t^2\bar u\bar z + 1) - bt^2\bar u\bar z - t^4\bar u^2\bar z^2 + 3t^2\bar u\bar z - t\bar u - t\bar z = 0. \tag{3.16}$$

By the proof of Lemma 3.22 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 3.23. *Let γ_1 be the linear place of $\mathbb{K}(\bar u, \bar z)$ centered at X_∞ with tangent $Y = a/t$, and let γ_2 be 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 1.3. Here, the role of $\bar x$ and $\bar y$ is played by $\bar u$ and $\bar z$, respectively. Then

$$v_{\gamma_1}(\bar z - a/t) + e_{\gamma_1} = j_2(\gamma_1), \tag{3.17}$$

$$v_{\gamma_1}(\bar u) + e_{\gamma_1} = 0, \tag{3.18}$$

$$v_{\gamma_1}(\bar z) + e_{\gamma_1} = 1. \tag{3.19}$$

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, (3.19) 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, (3.17) and (3.19) yield that $j_2(\gamma_1) = 1$, a contradiction. Consequently, from (3.19) it follows that $e_{\gamma_1} = 1$; then $v_{\gamma_1}(\bar u) = -1$ is obtained from (3.18).

As far as γ_2 is concerned, note that

$$v_{\gamma_2}(\bar{z}-a/t)+e_{\gamma_2}=1, \tag{3.20}$$

$$v_{\gamma_2}(\bar{u})+e_{\gamma_2}=0, \tag{3.21}$$

$$v_{\gamma_2}(\bar{z})+e_{\gamma_2}=j_2(\gamma_2). \tag{3.22}$$

Then the assertion about γ_2 can be easily obtained in a similar way to the assertions on γ_1, taking into account that $j_2(\gamma_2)>1$. □

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

Lemma 3.24. *Let γ_3 be the linear place of $\mathbb{K}(\bar{u},\bar{z})$ centered at Y_∞ with tangent $X=a/t$, and let γ_4 be 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 3.25. *Let γ_5 be the place of $\mathbb{K}(\bar{u},\bar{z})$ centered at Q_1, and let γ_6 be the place of $\mathbb{K}(\bar{u},\bar{z})$ 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 (3.16), the number of zeros (and poles) of either $\bar{u}$ or $\bar{z}$ is 2. Then the assertion follows from Lemmas 3.23 and 3.24. □

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 3.25, (1.3) of Theorem 1.22 holds, so $\mathbb{K}(\bar{u},\bar{y})$ is a Kummer extension of $\mathbb{K}(\bar{u},\bar{z})$ and for a place γ of $\mathbb{K}(\bar{u},\bar{z})$

$$r_\gamma=\begin{cases}1, & \text{if } \gamma\in\{\gamma_2,\gamma_3,\gamma_4,\gamma_6\}\\ m, & \text{otherwise}\end{cases}, \tag{3.23}$$

where r_γ is defined as in (1.4). Also, by Theorem 1.22, the genus of $\mathbb{K}(\bar{u},\bar{y})$ is equal to

$$1+m(g-1)+\frac{1}{2}\cdot 4(m-1)=m(g-1)+2m-1,$$

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 $\mathbb{K}(\bar{u}, \bar{y})$ is less than or equal to $2m-1$. 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 $\gamma_2, \gamma_3, \gamma_4, \gamma_6$, as the ramification index is equal to

$$e(\gamma'|\gamma) = \begin{cases} m, & \text{if } \gamma \in \{\gamma_2, \gamma_3, \gamma_4, \gamma_6\} \\ 1, & \text{otherwise} \end{cases}, \tag{3.24}$$

by (3.23), where γ' is a place of $\mathbb{K}(\bar{u}, \bar{y})$. 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 3.25 and Definition 1.15-ii), the divisor of $\bar{u}$ in $\mathbb{K}(\bar{u}, \bar{y})$ can be easily computed.

LEMMA 3.26. *In* $\mathbb{K}(\bar{u}, \bar{y})$,

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

We can now apply Theorem 1.22, together with Lemma 3.26, in order to deduce that the extension $\mathbb{K}(\bar{u}, \bar{y})(\bar{x}) = \mathbb{K}(\bar{x}, \bar{y})$ of $\mathbb{K}(\bar{u}, \bar{y})$ defined by the equation $\bar{x}^m = \bar{u}$ is a Kummer extension of $\mathbb{K}(\bar{u}, \bar{y})$. Also, note that the places $\bar{\gamma}$ of $\mathbb{K}(\bar{u}, \bar{y})$ which ramify in the extension field $\mathbb{K}(\bar{x}, \bar{y})$ are precisely $\bar{\gamma}_1^i, \bar{\gamma}_5^i$, for $i = 1, \ldots, m$, as

$$r_{\bar{\gamma}} = \begin{cases} 1, & \text{if } \bar{\gamma} \in \{\bar{\gamma}_1^i, \bar{\gamma}_5^i\}_{i=1,\ldots,m} \\ m, & \text{otherwise} \end{cases},$$

and

$$e(\bar{\gamma}'|\bar{\gamma}) = \begin{cases} m, & \text{if } \bar{\gamma} \in \{\bar{\gamma}_1^i, \bar{\gamma}_5^i\}_{i=1,\ldots,m} \\ 1, & \text{otherwise} \end{cases}. \tag{3.25}$$

Hence, by Theorem 1.22 the genus of $\mathbb{K}(\bar{x}, \bar{y})$ is equal to

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

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

PROPOSITION 3.28. *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

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

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 3.27. □

3.2.1.3. $a=0$.

LEMMA 3.29. *The plane quartic curve* $\mathcal{Q}_P : g_P(X,Y)=0$ *with equation*

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

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

PROOF. Both X_∞ and Y_∞ are cuspidal double points of $\mathcal{Q}_P$, with tangent lines $Y=0$ and $X=0$ respectively. Also, $\mathcal{Q}_P$ does not admit any linear component as X divides $g_P(X,Y)$ if and only if Y divides $g_P(X,Y)$ and $g_P(X,Y)\neq X^2Y^2$. The intersection multiplicity of $\mathcal{Q}_P$ and $Y=0$ at X_∞ is equal to 3 and similarly $\mathrm{I}(Y_\infty,\mathcal{Q}_P\cap\{X=0\})=3$. Therefore, precisely one irreducible component $\mathcal{C}$ of $\mathcal{Q}_P$ passes through Y_∞. Note that Y_∞ is a double point of $\mathcal{C}$ and the generic order sequence of a place γ centered at Y_∞ is $(0,2,j_2(\gamma))$, with $j_2(\gamma)\ge 3$. Consequently, by Theorem 1.31 and (1.6) of Section 1.3, there is only one place of $\mathbb{K}(\mathcal{C})$ centered at Y_∞, which is the place of the tangent line $Y=0$, with order sequence $(j_0,j_1,j_2)=(0,2,3)$. 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 by Proposition 1.28. □

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

$$-bt^2\bar{u}\bar{z} - t^4\bar{u}^2\bar{z}^2 + 3t^2\bar{u}\bar{z} - t\bar{u} - t\bar{z} = 0. \tag{3.26}$$

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 3.29 there is precisely one place of $\mathbb{K}(\bar{u}, \bar{z})$ centered at Y_∞. As $\mathcal{Q}_P$ is left invariant by the transformation $X \mapsto Y$, $Y \mapsto X$, the same holds for X_∞. Arguing as in the proofs of Lemmas 3.23, 3.24 and 3.25, the following lemma can be proved.

Lemma 3.30. *Let γ_2 and γ_3 be the linear places of $\mathbb{K}(\bar{u}, \bar{z})$ centered at Y_∞ and X_∞ respectively, with tangents $X = 0$ and $Y = 0$. Then*

$$v_{\gamma_2}(\bar{u}) = 1, \qquad v_{\gamma_2}(\bar{z}) = -2,$$

and

$$v_{\gamma_3}(\bar{u}) = -2, \qquad v_{\gamma_3}(\bar{z}) = 1.$$

Proof. We keep the notation of Section 1.3. Taking into account that the order sequence of γ_2 is equal to $(0,2,3)$, we obtain

$$v_{\gamma_2}(\bar{z}) + e_{\gamma_2} = 0, \tag{3.27}$$

$$v_{\gamma_2}(\bar{u}) + e_{\gamma_2} = 3, \tag{3.28}$$

$$v_{\gamma_2}(\bar{u} - 1) + e_{\gamma_2} = 2. \tag{3.29}$$

From here one can easily deduce that $v_{\gamma_2}(\bar{u} - 1) = 0$. In fact, if $v_{\gamma_2}(\bar{u} - 1) > 0$, then $v_{\gamma_2}(\bar{u}) = 0$, and hence (3.29), (3.28) yield that $2 > e_{\gamma_2} = 3$ a contradiction. On the other hand, if $v_{\gamma_2}(\bar{u} - 1) < 0$, then $v_{\gamma_2}(\bar{u} - 1) = v_{\gamma_2}(\bar{u})$ that yields again a contradiction by comparing (3.28) and (3.29). Consequently, $e_{\gamma_2} = 2$ and the assertions on the valuations on γ_2 holds by (3.28) and (3.27).
As $\mathcal{Q}_P$ is left invariant by the transformation $X \mapsto Y$, $Y \mapsto X$, the valuations on γ_3 is obtained at once. □

Consequently, the divisors of both $\bar{u}$ and $\bar{z}$ can be computed. Clearly, γ_1 is a zero of $\bar{u}$ and $\bar{z}$ and from (3.26), the number of zeros (and poles) of either $\bar{u}$ or $\bar{z}$ is 2. Then the subsequent result follows from Lemma 3.30.

Lemma 3.31. *In $\mathbb{K}(\bar{u}, \bar{z})$,*

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

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 3.31 and Theorem 1.22, $\mathbb{K}(\bar{u},\bar{y})$ is a Kummer extension of $\mathbb{K}(\bar{u},\bar{z})$. As m is odd, by Lemma 3.31 we have that

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

By Theorem 1.22, the genus of $\mathbb{K}(\bar{u},\bar{y})$ is equal to

$$g'=1+m(g-1)+\frac{1}{2}\cdot 3(m-1), \tag{3.30}$$

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 $\gamma_1,\gamma_2,\gamma_3$ as 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 3.31 and Definition 1.15-ii), the divisors of both $\bar{u}$ and $\bar{y}$ in $\mathbb{K}(\bar{u},\bar{y})$ can be easily computed.

Lemma 3.32. *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 $\mathbb{K}(\bar{u},\bar{y})(\bar{x})=\mathbb{K}(\bar{x},\bar{y})$ of $\mathbb{K}(\bar{u},\bar{y})$ such that $\bar{x}^m=\bar{u}$. In order to apply Theorem 1.22, 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 3.33. *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 the integer interval $[\frac{3m}{2e}+\frac{1}{2};\frac{3m}{e}]$ is of type $[n;2n-1]$ for $n=\frac{3m}{2e}+\frac{1}{2}\in\mathbb{N}$ and

$$\cup_{j=1}^{\infty}[jn;(j+1)n-1]=\mathbb{N}\setminus\{1,\ldots,n-1\}.$$

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

As a consequence of Lemma 3.33, $\mathbb{K}(\bar{x}, \bar{y})$ is a Kummer extension of $\mathbb{K}(\bar{u}, \bar{y})$ defined by the equation $\bar{x}^m = \bar{u}$ and by Theorem 1.22, we obtain the following estimate for the genus of such an extension.

LEMMA 3.34. *The genus of* $\mathbb{K}(\bar{x}, \bar{y})$ *is at most* $\frac{3m^2-3m+2}{2}$.

PROOF. As all the places of $\mathbb{K}(\bar{u}, \bar{y})$ do not ramify in the extension field $\mathbb{K}(\bar{x}, \bar{y})$ by Lemma 3.32, i.e. the extension $\mathbb{K}(\bar{x}, \bar{y}) : \mathbb{K}(\bar{u}, \bar{y})$ is unramified according to Definition 1.18, then by Theorem 1.22 the genus of $\mathbb{K}(\bar{x}, \bar{y})$ is equal to $1 + m(g' - 1)$, where $g' \leq \frac{3m-1}{2}$ by (3.30), by whom the assertion holds. □

Arguing as in the proof of Proposition 3.28, the following result is obtained.

PROPOSITION 3.35. *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* $\frac{3m^2-3m+2}{2}$.

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

$$\mathcal{Y}_{P,c} : \begin{cases} f_{a,b,t,m}(X, Y) = 0 \\ c(a - tX^m)(a - tY^m) = Z^2 \end{cases} . \tag{3.31}$$

The existence of a suitable $\mathbb{F}_q$-rational point of $\mathcal{Y}_{P,c}$ 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 3.2.2. Here we prove the existence of an absolutely irreducible component of the curve $\mathcal{Y}_{P,c}$, in order to apply the Hasse–Weil bound to guarantee the existence of such a point.

PROPOSITION 3.36. *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* $\mathcal{Y}_{P,c}$ *has a 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 3.2.1.1. 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 [**24**], 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

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

Then it is easy to see that

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

whence

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

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 Corollary 1.26 and Remark 1.27 applied to $u=c(a-t\bar{x}^m)(a-t\bar{y}^m)$, for each $c\in\mathbb{F}_q$, $c\neq 0$, the space curve with equations

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

has an irreducible component defined over $\mathbb{F}_q$ which is a double cover of $\mathcal{C}$. The genus of such a component is equal to $2g-1+m=m^2-2m+1$, where g is the genus of $\mathcal{C}$. The claim then follows as such curve is contained in $\mathcal{Y}_{P,c}$ 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 3.2.1.2. By Lemma 3.26, 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 $\bar{\gamma}_5^1,\ldots,\bar{\gamma}_5^m$ and their common ramification index is m as shown in (3.25). 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 by (3.25), (3.24) and the transitivity of the ramification indexes (cfr. Proposition 1.19). 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 (3.17)–(3.22), together with Lemma 3.25, we deduce that

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

holds in $\mathbb{K}(\bar{u},\bar{z})$; 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 $\mathbb{K}(\bar{x},\bar{y})$

$$\operatorname{div}\big((a-t\bar{x}^m)(a-t\bar{y}^m)\big)=m\Big(\sum_{i=1}^{m}(\bar{\bar{\gamma}}_5^i+\bar{\bar{\gamma}}_6^i-\bar{\bar{\gamma}}_4^i-\bar{\bar{\gamma}}_2^i)\Big) \tag{3.32}$$

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 Corollary 1.26 and Remark 1.27 applied to $u=c(a-t\bar{x}^m)(a-t\bar{y}^m)\in\mathbb{K}(\bar{x},\bar{y})$, for each $c\in\mathbb{F}_q$, $c\neq 0$, the curve $\mathcal{Y}_{P,c}$ has an irreducible component defined over $\mathbb{F}_q$, which is a double cover of the curve $\mathcal{C}_P$, with genus at most $6m^2-4m+1$.

Case 3: $a=0$ We keep the notation of Section 3.2.1.3. 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 3.31 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 of $\mathbb{K}(\bar{x}, \bar{y})$ 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 Corollary 1.26 and Remark 1.27 applied to $u = c(a - t\bar{x}^m)(a - t\bar{y}^m) \in \mathbb{K}(\bar{x}, \bar{y})$, for each $c \in \mathbb{F}_q$, $c \neq 0$, the curve $\mathcal{Y}_{P,c}$ has an irreducible component defined over $\mathbb{F}_q$, which is a double cover of the curve $\mathcal{C}_P$, with genus at most $3m^2 - 2m + 1$.

□

3.2.2. 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 $XY = (X-1)^3$ (see Proposition 1.32 in Section 1.4). 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 $Q_t = (t, (t-1)^3/t)$ be a point in $G \setminus K$. Then the coset $K_t = K \oplus Q_t$ 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:

$$K_t = \Big\{\Big(tw^m, \frac{(tw^m - 1)^3}{tw^m}\Big) \mid w \in \mathbb{F}_q^*\Big\}. \tag{3.33}$$

For a point $P = (a, b)$ in $AG(2, q) \setminus \mathcal{X}$, let $f_{a,b,t,m}(X, Y) = 0$, defined as in (3.15).

Proposition 3.37. *The point P 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

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

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 3.38. *If*

$$q + 1 - (12m^2 - 8m + 2)\sqrt{q} \geq 8m^2 + 8m + 1, \tag{3.34}$$

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 $\mathcal{Y}_{P,c}$ be as in (3.31). Let $\mathbb{K}(\bar{x},\bar{y},\bar{w})$ be the function field of $\mathcal{Y}_{P,c}$, so that

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

We argue as in the proof of Proposition 3.14. 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 3.36–Case 2, that the only places of $\mathbb{K}(\bar{u},\bar{z})$ which 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 (3.32), 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 3.25 we have that

$$\begin{aligned} \mathrm{div}(\bar{x}) &= \sum_{\gamma\in\Omega_4\cup\Omega_5} 2\gamma - \sum_{\gamma\in\Omega 2} 2\gamma - \sum_{\gamma\in\Omega_1} \gamma, \\ \mathrm{div}(\bar{y}) &= \sum_{\gamma\in\Omega_2\cup\Omega_6} 2\gamma - \sum_{\gamma\in\Omega 4} 2\gamma - \sum_{\gamma\in\Omega_3} \gamma, \end{aligned}$$

in $\mathbb{K}(\bar{x},\bar{y},\bar{w})$. Also, by (3.32),

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

As $\bar{x}^m - \bar{y}^m = \bar{u} - \bar{z}$, 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 the Hasse–Weil bound, 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 3.37, 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 3.39. *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* (3.34) *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

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

is a non-square in $\mathbb{K}(\bar{x})$. 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 Corollary 1.26 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, yields 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 is needed, (see Definition 2.18). Let M be a maximal 3-independent subset of the factor group G/K containing K_t. By Proposition 2.21 applied to the canonical projection $\pi : G \to G/K$, the union A of the cosets of K corresponding to M is a good maximal 3-independent subset of $(G, \oplus)$. In geometrical terms, since three points in G are collinear if and only if their sum is equal to the neutral element, A is an arc whose secants cover all the points in G. By Propositions 3.38 and 3.39, if K is large enough with respect to q, then A is a bicovering arc as well, and the following result holds.

THEOREM 3.40. *Let m be a proper divisor of $q-1$ such that $(m, 6) = 1$ and (3.34) 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*

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

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

3.2.3. Small complete caps from nodal cubics. We use Theorem 3.40, together with the results in Section 2.3 in order to construct small complete caps in affine spaces $AG(N, q)$. Note that (3.34) 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 3.41. *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 Theorem 2.20 in Section 2.4. Then Theorem 3.42 below follows at once from Corollary 3.41.

THEOREM 3.42. *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*

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

(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*

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

3.2.4. Comparison with previous results. We distinguish two possibilities for the integer h such that $q=p^h$.

3.2.4.1. $h \leq 8$. The best previously known general construction of complete caps in $AG(N,q)$ is that given in [**3**], providing complete caps of size approximately $q^{N/2}/3$. It is often possible to choose m_1, m_2 as in Theorem 3.42 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 3.42 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.

3.2.4.2. $h>8$. 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 Theorem 3.20 of Section 3.1.4. Theorem 3.42 provides an improvement on such bound whenever it is possible to choose m_1, m_2 so that

$$(m_1+m_2)/m_1m_2 < 2/p^{\lfloor(\lceil h/4\rceil-1)/2\rfloor}. \tag{3.35}$$

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, 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 (3.35) 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 $m_2 = v_2$, this gives $(m_1+m_2)/m_1 m_2 < 2/p$.

3.3. Isolated double point case

3.3.1. Further properties of the family of curves of Section 3.2.1. 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, $\bar{t}$ is a non-zero element in $\mathbb{F}_{q^2}$ which is not an m-th power in $\mathbb{F}_{q^2}$. Let $A, B \in \mathbb{F}_{q^2}$ with $AB \neq (A-1)^3$. An important role for the present investigation is played by the curve

$$\mathcal{C}_{A,B,\bar{t},m} : f_{A,B,\bar{t},m}(X,Y) = 0, \tag{3.36}$$

where $f_{A,B,\bar{t},m}(X,Y)$ is defined as in (3.15). The curve $\mathcal{C}_{A,B,\bar{t},m}$, with $A, B, \bar{t}, m$ in $\mathbb{F}_q$ was thoroughly investigated in Section 3.2.1.

Proposition 3.43 (Proposition 3.28 in Section 3.2.1.2). *Let $A, B \in \mathbb{F}_{q^2}$ such that $AB \neq (A-1)^3$; if*

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

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

Under the assumptions of Proposition 3.43, let $\bar{x}$ and $\bar{y}$ denote the rational functions associated to the affine coordinates X and Y, respectively. Then $\mathbb{K}(\mathcal{C}_{A,B,\bar{t},m}) = \mathbb{K}(\bar{x},\bar{y})$ with $f_{A,B,\bar{t},m}(\bar{x},\bar{y}) = 0$. Let $\bar{u} = \bar{x}^m$ and $\bar{z} = \bar{y}^m$. The following results from Section 3.2.1 about the function field extension $\mathbb{K}(\bar{x},\bar{y}) : \mathbb{K}(\bar{u},\bar{z})$ will be needed.

Proposition 3.44 (Lemma 3.25 in Section 3.2.1.2). *In the function field $\mathbb{K}(\bar{u},\bar{z})$, there exist six places γ_j, $j = 1, \ldots, 6$, such that*

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

The following propositions hold from the results in Section 3.2.1.

Proposition 3.45 (Case 2 in Section 3.2.1). *For each $j = 1, \ldots, 6$, the ramification indexes of the places over γ_j in the extension $\mathbb{K}(\bar{x},\bar{y})$ over $\mathbb{K}(\bar{u},\bar{z})$ are all equal to m and no other place is ramified.*

We keep the notation of Case 2 of Section 3.2.1 and denote by $\bar{\bar{\gamma}}_j^1, \ldots, \bar{\bar{\gamma}}_j^m$ the places of $\mathbb{K}(\bar{x},\bar{y})$ lying over the place γ_j of $\mathbb{K}(\bar{u},\bar{z})$, for $j = 1, \ldots, 6$.

Proposition 3.46 (Case 2 of Section 3.2.1). *In* $\mathbb{K}(\bar{x},\bar{y})$,

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

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 a cubic with an isolated double point we need to establish whether the rational function

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

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

Lemma 3.47. *Assume that A and B satisfy the conditions of Proposition 3.43. For $c\in\mathbb{K}$, $c\neq 0$, let*

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

If $A\neq 1$, then:

i) *the divisor of η is*

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

where $\bar{\bar{D}}$ is a divisor of degree $4m^2$ whose support consists of places not lying over any place γ_j of $\mathbb{K}(\bar{u},\bar{z})$, for $j=1,\dots,6$;

ii) *the function field $\mathbb{K}(\bar{x},\bar{y},\bar{\omega})$ with $\bar{\omega}^2=\eta$ is a Kummer extension of $\mathbb{K}(\bar{x},\bar{y})$;*

iii) *the genus of the function field $\mathbb{K}(\bar{x},\bar{y},\bar{\omega})$ is less than or equal to $8m^2-4m+1$.*

Proof. By Proposition 3.44 it is easy to deduce that

$$\operatorname{div}_\infty(1-t\bar{u})=-\gamma_1-\gamma_2,$$

while the degree-2 divisor D_1 of the zeros of $1-t\bar{u}$ does not contain the places γ_j, with $j=3,4,5,6$, as γ_3 and γ_4,γ_5 are the zeros of the rational functions $A-t\bar{u}$ and $\bar{u}$ respectively, with $A\neq 1$. Similarly,

$$\operatorname{div}_\infty(1-t\bar{z})=-\gamma_3-\gamma_4$$

and the degree-2 divisor D_2 of the zeros of $1-t\bar{z}$ does not contain the places γ_j, with $j=1,2,5,6$. Hence, in $\mathbb{K}(\bar{u},\bar{z})$ we have

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

where $D=D_1+D_2$ is an effective 4-degree divisor whose support does not contain $\{\gamma_j\mid j=1,\dots,6\}$. Therefore, by Proposition 3.45,

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

where $\bar{\bar{D}}$ is a divisor of degree $4m^2$ whose support is disjoint from the set of places lying over $\{\gamma_j \mid j = 1, \dots, 6\}$. Then, i) holds by Proposition 3.46.
Since m is odd, η is a non-square in $\mathbb{K}(\bar{x}, \bar{y})$, as there exist at least one place of $\operatorname{div}(\eta)$ having odd valuation. So by Theorem 1.22, assertion ii) and iii) holds, as the number of places of $\operatorname{div}(\eta)$ with odd valuation are at most $4m + 4m^2$. □

3.3.2. A family of curves defined over $\mathbb{F}_q$. For $a, b \in \mathbb{F}_q$ with $b(a^2 - \beta^2) \neq 1$, let $P = (a, b)$ be the point in $AG(2, q) \setminus \mathcal{X}$ and let

$$g_P(X, Y) := bX^2Y^2 - (b\beta^2 + 1)(X^2 + Y^2) - XY + a(X + Y) + \beta^2(b\beta^2 + 1).$$

Under the assumptions of Section 3.3.1, a crucial role for the investigation of the covering properties of a coset of index m in the abelian group of the non-singular $\mathbb{F}_q$-rational points of a cubic with an isolated double point is played by the curve

$$\mathcal{L}_P : \ell_{a,b,\bar{t},m}(X, Y) = 0, \tag{3.37}$$

where

$$\ell_{a,b,\bar{t},m}(X, Y) = (\bar{t}X^m - 1)^2(\bar{t}Y^m - 1)^2 g_P\Big(\beta\frac{\bar{t}X^m + 1}{\bar{t}X^m - 1}, \beta\frac{\bar{t}Y^m + 1}{\bar{t}Y^m - 1}\Big), \tag{3.38}$$

The curve $\mathcal{L}_P$ actually belongs to the family described in Section 3.3.1.

Lemma 3.48. *Let*

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

Then

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

where $f_{A,B,\bar{t},m}$ is defined as in (3.15).

Proof. The proof is a straightforward computation. □

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

Lemma 3.49. *If*

$$P \notin \Big\{(0, -\frac{9}{8\beta^2}), (\beta\sqrt{-3}, 0), (-\beta\sqrt{-3}, 0)\Big\} \tag{3.39}$$

then $\mathcal{L}_P$ is an absolutely irreducible curve with genus less than or equal to $3m^2 - 3m + 1$.

Proof. For A, B as in Lemma 3.48, let $\mathcal{C}_{A,B,\bar{t},m}$ be as in (3.36). By Lemma 3.48, the curve $\ell_{a,b,\bar{t},m}(X, Y) = 0$ is actually $\mathcal{C}_{A,B,\bar{t},m}$. Note that m divides $q^2 - 1$ and that each coefficient of $f_{A,B,\bar{t},m}(X, Y)$ lies in $\mathbb{F}_{q^2}$. Then by Proposition 3.43 the curve $\mathcal{C}_{A,B,\bar{t},m}$ is absolutely irreducible of genus $g \leq 3m^2 - 3m + 1$, provided that none of the following holds:

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

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

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

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

Remark 3.50. *Let $q = p^h$ with $p > 3$ a prime. Then -3 is a non-square in $\mathbb{F}_q$ if and only if h is odd and $p \equiv 2 \pmod 3$; see e.g.* [**26**, Lemma 4.5].

In order to show that if (3.39) holds then P is collinear with two distinct points of a coset of index m in the abelian group of the non-singular $\mathbb{F}_q$-rational points of a cubic with an isolated double point, we need to ensure the existence of a point (x, y) of the curve $\mathcal{L}_P$. Unfortunately, Hasse-Weyl bound cannot be directly applied, as $\mathcal{L}_P$ is not defined over $\mathbb{F}_q$. To this end, it is useful to consider a curve which is birationally equivalent to $\mathcal{L}_P$, but, unlike $\mathcal{L}_P$, is defined over $\mathbb{F}_q$. Let

$$\mathcal{M}_P : m_{a,b,\bar{t},m}(R, V) = 0, \tag{3.40}$$

where

$$m_{a,b,\bar{t},m}(R, V) := (R-\beta)^{2m}(V-\beta)^{2m}\ell_{a,b,\bar{t},m}\Big(\frac{R+\beta}{R-\beta}, \frac{V+\beta}{V-\beta}\Big) = 0. \tag{3.41}$$

Lemma 3.51. *If* (3.39) *holds, then $\mathcal{M}_P$ is an absolutely irreducible curve birationally equivalent to $\mathcal{L}_P$.*

Proof. Let $\mathbb{K}(\bar{x}, \bar{y})$ be the function field of the curve $\mathcal{L}_P$, so that $\ell_{a,b,\bar{t},m}(\bar{x}, \bar{y}) = 0$. 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

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

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

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

we have

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

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. □

LEMMA 3.52. *The curve $\mathcal{M}_P$ is defined over $\mathbb{F}_q$.*

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

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

Let

$$t = \beta\frac{\bar{t}+1}{\bar{t}-1}, \tag{3.42}$$

As both t and β^2 belong to $\mathbb{F}_q$ by (3.47), the polynomials

$$h(Z) = t\theta_1(Z) + \beta^2\theta_2(Z), \qquad l(Z) = \theta_1(Z) + t\theta_2(Z) \tag{3.43}$$

actually lie in $\mathbb{F}_q[Z]$. Taking into account (3.42), a straightforward computation gives

$$\bar{t}\Big(\frac{Z+\beta}{Z-\beta}\Big)^m = \frac{\frac{h(Z)}{l(Z)}+\beta}{\frac{h(Z)}{l(Z)}-\beta}. \tag{3.44}$$

Whence,

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

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

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

From

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

we obtain

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

whence the assertion. □

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 a cubic with an isolated double point we need to consider the rational function $\big(a - \frac{h(\bar{r})}{l(\bar{r})}\big)\big(a - \frac{h(\bar{v})}{l(\bar{v})}\big)$ in the function field of the curve $\mathcal{M}_P$, where $h(Z)$ and $l(Z)$ are defined as in (3.43).

LEMMA 3.53. *Let $a, b \in \mathbb{F}_q$ satisfying* (3.39)*, with $b(a^2-\beta^2) \neq 1$, and let $\mathbb{K}(\bar{r},\bar{v})$ be the function field of $\mathcal{M}_P$, so that $m_{a,b,\bar{t},m}(\bar{r},\bar{v}) = 0$. Then the rational function $\nu = \big(a - \frac{h(\bar{r})}{l(\bar{r})}\big)\big(a - \frac{h(\bar{v})}{l(\bar{v})}\big)$ is not a square in $\mathbb{K}(\bar{r},\bar{v})$.*

Proof. Let $\bar{x}$ and $\bar{y}$ be as in the proof of Lemma 3.51, so that $\mathbb{K}(\bar{r},\bar{v})=\mathbb{K}(\bar{x},\bar{y})$ with $f_{A,B,\bar{t},m}(\bar{x},\bar{y})=0$. Then, by (3.44),

$$\frac{h(\bar{r})}{l(\bar{r})}=\beta\frac{\bar{t}\bar{x}^m+1}{\bar{t}\bar{x}^m-1},\qquad \frac{h(\bar{v})}{l(\bar{v})}=\beta\frac{\bar{t}\bar{y}^m+1}{\bar{t}\bar{y}^m-1}.$$

Consequently, as $a=\beta\frac{A+1}{A-1}$ by Lemma 3.48, then after some computation

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

from whom

$$\left(a-\frac{h(\bar{r})}{l(\bar{r})}\right)\left(a-\frac{h(\bar{v})}{l(\bar{v})}\right)=\frac{4\beta^2(\bar{t}\bar{x}^m-A)(\bar{t}\bar{y}^m-A)}{(A-1)^2(\bar{t}\bar{x}^m-1)(\bar{t}\bar{y}^m-1)}. \tag{3.45}$$

Then, the assertion follows from Lemma 3.47. □

The hypothesis of Corollary 1.26 are satisfied by the curve $\mathcal{C}=\mathcal{M}_P$ and by the rational function $u=\nu$. So, we deduce the following result by applying Corollary 1.26 and Remark 1.27, taking into account (3.45).

Proposition 3.54. *Let $a,b\in\mathbb{F}_q$ satisfying (3.39), with $b(a^2-\beta^2)\neq 1$. For each $c\in\mathbb{F}_q(\mathbb{K}?)$, $c\neq 0$, the space curve*

$$\mathcal{Y}_{P,c}:\begin{cases} m_{a,b,\bar{t},m}(R,V)=0\\ c(a-tR^m)(a-tV^m)=Z^2(1-tR^m)(1-tV^m)\end{cases}$$

has a component defined over $\mathbb{F}_q$ with genus less than or equal to $8m^2-4m+1$.

3.3.3. Complete arcs from 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 $\beta^2\in\mathbb{F}_q$. If $\mathcal{X}$ is a singular plane cubic defined over $\mathbb{F}_q$ with an isolated double point and at least one $\mathbb{F}_q$-rational inflection, then a canonical equation for $\mathcal{X}$ is

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

(see Proposition 1.32 in Section 1.4). 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 $\mathcal{X}$.

A non-standard parametrization for the points of $\mathcal{X}\setminus\{Y_\infty\}$ is taking into account. For $v\in\mathbb{K}\setminus\{0,1\}$, let Q_v be the point with affine coordinates $\left(\frac{v+1}{v-1}\beta,\frac{(v-1)^2}{4v\beta^2}\right)$; it is easily seen that $Q_v\in\mathcal{X}$ as

$$\frac{(v-1)^2}{4v\beta^2}=\frac{1}{\left(\frac{v+1}{v-1}\beta\right)^2-\beta^2}.$$

Also, let $Q_0 = Y_\infty$ and $Q_1 = X_\infty$. Such a parametrization actually defines an isomorphism between the multiplicative group of $\mathbb{K}$ and $(\mathcal{X} \setminus \{Y_\infty\}, \oplus)$, defined by $\phi(v) = Q_v$, for all $v \in \mathbb{K}^*$. In fact,

$$Q_v \oplus Q_w = Q_{vw}, \tag{3.46}$$

holds for $v, w \in \mathbb{K}^*$. This can be easily proved in few steps by using the collinearity condition of three distinct affine points Q_v, Q_w, Q_x of $\mathcal{X}$, that is

$$\det \begin{pmatrix} \frac{v+1}{v-1}\beta & \frac{(v-1)^2}{4v\beta^2} & 1 \\ \frac{w+1}{w-1}\beta & \frac{(w-1)^2}{4w\beta^2} & 1 \\ \frac{x+1}{x-1}\beta & \frac{(x-1)^2}{4x\beta^2} & 1 \end{pmatrix} = 0;$$

after some computation, this is equivalent to

$$\frac{(v-w)(v-x)(w-x)(xvw-1)}{2vwx\beta(w-1)(v-1)(x-1)} = 0$$

that holds if and only if $x = 1/vw$. Consequently, (3.46) holds, taking into account that $\ominus Q_x = Q_{1/x} = Q_{vw}$.

For $u \in \mathbb{K} \setminus \{\pm\beta\}$, let $P_u = \left(u, \frac{1}{u^2-\beta^2}\right)$ be the standard parametrization of an affine point on $\mathcal{X}$;

Remark 3.55. *The point P_u coincides with Q_v if $v = \frac{u+\beta}{u-\beta}$ or equivalently if $u = \beta\frac{v+1}{v-1}$, i.e. it is possible to pass from the trivial to the non standard parametrization of the points of $\mathcal{X}$ through the invertible application $u \mapsto \frac{u+\beta}{u-\beta}$, where $u \in \mathbb{K} \setminus \{0, 1\}$, in fact*

$$Q_{\frac{u+\beta}{u-\beta}} = \left(\frac{\frac{u+\beta}{u-\beta}+1}{\frac{u+\beta}{u-\beta}-1}\beta, \frac{\left(\frac{u+\beta}{u-\beta}-1\right)^2}{4\frac{u+\beta}{u-\beta}\beta^2} \right) = \left(\frac{\frac{2u}{u-\beta}}{\frac{2\beta}{u-\beta}}\beta, \frac{\frac{4\beta^2}{(u-\beta)^2}}{4\frac{u+\beta}{u-\beta}\beta^2} \right) =$$

$$= \left(u, \frac{4\beta^2}{(u-\beta)^2} \cdot \frac{u-\beta}{4\beta^2(u+\beta)}\right) = \left(u, \frac{1}{u^2-\beta^2}\right) \in \mathcal{X}.$$

The group G of the $(q+1)$ non-singular $\mathbb{F}_q$-rational points of $\mathcal{X}$ form a cyclic subgroup of $(\mathcal{X} \setminus \{Y_\infty\}, \oplus)$. By Remark 3.55, it is easily seen that

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

The group G has precisely one subgroup K of index m, with $(m, 6) = 1$, consisting of the m-th powers in G. By (3.46),

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

Let $P_t = Q_{\bar{t}}$ be a point in $G \setminus K$; then, by Remark 3.55

$$t = \beta\frac{\bar{t}+1}{\bar{t}-1} \in \mathbb{F}_q \tag{3.47}$$

and let

$$K_{\bar{t}} = K \oplus Q_{\bar{t}} = \left\{ Q_{\bar{t}(\frac{u+\beta}{u-\beta})^m} \mid u \in \mathbb{F}_q \right\} \cup \{Q_{\bar{t}}\}. \tag{3.48}$$

be a coset of K in G.

Remark 3.56. *By definition, the X-coordinate of the point $Q_{\bar{t}(\frac{z+\beta}{z-\beta})^m}$ in $K_{\bar{t}}$ is $u = \beta(\bar{t}(\frac{z+\beta}{z-\beta})^m + 1)/(\bar{t}(\frac{z+\beta}{z-\beta})^m - 1)$. Then, by* (3.44)*, $u = \frac{h(z)}{l(z)} \in \mathbb{F}_q$, as $h(Z)$ and $l(Z)$ defined as in* (3.43) *are polynomials in $\mathbb{F}_q[Z]$. Consequently, if $\bar{z}$ is trascendental over $\mathbb{F}_q$, then $u(\bar{z})$ is defined over $\mathbb{F}_q$.*

For a point $P = (a, b)$ in $AG(2, q) \setminus \mathcal{X}$, let $\ell_{a,b,\bar{t},m}(X, Y) = 0$, defined as in (3.38).

Lemma 3.57. *Let (x, y) be an affine point of the curve $\ell_{a,b,\bar{t},m}(X, Y) = 0$. If*

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

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

Proof. We first note that for u, v distinct elements in $\mathbb{K} \setminus \{\pm\beta\}$, the point P is collinear with P_u and P_v if and only if $g_P(u, v) = 0$. In fact,

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

is equal to

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

that is equal to zero if and only if $g_P(u, v) = 0$, as P_u and P_v are distinct points. Also, by Remark 3.55, the points $Q_{\bar{t}x^m}$ and $Q_{\bar{t}y^m}$ coincide with P_u and P_v respectively, precisely when

$$u = \beta\frac{\bar{t}x^m + 1}{\bar{t}x^m - 1}, \qquad v = \beta\frac{\bar{t}y^m + 1}{\bar{t}y^m - 1}.$$

Then the claim follows by the definition of $\ell_{a,b,\bar{t},m}$ in (3.38). □

Remark 3.58. *If (r, v) is an $\mathbb{F}_q$-rational affine point of the curve $\mathcal{M}_P$ defined as in* (3.40)*, 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 (3.48).

Proposition 3.59. *Let $P = (a, b)$ be a point in $AG(2, q)$ off $\mathcal{X}$. Assume that* (3.39) *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 $\mathcal{M}_P$, 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 3.51, we have that

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

satisfy $f_{A,B,\bar{t},m}(\bar{x},\bar{y})=0$. Therefore, by Propositions 3.44 and 3.45 the number places satysfying (2) is $4m$. Also, by Proposition 3.44 follows 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 zeros of $\bar{x}^m-\bar{y}^m$ in $\mathbb{K}(\bar{x},\bar{y})$ has size less than or equal to $4m^2$. This shows that E comprises at most $4m^2+8m$ places. Our assumption on q and m, together with the Hasse–Weil bound, ensures the existence of at least $4m^2+8m+1$ $\mathbb{F}_q$-rational places of $\mathbb{K}(\bar{r},\bar{v})$; hence, there exists at least one $\mathbb{F}_q$-rational place γ_0 of $\mathbb{K}(\bar{r},\bar{v})$ not in E. Let $\tilde{r}=\bar{r}(\gamma_0)$ and $\tilde{v}=\bar{v}(\gamma_0)$. By Remark 3.58, $P=(a,b)$ is collinear with $Q_{\bar{t}(\frac{\tilde{r}+\beta}{\tilde{r}-\beta})^m}$ and $Q_{\bar{t}(\frac{\tilde{v}+\beta}{\tilde{v}-\beta})^m}$, which are two distinct points in $K_{\bar{t}}$. □

The following technical variant of Proposition 3.59 will also be needed.

Proposition 3.60. *Let $P=(a,b)$ be a point in $AG(2,q)$ off $\mathcal{X}$. Assume that* (3.39) *holds. If*

$$q+1-(6m^2-6m+2)\sqrt{q}\geq 8m^2+8m+1 \tag{3.49}$$

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

Proof. One can argue as in the proof of Proposition 3.59. We need to ensure that neither $Q_{\bar{t}(\frac{\tilde{r}+\beta}{\tilde{r}-\beta})^m}$ or $Q_{\bar{t}(\frac{\tilde{v}+\beta}{\tilde{v}-\beta})^m}$ coincides with $Q_{\bar{t}}$. This is equivalent to γ_0 not being a zero of either $(\frac{\bar{r}+\beta}{\bar{r}-\beta})^m-1$ or $(\frac{\bar{v}+\beta}{\bar{v}-\beta})^m-1$ in the function field $\mathbb{K}(\bar{r},\bar{v})$. By Proposition 3.44, 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. □

If (3.39) is not satisfied, then P is not collinear with any two points of $K_{\bar{t}}$. Actually, a stronger statement holds.

Proposition 3.61. *If*

$$P \in \Big\{(0, -\frac{9}{8\beta^2}), (\beta\sqrt{-3}, 0), (-\beta\sqrt{-3}, 0)\Big\}.$$

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

Proof. We recall that by the proof of Lemma 3.57, the point P is collinear with $(u, \frac{1}{u^2-\beta^2})$ and $(v, \frac{1}{v^2-\beta^2})$, with $u, v \in \mathbb{F}_q$, if and only if $g_P(u, v) = 0$. If $(a, b) = (0, -\frac{9}{8\beta^2})$ then

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

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

If $g_P(u, v) = 0$, then either

$$3uv - u\beta + v\beta + \beta^2 = 0 \quad \text{or} \quad 3uv + u\beta - v\beta + \beta^2 = 0. \tag{3.50}$$

If $(u, v) \in \mathbb{F}_q$, then both u and v are fixed by the Frobenius map over $\mathbb{F}_q$, and hence both equalities in (3.50) hold. This easily implies $u = v$. Then no two distinct $\mathbb{F}_q$-rational affine points of $\mathcal{X}$ can be collinear with (a, b).

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

$$g_{\beta\sqrt{-3},0}(X, Y) = -(X^2 + Y^2) - XY + \beta\sqrt{-3}(X + Y) + \beta^2 =$$

$$= -\Big(X + \frac{1 + \sqrt{-3}}{2}Y + \frac{-\beta\sqrt{-3} + \beta}{2}\Big)\Big(X + \frac{1 - \sqrt{-3}}{2}Y + \frac{-\beta\sqrt{-3} - \beta}{2}\Big)$$

and

$$g_{-\beta\sqrt{-3},0}(X, Y) = -(X^2 + Y^2) - XY - \beta\sqrt{-3}(X + Y) + \beta^2 =$$

$$= -\Big(X + \frac{1 - \sqrt{-3}}{2}Y + \frac{\beta\sqrt{-3} + \beta}{2}\Big)\Big(X + \frac{1 + \sqrt{-3}}{2}Y + \frac{\beta\sqrt{-3} - \beta}{2}\Big)$$

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

In order to cover the points on $\mathcal{X}$, union of distinct cosets need to be considered and the notion of a maximal 3-independent subset as defined in Section 2.4 is fundamental. Assume that S is a good maximal 3-independent subset of G. Since three points in G are collinear if and only if their sum is equal to the neutral element, S

is an arc whose secants cover all the points in G. If m and $(q+1)/m$ are coprime, Theorem 2.20 can be applied to G.

Proposition 3.62. *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 $T = R' \ominus 2R$. Then*

$$\mathcal{A} = K_{\bar{t}} \setminus \{T\} \quad \bigcup \quad (H \oplus R) \setminus \{\ominus 2R' \oplus R\}$$

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 (3.39). By Remark 3.50, the size of $\mathcal{E}$ is 3 precisely when h is odd and $p \equiv 2 \pmod 3$; otherwise, $\mathcal{E}$ consists of the point with coordinates $(0, -\frac{9}{8\beta^2})$.

Let $\mathcal{A}$ be as in Proposition 3.62. We use Propositions 3.60, 3.61, and 3.62 in order to construct small complete arcs in Galois planes. Note that (3.49) is implied by $m \leq \frac{\sqrt[4]{q}}{\sqrt{6}}$.

Theorem 3.63. *Let $q = p^h$ 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 h 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 h 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 $m + \frac{q+1}{m}$.*

3.3.4. Bicovering arcs from cubics with an isolated double point.

Throughout this section $q = p^h$ with p a prime, $p > 3$. Also, $\mathcal{X}$, G, m, K and $K_{\bar{t}}$ are as in Section 3.3.3. With a similar proof to that of Propositions 3.59 and 3.60, it can be proved that every point off $\mathcal{X}$ is bicovered by $K_{\bar{t}}$.

Proposition 3.64. *Let $P = (a,b)$ be a point in $AG(2,q)$ off $\mathcal{X}$. Assume that (3.39) holds. If*

$$q + 1 - (16m^2 - 8m + 2)\sqrt{q} \geq 16m^2 + 24m + 1 \tag{3.51}$$

then P is bicovered by the points of $K_{\bar{t}}$.

Proof. Let $\mathbb{K}(\bar{r}, \bar{v})$ be the function field of the curve $\mathcal{M}_P$, so that $m_{a,b,\bar{t},m}(\bar{r}, \bar{v}) = 0$. By Lemma 3.47 and Lemma 3.53, for every $c \in \mathbb{F}_q^*$ the equation

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

defines a Kummer extension $\mathbb{K}(\bar{r}, \bar{v}, \bar{w})$ of $\mathbb{K}(\bar{r}, \bar{v})$ with genus less than or equal to $8m^2 - 4m + 1$. Let E be as in the proof of Proposition 3.59, and let E' be the set of places of $\mathbb{K}(\bar{r}, \bar{v}, \bar{w})$ that either lie over a place in E or over a zero or a pole of

$\big(a - \frac{h(\bar{r})}{l(\bar{r})}\big)\big(a - \frac{h(\bar{v})}{l(\bar{v})}\big)$. Then, by Lemma 3.47 together with the proof of Proposition 3.59,

$$|E'| \leq 2|E| + 2(4m^2 + 8m) \leq 16m^2 + 24m$$

and an upper bound for the size of E' is $16m^2 + 24m$. Our assumption on q and m, together with Theorem 1.30, ensures the existence of at least $16m^2 + 24m + 1$ $\mathbb{F}_q$-rational places of $\mathbb{K}(\bar{r}, \bar{v}, \bar{w})$; hence, there exists at least one $\mathbb{F}_q$-rational place γ_c of $\mathbb{K}(\bar{r}, \bar{v}, \bar{w})$ not in E'. Let

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

As $\mathbb{K}(\bar{r}, \bar{v}, \bar{w})$ is the function field of some irreducible component of the curve $\mathcal{Y}_{P,c}$, defined as in Proposition 3.54, then $P_c = (\tilde{r}, \tilde{v})$ is an $\mathbb{F}_q$-rational affine point of the curve $\mathcal{M}_P$. Therefore, by Remark 3.58, P is collinear with two distinct points

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

According to whether c is a non-zero square or not, then the point P is external or internal to the segment $P_{1,c}P_{2,c}$. This proves the assertion. □

In the final part of this section we deal with points in $\mathcal{X}$. Actually, all the $\mathbb{F}_q$-rational points of $\mathcal{X}$ but one are bicovered by the union of two distinct coset.

Proposition 3.65. *Let $K_{\bar{t}'}$ be a coset of K such that $K_{\bar{t}} \cup K_{\bar{t}'}$ is an arc. For $u \in \mathbb{F}_q$, let $P_u = (u, \frac{1}{u^2-\beta^2})$ be an $\mathbb{F}_q$-rational affine point of $\mathcal{X}$ not belonging to $K_{\bar{t}} \cup K_{\bar{t}'}$ but collinear with a point of $K_{\bar{t}}$ and a point of $K_{\bar{t}'}$.*

(i) *If $u \neq 0$ and (3.51) holds, then P_u is bicovered by $K_{\bar{t}} \cup K_{\bar{t}'}$.*
(ii) *The point $P_0 = (0, -\frac{1}{\beta^2})$ is not bicovered by $K_{\bar{t}} \cup K_{\bar{t}'}$. It is internal (resp. external) to every segment cut out on $K_{\bar{t}} \cup K_{\bar{t}'}$ by a line through P_0 when $q \equiv 1 \pmod 4$ (resp. $q \equiv 3 \pmod 4$).*

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

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

for some $x \in \mathbb{F}_q$, (see Remark 3.56). In this case, $Q = \big(s(e), \frac{1}{s(e)^2-\beta^2}\big)$ with $s(e) = -\frac{ue+\beta^2}{u+e}$. Also, for an element $\bar{x}$ transcendental over $\mathbb{K}$, the rational function describing the X-coordinate of the point P is given by

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

In order to determine whether P_u is bicovered by $K_{\bar{t}} \cup K_{\bar{t}'}$ we need to investigate whether the rational function

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

is a square in $\mathbb{K}(\bar{x})$. Let γ be a zero of $\bar{t}(\frac{\bar{x}+\beta}{\bar{x}-\beta})^m - 1$ in $\mathbb{K}(\bar{x})$. Note that since $(m, p) = 1$, the polynomial $tZ^m - 1$ has no multiple roots in $\mathbb{K}[Z]$. Then the valuation $v_\gamma(e(\bar{x}))$ of $e(\bar{x})$ at γ is -1. If in addition $u \neq 0$, then $v_\gamma(\eta(\bar{x})) = v_\gamma(e(\bar{x})) = -1$, whence $\eta(\bar{x})$ is not a square in $\mathbb{K}(\bar{x})$ and Proposition 1.26 applies to $c\eta(\bar{x})$ for each $c \in \mathbb{F}_q^*$. Since the number of poles of $\eta(\bar{x})$ is at most $2m$, the genus of the Kummer extension $\mathbb{K}(\bar{x}, \bar{w})$ of $\mathbb{K}(\bar{x})$ with $\bar{w}^2 = c\eta(\bar{x})$ is at most $2m - 1$.

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

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

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

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

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

Assume now that $u = 0$. First note that P_0 coincides with Q_{-1}, and hence belongs to K. Therefore, as m is odd, P_0 cannot be collinear with any two points from the same coset of K. Assume then that P_0 is collinear with $P = (e, \frac{1}{e^2-\beta^2}) \in K_{\bar{t}}$ and $Q = \left(s(e), \frac{1}{s(e)^2-\beta^2}\right) \in K_{\bar{t}'}$. 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 $q \equiv 1 \pmod 4$. □

Let M be a maximal 3-independent subset of the factor group G/K containing $K_{\bar{t}}$. Then the union

$$S = \bigcup_{K_{\bar{t}_i} \in M} K_{\bar{t}_i}$$

of the cosets of K corresponding to M is a good maximal 3-independent subset of G; (see Proposition 2.21 in Section 2.4). 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 h is even or $p \equiv 1 \pmod 3$, by Propositions 3.61, 3.64, and 3.65, 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, or equivalently that (3.51) holds.

THEOREM 3.66. *Let $q = p^h$ with $p > 3$ a prime, and assume that either h is even or $p \equiv 1 \pmod 3$. Let m be a proper divisor of $q+1$ such that $(m, 6) = 1$ and (3.51) holds. For M a maximal 3-independent subset of the factor group G/K, the point set*

$$\mathcal{B} = \Big(\bigcup_{K_{\bar{t}_i} \in M} K_{\bar{t}_i} \Big) \bigcup \mathcal{E} \tag{3.52}$$

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 h is odd and $p \equiv 2 \pmod 3$ a further condition on M is needed in order to ensure that $\mathcal{B}$ as in (3.52) is an almost bicovering arc. Note that by Proposition 3.61, there is precisely one point in G collinear with any two points in $\mathcal{E}$. In particular, a point Q_1 in G is collinear with $(0, -\frac{9}{8\beta^2})$ and $(\beta\sqrt{-3}, 0)$; similarly, only one point Q_2 in G is collinear with $(0, -\frac{9}{8\beta^2})$ and $(-\beta\sqrt{-3}, 0)$. Consequently, it is sufficient to require the set S not to contain the cosets having as representatives these points of G, in order to obtain an almost bicovering arc.

THEOREM 3.67. *Let $q = p^h$ with $p > 3$ a prime. Assume that h is odd and $p \equiv 2 \pmod 3$. Let m be a proper divisor of $q + 1$ such that $(m, 6) = 1$ and (3.51) holds. 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*

$$\mathcal{B} = \Big(\bigcup_{K_{\bar{t}_i} \in M} K_{\bar{t}_i} \Big) \bigcup \mathcal{E}$$

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

3.3.5. Small Complete caps from cubics with an isolated double point.

We use Theorems 3.66 and 3.67, together with Theorem 2.16, 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 (see Theorem 2.20) 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 (3.51) is implied by $m \leq \frac{\sqrt[4]{q}}{4}$, the following result holds.

THEOREM 3.68. *Let $q = p^h$ with $p > 3$, and let m be a proper divisor of $q + 1$ such that $(m, 6) = 1$ and $m \leq \frac{\sqrt[4]{q}}{4}$. Assume that $m = m_1 m_2$ with $(m_1, m_2) = 1$. Then*

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

$$(m_1 + m_2 - 3) \cdot \frac{q+1}{m} + 3;$$

(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*

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

3.4. Bicovering arcs and complete caps for m a prime

By Corollary 3.41, Theorem 3.66 and Theorem 3.67, when q is large enough with respect to m, bicovering 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 3.42 and 3.68, m is assumed to be a composite integer in order to apply the explicit construction of maximal 3-independent subsets provided by Szőnyi (see Theorem 2.20 in Section 2.4). As to the prime case, it was shown in [**78**] 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 bicovering arcs of size less than $q/3$ and complete caps of size less than $\frac{1}{3}q^{N/2}$. In [**33**] 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 [**33**, Theorem 3.4] can be proved by straightforward computation.

Proposition 3.69. *Let $m > 3$ be a prime. For an odd divisor $m' \geq 7$ of $m+5$, let $k = (m+5)/m' > 4$. Then*

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

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 3.69, together with Corollary 3.41, Theorem 3.66 and Theorem 3.67, complete caps in $AG(N,q)$ with approximately

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

points can be constructed. This shows that, apart from the constant $3/2$, Theorems 3.42 and 3.68 remain valid for m a prime, and m_1, m_2 suitable divisors of $m+5$.

3.5. Complete caps and quasi-perfect linear codes

In this section we keep the notation of Section 1.5 and we will survey some applications of complete caps to Coding theory. In fact, a complete cap (see Definition 2.1) is the geometrical counterpart of a code with covering radius $R = 2$ and $d = 4$, i.e. a quasi-perfect linear code that is both 1-error correcting and 2-error detecting.

Interestingly, the points of a complete cap in the finite projective space $PG(s-1,q)$ can be considered as the columns of a parity check matrix of an $[n, n-s, 4]_q 2$-code. Consequently, the problem of constructing small complete caps in a given projective space $PG(s-1,q)$ translates into the language of covering codes as that of constructing quasi-perfect codes with covering radius 2 and small density, as the following result holds.

Proposition 3.70.

$$l(s,2,q)_4 = \min\{n \mid \textit{ there exists a complete cap of size } n \textit{ in } PG(s-1,q)\}. \tag{3.53}$$

This makes it possible to use methods from both Galois Geometries and Algebraic Geometry in order to investigate covering-radius-2 codes with small density.

Here, we are going to discuss some recently obtained upper bounds on $l(s,2,q)_4$ which are valid for arbitrarily large values of q, based on the results of this chapter.

In fact, results on complete caps in projective spaces can be deduced from results on complete caps in affine spaces, and conversely. The affine space $AG(s,q)$ is embedded in the projective space $PG(s,q)$. Also, for any hyperplane $\mathcal{H}_\infty$ of $PG(s,q)$, the affine space obtained by removing the points of $\mathcal{H}_\infty$ is isomorphic to $AG(s,q)$. A complete k-cap C in $PG(s,q)$ can then be viewed as a complete cap in $AG(s,q)$, provided that there exists a hyperplane containing no point of C. Conversely, for any embedding of $AG(s,q)$ in $PG(s,q)$, it is always possible to obtain a complete cap in $PG(s,q)$ from a complete cap of $AG(s,q)$ by adding some points on the hyperplane at infinity. Therefore, taking into account equality (3.53), the following relation holds:

$$l(s+1,2,q)_4 \leq t(AG(s,q)) + L(s,2,q)_4.$$

Here $L(s,2,q)_4$ denotes the maximal length n of a quasi-perfect $[n, n-s, 4]_q 2$-code with codimension s and order q (or, equivalently, the maximal size of a complete cap in $PG(s-1,q)$).

Based on this assumptions and equality (3.53), here we reformulate Theorems 3.20, 3.42 and 3.68 of Chapter 3, translated into the language of codes.

Theorem 3.71. *Let $q = p^h$ with $p > 3$ a prime, $h > 8$. Let $N \equiv 0 \pmod 4$, $N \geq 4$. Let υ_h be the integer in $\{1, \dots, 8\}$ such that $\upsilon_h \equiv h \pmod 8$, and let t_h be the integer in $\{1, \dots, 4\}$ such that $t_h \equiv h \pmod 4$. Assume that $p^{t_h} > 144$. Then*

$$l(N+1,2,q)_4 < \left(2^{p^h - \lfloor(\lceil h/4\rceil - 1)/2\rfloor}\right) q^{\frac{N-2}{2}} + L(N,2,q)_4 \leq$$
$$\leq 2p^{\frac{v_h}{8}} q^{\frac{N}{2}-\frac{1}{8}} + L(N,2,q)_4 \leq 2pq^{\frac{N}{2}-\frac{1}{8}} + L(N,2,q)_4.$$

In particular,

$$l(5,2,q)_4 < 2pq^{\frac{15}{8}} + q^2 + 1.$$

THEOREM 3.72. *Let* $q = p^h$ *with* $p > 3$ *a prime,* $N \equiv 0 \pmod 4$, $N \geq 4$, *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*

$$l(N+1,2,q)_4 < \frac{m_1+m_2}{m}\left(q^{\frac{N}{2}} - q^{\frac{N}{2}-1}\right) + L(N,2,q)_4.$$

In particular,

$$l(5,2,q)_4 < \left(1 + \frac{m_1+m_2}{m}\right) q^2 - \frac{m_1+m_2}{m} q + 1.$$

THEOREM 3.73. *Let* $q = p^h$ *with* $p > 3$ *a prime,* $N \equiv 0 \pmod 4$, $N \geq 4$, *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*

$$l(N+1,2,q)_4 < \Big((m_1+m_2-3)\cdot\frac{q+1}{m} + 3\Big) q^{\frac{N-2}{2}} + L(N,2,q)_4.$$

In particular,

$$l(5,2,q)_4 < \Big(\frac{(m_1+m_2-3)}{m} + 1\Big) q^2 + \Big(\frac{(m_1+m_2-3)}{m} + 3\Big) q + 1.$$

CHAPTER 4

Small complete arcs in $PG(N, q)$

Let $\mathbb{K}$ be the algebraic closure of $\mathbb{F}_q$ and assume that the characteristic of $\mathbb{F}_q$ is $p > 3$. Then let

$$\mathcal{E} : Y^2 - X^3 - AX - B = 0 \tag{4.1}$$

be the elliptic plane curve defined over $\mathbb{F}_q$, with $4A^3 + 27B^2 neq 0$, and denote by G the set of its $\mathbb{F}_q$-rational points. In analogy to the case of singular cubic curves taken into account in Chapter 3, it is possible to define a binary operation $\oplus$ on the set G in such a way that $(G, \oplus)$ is an abelian group having the flex $O = (0 : 0 : 1)$ of the elliptic curve as neutral element. The key property here is that three distinct points are collinear if and only if their sum is equal to O. Any plane elliptic curve defined over $\mathbb{F}_q$ and with at least one $\mathbb{F}_q$-rational point of inflection is projectively equivalent to (4.1).

In this chapter we assume that G is a cyclic group with $G = \mathbb{Z}_m \times K$, for $m > 3$ a prime. This allows us to obtain plane arcs contained in G in a rather easy way. The proof is analogous to that of Proposition 3.1.

Proposition 4.1 ([**80**]). *Any non-trivial coset $S = K \oplus P$ of K in G is an arc.*

The plane arcs of Proposition 4.1 were investigated in [**3, 23, 26, 28, 43, 68, 77, 78**]. For the dimension $N > 2$, infinite families of complete arcs other than the normal rational curve have rarely appeared in the literature so far (see e.g. [**71**, Remark 5], [**20**, Remark 1]), and the natural idea to try to use some kind of lifting methods for plane arcs usually does not work. Here we show how it is possible to obtain arcs in $PG(N, q)$ with $N > 2$, by considering non-trivial cosets of the abelian group of the $\mathbb{F}_q$-rational points of an elliptic curve in the space.

Let $\mathbb{K}(\mathcal{E}) = \mathbb{K}(x, y)$ be the function field of $\mathcal{E}$, with $x, y \in \mathbb{K}(\mathcal{E})$ satisfying $y^2 = x^3 + Ax + B$, and let Φ_N denote the morphism $\mathcal{E} \to PG(N, \mathbb{K})$ defined by

$$\Phi_N = (1 : \phi_1 : \phi_2 : \ldots : \phi_N), \tag{4.2}$$

where $\phi_0, \phi_1, \ldots, \phi_N$ form an $\mathbb{F}_q$-basis of $L((N+1)O)$. From now on, we will assume that this basis is chosen by setting $\phi_0 = 1$ and, for any integer $i = 1, \ldots, N$,

$$\phi_i := \begin{cases} y^j & \text{if } i = 3j - 1,\ j \geq 1\,, \\ xy^j & \text{if } i = 3j + 1,\ j \geq 0\,, \\ x^2y^j & \text{if } i = 3j + 3,\ j \geq 0\,. \end{cases}$$

Note that $\Phi_N(O) = (0:0:\ldots:0:1)$. As Φ_N is a birational map, $\mathcal{X} = \Phi_N(\mathcal{E})$ is an elliptic curve of $PG(N,q)$ and denote by $\bar{G}$ the set of its $\mathbb{F}_q$-rational points. It is possible to consider the abelian group $(\bar{G},\oplus)$ on $\mathcal{X}$, having $\bar{O} = \Phi_N(O)$ as neutral element. We introduce the notation:

- $\bar{K} := \Phi_N(K)$,
- $\bar{P} := \Phi_N(P) \in \bar{G}$, with $P \in G$.

Clearly, Φ_N induces a natural isomorphism from G to $\bar{G}$, and the key property of G naturally extends to $\bar{G}$.

Proposition 4.2. *Let $\bar{P}_1,\ldots,\bar{P}_{N+1} \in \bar{G}$. Then there exists a hyperplane $\mathcal{H}$ of $PG(N,q)$ such that $\bar{P}_i \in \mathcal{H}$, for $i = 1,\ldots,N+1$, if and only if $\bar{P}_1 \oplus \ldots \oplus \bar{P}_{N+1} = \bar{O}$.*

Proof. Let $\mathbb{K}(\mathcal{X})$ denote the rational function field of $\mathcal{X}$ and let $\mathcal{H}$: $F(X_0,\ldots,X_N) = 0$ be the hyperplane of $PG(N,q)$ such that $\bar{P}_i \in \mathcal{H}$, for $i = 1,\ldots,N+1$ by assumption. Let

$$\alpha = \frac{F + I(\mathcal{X})}{X_0 + I(\mathcal{X})} \in \mathbb{K}(\mathcal{X}),$$

where $\mathcal{H}_\infty : X_0 = 0$ is a hyperplane such that $\mathcal{H}_\infty \cap \mathcal{X} = \{\bar{O}\}$. Then

$$div(\alpha) = \bar{P}_1 + \ldots + \bar{P}_{N+1} - (N+1)\bar{O}$$

is the principal divisor associated to α. Consequently, in $Pic^0(\mathcal{X}) := Div_0(\mathcal{X})/\mathcal{P}(\mathcal{X})$,

$$[\bar{P}_1 + \ldots + \bar{P}_{N+1} - (N+1)\bar{O}] = [\bar{P}_1 - \bar{O}] \oplus \ldots \oplus [\bar{P}_{N+1} - \bar{O}] = \bar{O}$$

from which the assertion.
Conversely, let $\mathcal{H}$ be a hyperplane containing $\bar{P}_1,\ldots,\bar{P}_N$. Suppose that $Q \in \mathcal{X}$ is the point such that $\mathcal{H} \cap \mathcal{X} = \{\bar{P}_1,\ldots,\bar{P}_N,\bar{Q}\}$. Then, by the necessary condition, $\bar{P}_1 \oplus \ldots \oplus \bar{P}_N \oplus \bar{Q} = \bar{O}$, and from our hypothesis $\bar{P}_{N+1} = \bar{Q}$ holds. □

Proposition 4.3. *If $(N+1,m) = 1$, then $\Phi_N(S)$ is an arc.*

Proof. By contradiction, assume that $\bar{R}_1,\ldots,\bar{R}_{N+1}$, are distinct points in $\bar{K}$ such that

$$(\bar{R}_1 \oplus \bar{P}) \oplus \ldots \oplus (\bar{R}_{N+1} \oplus \bar{P}) = O.$$

Then in the factor group $\bar{G}/\bar{K}$

$$\bar{K} \oplus (N+1)\bar{P} = \bar{K}$$

holds. This implies $\bar{P} \in \bar{K}$, as $(N+1,m) = 1$; but this is a contradiction. □

Remark 4.4. *In general, the arc $\Phi_N(S)$ of Proposition 4.3 is not complete. By Proposition 4.2, necessary conditions for a subset T of $\bar{G}$ to be a complete arc in* $\mathrm{PG}(N,q)$ *are:*

(i) *the sum of $N+1$ distinct points in T is never zero;*
(ii) *every point in $\bar{G}\setminus T$ is the sum of N distinct points in $\ominus T$.*

In order to find a subset T of $\bar{G}$, satisfying properties (i) and (ii) in Remark 4.4, it is useful to present a general construction of such a subset of a cyclic group $\mathfrak{G}$ of composite orders, as we will see in the next section.

4.1. Maximal k-independent subsets in cyclic groups of composite orders

According to Remark 4.4, in this section we investigate subsets A of a finite abelian group $\mathfrak{G}$ such that the sum of k elements in A is never zero and every element in $\mathfrak{G}\setminus A$ is the sum of $k-1$ elements in A.

For a subset A of a finite abelian group $\mathfrak{G}$ and for an integer $s\geq 1$, let s^A denote the s-fold restricted sumset of A, that is

$$s^\wedge A=\{y_1+\ldots+y_s \mid y_1,\ldots,y_s\in A, y_i\neq y_j \text{ for all } 1\leq i\neq j\leq s\}.$$

Also, let $0^\wedge A=\{0\}$.

Definition 4.5. For an integer $k\geq 3$, a *k-indipendent subset* of $\mathfrak{G}$ is a subset A such that $0\notin k^\wedge A$. An element $g\in\mathfrak{G}\setminus A$ is said to be *covered* by A if $0\in k^\wedge(A\cup\{g\})$, or, equivalently, if $-g\in(k-1)^\wedge A$. If every element in $\mathfrak{G}\setminus A$ is covered by A then A is said to be a *maximal* k-indipendent subset.

Remark 4.6. *Note that the condition $0\notin k^\wedge A$ precisely means that the sum of k pairwise distinct elements of A is always different from 0, whereas $0\in k^\wedge(A\cup\{g\})$ holds if and only if there exist $k-1$ pairwise distinct elements of A having sum equal to $-g$.*

The proof of the following statement is straightforward.

Lemma 4.7. *Let A be a k-indipendent subset of a finite abelian group $\mathfrak{G}$. If n is the number of elements not covered by A, then there exists a maximal k-independent subset of $\mathfrak{G}$ containing A with at most $|A|+n$ elements.*

4.1.1. Pre-independent Subsets of $\mathbb{Z}_m$.

In [**68**] Szőnyi described a particular construction of a maximal 3-independent subset of an abelian group $\mathfrak{G}$ beeing the direct product of two non-elementary abelian 3-groups A and B (see Theorem 2.20 in Section 2.4). The natural idea is that of trying to extend this construction to maximal k-independent subsets. Unfortunately, the naive modification

$$(4.3)\quad T_1=\{(a,x)|x\in B, x\neq-(k-1)b\},\qquad T_2=\{(y,b)|y\in A, y\neq-(k-1)a\}.$$

does not work, since $\overline{T}=T_1\cup T_2$ is not k-independent. In order to overcome this difficulty, the notion of a pre-independent subset of a cyclic group $\mathbb{Z}_m$ is introduced.

Definition 4.8. For an integer $k \geq 4$, a subset A of $\mathbb{Z}_m$ is said to be *k-pre-independent* if

$$(k-\ell) \notin \ell^\wedge A \text{ for every } \ell = 1, \dots, k-2.$$

We show that k-pre-independent subsets of $\mathbb{Z}_m$ give rise to k-independent subsets of groups $\mathfrak{G} = \mathbb{Z}_m \times H$, with H not elementary k-abelian and m a prime.

Proposition 4.9. *Let $4 \leq k < m$, with m a prime, and let $\mathfrak{G} = \mathbb{Z}_m \times H$, with H not elementary k-abelian. For a k-pre-independent subset A of $\mathbb{Z}_m$, and for an element $b \in H$ such that* $\mathrm{ord}(b) > k$, *let*

$$T_1 = \{(-1, x) | x \in H, x \neq -(k-1)b\}, \quad T_2 = \{(y, b) | y \in A\}.$$

Then $T_A := T_1 \cup T_2$ is a k-independent subset of $\mathfrak{G}$.

Proof. Let $R \in k^\wedge T_A$. Then $R = P_1 + \dots + P_{k-\ell} + Q_1 + \dots + Q_\ell$ for some $0 \leq \ell \leq k$, and for pairwise distinct elements $P_1, \dots, P_{k-\ell} \in T_1$ and $Q_1, \dots, Q_\ell \in T_2$. Then,

$$R = \left(\ell - k + \sum_{i=1}^{\ell} y_i, \ell b + \sum_{i=1}^{k-\ell} x_i\right),$$

with $y_i \in A$ and $x_i \in H \setminus \{-(k-1)b\}$. We prove that $R \neq 0$. If either $\ell = 0$ or $\ell = k$ this follows from $-k \neq 0 \neq kb$. When $\ell = k-1$, the condition is implied by $x_1 \neq -(k-1)b$. Finally, A being k-pre-independent ensures $\ell - k + \sum_{i=1}^{\ell} y_i \neq 0$ for each $\ell \in [1, \dots, k-2]$. □

This section is devoted to the construction and the investigation of k-pre-independent subsets of groups $\mathbb{Z}_m$. Let m be a prime and let $k \geq 4$ be an integer with $m > \max\{\frac{(k-2)^3}{2}, \frac{3k^2-k-12}{2}\}$. Let

$$A := A_1 \cup A_2 \cup \{0\} \subset \mathbb{Z}_m$$

with

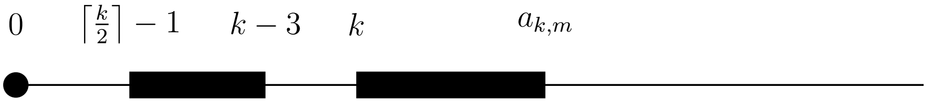
$$A_1 := \{\lceil k/2 \rceil - 1, \lceil k/2 \rceil, \dots, k-3\}, \qquad A_2 := \{k, k+1, \dots, a_{k,m}\}, \tag{4.4}$$

where $a_{k,m}$ denotes the maximum integer such that

$$\sum_{i=0}^{k-3} (a_{k,m} - i) \leq m+1. \tag{4.5}$$

(see Figure 1).

Figure 1. The set A



It is straightforward to check that

$$a_{k,m} = \left\lfloor \frac{m+1}{k-2} + \frac{k-3}{2} \right\rfloor .$$

Proposition 4.10. *The set A is a k-pre-independent subset of $\mathbb{Z}_m$.*

Proof. Clearly both $(k-1) \notin 1^\wedge A$ and $(k-2) \notin 1^\wedge A$ hold. For an integer ℓ with $3 \leq \ell \leq k-2$, let s be an element in $\ell^\wedge A$. Then it is easily seen that

$$k-1 \leq s \leq m+1,$$

and hence $(k-\ell) \in \{2, \ldots, k-3\}$ cannot be equivalent to s mod m. □

Next we determine what elements z of $\mathbb{Z}_m$ can be written as the difference of the integer $k-1-j$ and the sum of j pairwise distinct elements of A, for some $j = 0, \ldots, k-3$. This is needed in order to investigate the number of elements of $\mathfrak{G}$ that are covered by the k-independent subset T_A constructed from A in Proposition 4.16. The more z's satisfy the above request, the more elements are covered by the k-independent subset. The proof of the following Proposition does not involve deep mathematical concepts, but unfortunately requires a large number of straightforward inequalities.

Proposition 4.11. *Let m be a prime and let $k \geq 4$ be an integer with $m > \max\{\frac{(k-2)^3}{2}, \frac{3k^2-k-12}{2}\}$. Let $A := A_1 \cup A_2 \cup \{0\} \subset \mathbb{Z}_m$, with A_i as in (4.4). Then the set*

$$\tilde{A} := \bigcup_{j=0}^{k-3} \Big((k-1-j) - j^\wedge A \Big)$$

contains all the integers in

$$\left[0, k - \left\lceil \frac{k}{2} \right\rceil - 1\right] \bigcup [k-2, k-1] \bigcup \left[m + 2 - (k-3)\left(a_{k,m} - \frac{k-4}{2}\right), m-2\right]$$

for $k \geq 5$, whereas for $k = 4$

$$\tilde{A} = \{1, 2, 3, (m+3)/2, \ldots, m-3, m-2\}.$$

Proof. Assume first that $k \geq 5$. Note that $\{k-1, k-2\} \in \tilde{A}$ since

$$k-1 \in (k-1) - 0^\wedge A \text{ and } k-2 \in (k-2) - 1^\wedge A.$$

The set $2^\wedge A$ contains all the integers in the intervals

$$[\lceil k/2 \rceil - 1, \ldots, k-3], \quad [k, \ldots, a_{k,m}], \quad [2k+1, \ldots, 2a_{k,m} - 1].$$

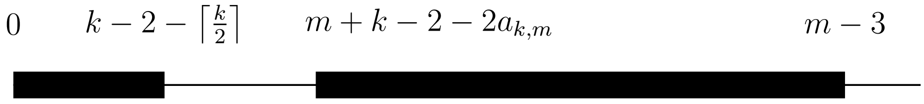
Note that $m > \max\{\frac{(k-2)^3}{2}, \frac{3k^2-k-12}{2}\}$ implies $a_{k,m} > 2k$. Therefore,

$$A_1 \cup \{k, \ldots, 2a_{k,m} - 1\} \subseteq 2^\wedge A,$$

and hence (see also Figure 2)

$$(4.6)\ \ (k-3)-2^{\wedge}A \supseteq \{m+k-2-2a_{k,m},\dots,m-3\} \cup \left\{0,1,\dots,k-2-\left\lceil\frac{k}{2}\right\rceil\right\}.$$

Figure 2. Subset of $(k-3)-2^{\wedge}A$



Next we show that

$$\left\{2a_{k,m}+4-k,\dots,\sum_{i=0}^{k-4}(a_{k,m}-i)\right\} \subseteq (k-3)^{\wedge}A. \tag{4.7}$$

It is easy to see that

$$(k-3)^{\wedge}A_2 = \left\{\sum_{i=0}^{k-4}(k+i),\dots,\sum_{i=0}^{k-4}(a_{k,m}-i)\right\} \subseteq (k-3)^{\wedge}A. \tag{4.8}$$

Let $b_{k,m}$ be the sum of the $(k-3)$ distinct integers $a \in A$ such that $a \leq \left(\lceil\frac{k}{2}\rceil + k - 4\right)$. Then

$$b_{k,m} = (k-2)\left(\left\lceil\frac{k}{2}\right\rceil + \frac{k-7}{2}\right) - 1.$$

From $m > \frac{3k^2-k-12}{2}$ it follows that $a_{k,m} > 2k$, and hence it is easily seen that $(k-3)^{\wedge}A$ contains all the integers in the interval

$$\left[b_{k,m}, \left\lceil\frac{k}{2}\right\rceil - 1 + \sum_{i=0}^{k-5}(a_{k,m}-i)\right].$$

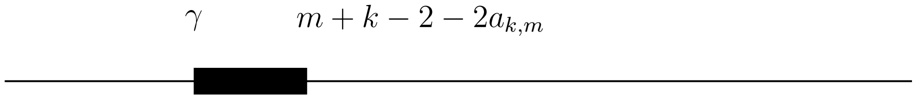
Note that

$$\left\lceil\frac{k}{2}\right\rceil - 1 + \sum_{i=0}^{k-5}(a_{k,m}-i) \geq \sum_{i=0}^{k-4}(k+i).$$

Also, from $m > \frac{(k-2)^3}{2}$ it follows $b_{k,m} \leq 2a_{k,m}+4-k$, and hence, taking into account (4.8), we have that (4.7) holds. Therefore (see also Figure 3),

$$2-(k-3)^{\wedge}A \supseteq \left\{\gamma = m+2-(k-3)\left(a_{k,m}-\frac{k-4}{2}\right),\dots,m+2-(2a_{k,m}+4-k)\right\}.$$

Figure 3. Subset of $2-(k-3)^{\wedge}A$



Taking into account (4.6), it follows that

$$\tilde{A} \supseteq \left\{ m + 2 - (k-3)\left(a_{k,m} - \frac{k-4}{2}\right), \dots, m-3 \right\}.$$

To complete the proof it is enough to note that (see also Figure 4)

$$(k-2) - 1^\wedge A = k - 2 - A \supseteq \left\{ 1, \dots, k - \left\lceil \frac{k}{2} \right\rceil - 1 \right\} \bigcup \{m - a_{k,m} + k - 2, \dots, m-2\}.$$

The above information is summarized in Figure 4.

Figure 4. Subset of $(k-2) - 1^\wedge A$

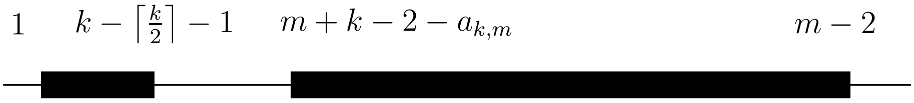
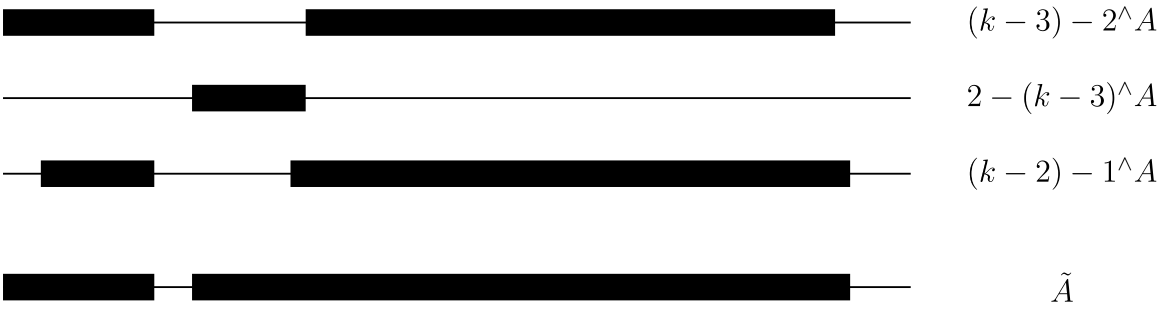


Figure 5. Subset of $\tilde{A}$



When $k = 4$,

$$A = \{0, 1, 4, \dots, (m+1)/2\},$$

and the proof of (ii) is straightforward. In fact,

$$(k-2) - 1^\wedge A \supseteq \{1 = 2 - 1, 2 = 2 - 0, (m+3)/2, \dots, m-3, m-2\},$$

and

$$(k-1) - 0^\wedge A = \{3\}.$$

□

In the following we also study the sets $1 - (k-2)^\wedge A$ and $-(k-1)^\wedge A$; this information will be used in Proposition 4.16.

Proposition 4.12. *Let A be as in Proposition* 4.11. *Then the set*

$$1-(k-2)^\wedge A$$

contains all the integers in the interval

$$\left[m+1-\sum_{i=0}^{k-3}(a_{k,m}-i), m+1-(k-3)\left(a_{k,m}-\frac{k-4}{2}\right)\right].$$

for $k \geq 5$, whereas for $k=4$

$$1-2^\wedge A=\{0,1,\ldots,m-3\}.$$

Proof. The proof for $k=4$ is straightforward. Assume then that $k \geq 5$. Clearly

$$\left\{\sum_{i=0}^{k-3}(k+i),\ldots,\sum_{i=0}^{k-3}(a_{k,m}-i)\right\} \subseteq (k-2)^\wedge A,$$

whence $1-(k-2)^\wedge A$ contains all the integers in the interval

$$\left[m+1-\sum_{i=0}^{k-3}(a_{k,m}-i), m+1-\sum_{i=0}^{k-3}(k+i)\right].$$

The claim then follows from

$$\sum_{i=0}^{k-3}(k+i)=(k-2)\left(k+\frac{k-3}{2}\right) \leq (k-3)\left(a_{k,m}-\frac{k-4}{2}\right).$$

□

Proposition 4.13. *Let A be as in Proposition* 4.11. *Then the set $-(k-1)^\wedge A$ contains -1.*

Proof. We need to show that $1 \in (k-1)^\wedge A$. Note that every integer in

$$I:=[(k-1)(3k-2)/2, \sum_{i=0}^{k-2}(a_{k,m}-i)]$$

belongs to $(k-1)^\wedge A_2 \subseteq (k-1)^\wedge A$. By definition, $\sum_{i=0}^{k-3}((a_{k,m}+1)-i) > m+1$. Also, $a_{k,m} \geq 2k-5$ is implied by $m>(k-2)^3/2$. Therefore,

$$\sum_{i=0}^{k-2}(a_{k,m}-i)=\sum_{i=0}^{k-3}(a_{k,m}-i)+(a_{k,m}-(k-2)) \geq k-3+\sum_{i=0}^{k-3}(a_{k,m}-i) \geq m+1.$$

On the other hand, $m>(k-2)^3/2$ yields

$$(k-1)(3k-2)/2 \leq m+1,$$

whence

$$1 \in I.$$

□

Finally, we summarize the information on A in the following corollary.

COROLLARY 4.14. *Let A and $\tilde{A}$ be as in Proposition 4.11. Then*

(i) *the size of $\mathbb{Z}_m \setminus (\tilde{A} \cup \{-1\})$ is at most $\frac{m+1}{k-2} - 1$;*
(ii) *the size of $\mathbb{Z}_m \setminus (\tilde{A} \cup (1-(k-2)^\wedge A) \cup \{-1\})$ is at most $\lceil k/2 \rceil - 2$.*

PROOF. Let

$$I := \left\{1, \dots, k - \left\lceil \frac{k}{2} \right\rceil - 1\right\} \cup \{k-2, k-1\} \cup \left\{m + 2 - (k-3)\left(a_{k,m} - \frac{k-4}{2}\right), \dots, m-1\right\}$$

and

$$I' = \left\{0, k - \left\lceil \frac{k}{2} \right\rceil - 1\right\} \cup \{k-2, k-1\} \cup \left\{m + 1 - (k-2)\left(a_{k,m} - \frac{k-3}{2}\right), \dots, m-1\right\}.$$

By Propositions 4.11 and 4.12 we have $I \subseteq \tilde{A}$ and $I' \subseteq (\tilde{A} \cup (1-(k-2)^\wedge A) \cup \{-1\})$.

(i) Let

$$c_{k,m} := m + 1 - (k-3)\left(a_{k,m} - \frac{k-4}{2}\right).$$

The set $\mathbb{Z}_m \setminus I$ contains $\mathbb{Z}_m \setminus \tilde{A}$ and consists of 0 together with the non-negative integers x with

$$k - \left\lceil \frac{k}{2} \right\rceil \leq x \leq c_{k,m}, \qquad x \notin \{k-1, k-2\}.$$

By definition of $a_{k,m}$ we have

$$c_{k,m} \leq \frac{k-3}{2} + \frac{m+1}{k-2},$$

whence the assertion.

(ii) The proof is analogous to that of (ii). Here I is replaced by I', and the claim follows from

$$m - (k-2)\left(a_{k,m} - \frac{k-3}{2}\right) \leq k-3.$$

□

4.1.2. Maximal k-independent subsets. Throughout this section $\mathfrak{G} = \mathbb{Z}_m \times H$ is a cyclic group, with m a prime, and $k \geq 4$ is an integer such that $m > \max\{\frac{(k-2)^3}{2}, \frac{3k^2-k-12}{2}\}$. We first prove an elementary result for which we could not find a reference.

LEMMA 4.15. *Assume that $|H| \geq \max\{7, k+3\}$. Let $B := H \setminus \{h_0\}$ for some $h_0 \neq 0$. Then $\ell^\wedge B = H$ for each $\ell = 2, \dots, k-1$.*

PROOF. Let $B' = B \setminus \{0\}$. Then clearly both $\ell^\wedge B' \subseteq \ell^\wedge B$ and $\ell^\wedge B' \subseteq (\ell+1)^\wedge B$ hold. For each h in H, there exist at most 2 elements $b \in B'$ with $h = 2b$, and at most other two elements $b' \in B'$ such that $h - b' \notin B'$. Since $|H| > 6$, we have that $2^\wedge B' = H$, whence the claim for $\ell = 2$. Assume that $\ell > 2$ is even. For each $h \in H$ there exist distinct $h_1, h_2 \in B'$ with $h_1 + h_2 = h$. Since $|B'| \geq k+1 > \ell$, and since there is at most one involution in B', it is possible to choose $(\ell-2)/2$ distinct elements $a_1, \ldots, a_{(\ell-2)/2} \in B' \setminus \{\pm h_1, \pm h_2\}$ such that $2a_i \neq 0$, $a_i \neq -a_{i'}$ for $i \neq i'$. Then

$$h = h_1 + h_2 + a_1 + \ldots + a_{(\ell-2)/2} + (-a_1) + \ldots + (-a_{(\ell-2)/2}) \in \ell^\wedge B'.$$

Whence $H = \ell^\wedge B' = \ell^\wedge B$. The claim for ℓ odd follows from $\ell^\wedge B' \subseteq (\ell+1)^\wedge B$. □

This proposition shows the connection between k-pre-independent subsets of $\mathbb{Z}_m$ introduced in the previous section and k-independent subsets in $\mathfrak{G}$.

PROPOSITION 4.16. *Let $4 \leq k < m$. For a k-pre-independent subset A of $\mathbb{Z}_m$, let*

$$\tilde{A} = \bigcup_{j=0}^{k-3} (k-1-j) - j^\wedge A.$$

For an element $b \in H$ such that $\operatorname{ord}(b) > k$ *let*

$$T_1 = \{(-1, x) | x \in H, x \neq -(k-1)b\} \quad T_2 = \{(y, b) | y \in A\}. \tag{4.9}$$

Then

(i) $T_A := T_1 \cup T_2$ *is a k-independent subset of $\mathfrak{G}$;*
(ii) *every element in*

$$\Big\{(\alpha,\beta)|\alpha \in \tilde{A}, \beta \in H\Big\} \bigcup \{(\alpha,\beta)|\alpha \in 1-(k-2)^\wedge A, \beta \in H \setminus \{b\}\} \bigcup \{(-1, -(k-1)b)\} \tag{4.10}$$

is covered by T_A.

PROOF. (i) This is Proposition 4.9.

(ii) We first prove that $(-1, -(k-1)b)$ is covered by T_A. By Proposition 4.13, there exist distinct $y_1, \ldots, y_{k-1} \in A$ with

$$-1 = -(y_1 + \ldots + y_{k-1}),$$

whence

$$(-1, -(k-1)b) + \sum_{i=1}^{k-1} (y_i, b) = (0,0).$$

Consider an element $(\alpha, \beta) \in \mathfrak{G} \setminus T_A$, with $\alpha \in \tilde{A}$. Then there exist pairwise distinct $y_1, \ldots, y_j \in A$ such that $y_1 + \cdots + y_j = (k-1-j) - \alpha$, for some $j = 0, \ldots, k-3$.

If $j > 0$ then $2 \leq k-1-j \leq k-2$ and hence by Lemma 4.15 it is possible to find pairwise distinct $x_1, \ldots, x_{k-1-j} \in H \backslash \{-(k-1)b\}$ such that $x_1 + \ldots + x_{k-1-j} = -\beta - jb$. Then

$$(\alpha, \beta) + \sum_{i=1}^{k-1-j} (-1, x_i) + \sum_{i=1}^{j} (y_i, b) = (0,0)$$

and (α, β) is covered by T_A.

If $j = 0$ then $\alpha = 1-k$; again by Lemma 4.15 there exist distinct $x_1, \ldots, x_{k-1} \in H \setminus \{-(k-1)b\}$ such that $x_1 + \ldots + x_{k-1} = -\beta$, and hence

$$(1-k, \beta) + (-1, x_1) + \ldots + (-1, x_{k-1}) = (0,0).$$

Assume now that $(\alpha, \beta) \in \mathfrak{G} \setminus T_A$, with $\alpha \in 1-(k-2)\hat{}A$, $\beta \in H \setminus \{b\}$. Then there exist pairwise distinct $y_1, \ldots, y_{k-2} \in A$ such that $y_1 + \cdots + y_{k-2} = 1 - \alpha$. The element $x = -\beta - (k-2)b$ is different from $(-(k-1)b)$ as $\beta \neq b$, whence $(-1, x) \in T_1$. Clearly,

$$(\alpha, \beta) + (-1, x) + \sum_{i=1}^{k-2} (y_i, b) = (0,0)$$

holds. □

Finally, we prove the existence of a maximal k-independent subset in $\mathfrak{G}$ of small size. Also, Proposition 4.17(ii) is a technical request which will be used in the construction of small complete arcs in Section 4.2.

Proposition 4.17. *Let $k \geq 4$ and m be a prime with $m > \max\{\frac{(k-2)^3}{2}, \frac{3k^2-k-12}{2}\}$. For A as in Proposition 4.11, let T_1, T_2, T_A be as in Proposition 4.16. Then*

(i) *there exists a maximal k-independent subset of $\mathbb{Z}_m \times H$ containing T_A of size at most*

$$|A| + (\lceil k/2 \rceil - 1)(|H| - 1) + \frac{m+1}{k-2} - 1;$$

(ii) *there exist pairwise distinct elements $P_1, \ldots, P_{k-4}, Q_1, Q_2, Q_3 \in T_2$ such that for each $R \in T_1 \cup \{(-1, -(k-1)b)\}$ and for each $i = 1, 2, 3$,*

$$3R + P_1 + \ldots + P_{k-4} + Q_i \neq (0,0).$$

Proof. Note that the only element of type $(-1, \beta)$ not belonging to T_A is $(-1, -(k-1)b)$; it is covered by T_A by Proposition 4.16. Then by Corollary 4.14 and Proposition 4.16 the number of elements in $\mathbb{Z}_m \times H$ that are not covered by T_A is at most $(\lceil k/2 \rceil - 2)|H| + \frac{m+1}{k-2} - 1 - (\lceil k/2 \rceil - 2)$. Therefore, by Lemma 4.7 there exists a maximal k-independent subset of $\mathbb{Z}_m \times H$ containing T_A of size at most

$$(|H| - 1) + |A| + (\lceil k/2 \rceil - 2)|H| + \frac{m+1}{k-2} - 1 - (\lceil k/2 \rceil - 2).$$

Then (i) follows from straightforward computation.

In order to prove (ii), fix pairwise distinct $y_1, \ldots, y_{k-4} \in A$ and for each $i = 1, 2, 3$ choose $\tilde{y}_i \in A$ such that

$$(y_1 + \ldots + y_{k-4}) + 3 \neq -\tilde{y}_i.$$

Let $P_i = (y_i, b)$ for $i = 1, \ldots, k-4$, and $Q_i = (\tilde{y}_i, b)$ for $i = 1, 2, 3$. Note that for each $R \in T_1 \cup \{(-1, -(k-1)b)\}$, the element $-3R$ is $(-3, -3x)$ for some $x \in H$. Then clearly $3R + P_1 + \ldots + P_{k-4} + Q_i \neq 0$ for each $i = 1, 2, 3$. □

4.2. The construction

This section is devoted to the construction of a complete arc containing the set T of Remark 4.4.

We keep the notation at the beginning of Chapter 4. The following result can be obtained by applying Proposition 4.17 to the case $\mathfrak{G} = \bar{G}$, $H = \Phi_N(K)$, $k = N+1$.

Proposition 4.18. *Assume that* $m > \max\{\frac{(N-1)^3}{2}, \frac{3N^2+5N-10}{2}\}$. *Then*

i) *there exists a maximal* $(N+1)$*-independent subset* T *of* $\bar{G}$ *containing* $\Phi_N(S \setminus \{P\})$ *whose size is at most*

$$(\lceil (N+1)/2 \rceil - 1)(|S| - 1) + 2\frac{m+1}{N-1} - \frac{3}{2};$$

ii) *there exist* $\bar{P}_1, \ldots, \bar{P}_{N-3}$, $\bar{Q}_1$, $\bar{Q}_2$, $\bar{Q}_3 \in T \setminus \Phi_N(S)$ *such that for each* R *in* S *and for each* $i = 1, 2, 3$,

$$3\bar{R} \oplus \bar{P}_1 \ldots \oplus \bar{P}_{N-3} \oplus \bar{Q}_i \neq \bar{O}.$$

Henceforth, T, $\bar{P}_1, \ldots, \bar{P}_{N-3}$, $\bar{Q}_1$, $\bar{Q}_2$, $\bar{Q}_3$ are as in Proposition 4.18. For $i = 1, 2, 3$, let W_i be the subspace generated by $\bar{P}_1, \ldots, \bar{P}_{N-3}$, $\bar{Q}_i$. Note that $\dim(W_i) = N - 3$. Fix a plane σ_i such that $W_i \cap \sigma_i = \emptyset$.

For $i = 1, 2, 3$, consider the projections

$$\begin{array}{rcl} \pi_i : \mathcal{X} \setminus W_i & \longrightarrow & \sigma_i \\ \bar{U} & \longmapsto & < W_i, \bar{U} > \cap \sigma_i, \end{array}$$

from W_i onto the plane σ_i, and denote by $\psi_i := \pi_i \circ \Phi_N : \mathcal{E} \to PG(2, q)$ the composition of π_i and Φ_N.

Next section is devoted to the proof of the following result, which is needed in order to apply Proposition 2.23 to the elliptic curve $\psi_i(\mathcal{E})$.

Proposition 4.19. *The curve* $\psi_i(\mathcal{E})$ *has an* $\mathbb{F}_q$*-rational inflection point.*

4.2.1. Existence of a rational inflection point for $\psi_i(\mathcal{E})$. Set $\psi := \psi_i$, $\sigma := \sigma_i$, $\pi := \pi_i$, $W := W_i$, $\bar{Q} := \bar{Q}_i$, for $i = 1, 2, 3$. Without loss of generality assume that σ has equations

$$\sigma : \begin{cases} X_{i_1} = 0 \\ \vdots \\ X_{i_{N-2}} = 0 \end{cases} \qquad i_j \in \{0, \ldots, N\}.$$

For the sake of simplicity, assume also $i_j = j + 2$ whence $(X_0 : X_1 : X_2)$ are homogeneous coordinates for the plane σ. For $j = 0, 1, 2$, let $W^{(j)} =< W, r_j >$ be the hyperplane generated by W and the line $r_j : X_j = 0, X_3 = 0, \ldots, X_N = 0$. Also, set $R_0 = r_0 \cap r_1$, $R_1 = r_1 \cap r_2$, $R_2 = r_0 \cap r_2$. Note that

$$W = \bigcap_{j=0,1,2} W^{(j)}. \tag{4.11}$$

Assume that $L_j(X_0, \ldots, X_N) = 0$ is an equation of $W^{(j)}$.

Lemma 4.20. *Let $\bar{U}$ be an affine point of $\mathcal{X} \setminus W$. Then*

$$\pi(\bar{U}) = (L_0(\bar{U}) : L_1(\bar{U}) : L_2(\bar{U})).$$

Proof. If $\pi(\bar{U}) = R_j$ for some $j = 1, 2, 3$, then without loss of generality we can assume that $\pi(\bar{U}) = R_0$. Consequently $\bar{U} \in W^{(1)} \cap W^{(2)}$, which implies $L_1(\bar{U}) = L_2(\bar{U}) = 0$ and $L_0(\bar{U}) \neq 0$.
Otherwise, $\bar{U} = \eta\bar{R}_0 + \epsilon\bar{R}_1 + \lambda\bar{R}_2$, where $\pi(\bar{R}_j) = R_j$; thus, by the previous case

$$\pi(\bar{U}) = \pi(\eta\bar{R}_0 + \epsilon\bar{R}_1 + \lambda\bar{R}_2) = \eta\pi(\bar{R}_0) + \epsilon\pi(\bar{R}_1) + \lambda\pi(\bar{R}_2) =$$

$$= \eta(L_0(\bar{R}_0) : L_1(\bar{R}_0) : L_2(\bar{R}_0)) + \epsilon(L_0(\bar{R}_1) : L_1(\bar{R}_1) : L_2(\bar{R}_1)) + \lambda(L_0(\bar{R}_2) : L_1(\bar{R}_2) : L_2(\bar{R}_2)) =$$

$$= (\eta L_0(\bar{R}_0) + \epsilon L_0(\bar{R}_1) + \lambda L_0(\bar{R}_2) : \eta L_1(\bar{R}_0) + \epsilon L_1(\bar{R}_1) + \lambda L_1(\bar{R}_2) : \eta L_2(\bar{R}_0) + \epsilon L_2(\bar{R}_1) + \lambda L_2(\bar{R}_2)) =$$

$$= (L_0(\eta\bar{R}_0 + \epsilon\bar{R}_1 + \lambda\bar{R}_2) : L_1(\eta\bar{R}_0 + \epsilon\bar{R}_1 + \lambda\bar{R}_2) : L_2(\eta\bar{R}_0 + \epsilon\bar{R}_1 + \lambda\bar{R}_2)).$$

□

The rational map ψ has coordinates $\psi = (L_0(1, x, y, \ldots) : L_1(1, x, y, \ldots) : L_2(1, x, y, \ldots))$. Let $\bar{R} \in \bar{G}$ be such that $-3\bar{R} = \bar{P}_1 \oplus \ldots \bar{P}_{N-3} \oplus \bar{Q}$. Then, by Proposition 4.2, there exists a linear polynomial $f_{\bar{R}}(X_0, \ldots, X_N)$ such that the zero divisor of $f_{\bar{R}}(1, \phi_1, \phi_2, \ldots, \phi_N)$ is

$$(f_{\bar{R}}(1, \phi_1, \phi_2, \ldots, \phi_N))_0 = 3\bar{R} + \bar{P}_1 + \ldots + \bar{P}_{N-3} + \bar{Q}. \tag{4.12}$$

Also, by Proposition 4.18,

$$R \notin S. \tag{4.13}$$

Lemma 4.21. *There exists $j \in \{0, 1, 2\}$ such that $\bar{R} \notin W^{(j)}$.*

Proof. Assume on the contrary that $\bar{R} \in W^{(0)} \cap W^{(1)} \cap W^{(2)}$. Then $\bar{R} \in W$ by (4.11). Let $\bar{S}_0$ be a point in $\mathcal{X} \setminus W$. Then $T_1 =< W, \bar{S}_0 >$ is such that $\dim(T_1) = N - 2$. If $\bar{S}_1, \bar{S}_2$ are two distinct points in $\mathcal{X} \setminus T_1$, then $Z_1 =< T_1, \bar{S}_1 >$ and $Z_2 =< T_2, \bar{S}_2 >$ are two different hyperplanes. Thus, by Proposition 4.2,

$$\bar{P}_1 \oplus \ldots \oplus \bar{P}_{N-3} \oplus \bar{Q} \oplus \bar{R} \oplus \bar{S}_0 \oplus \bar{S}_1 = \bar{O},$$

$$\bar{P}_1 \oplus \ldots \oplus \bar{P}_{N-3} \oplus \bar{Q} \oplus \bar{R} \oplus \bar{S}_0 \oplus \bar{S}_2 = \bar{O},$$

from which $\bar{S}_1 = \bar{S}_2$, a contradiction. □

From now on, assume that $\bar{R} \notin W^{(0)}$ and let

$$u = \frac{X_1 + I(\psi(\mathcal{E}))}{X_0 + I(\psi(\mathcal{E}))}, \quad v = \frac{X_2 + I(\psi(\mathcal{E}))}{X_0 + I(\psi(\mathcal{E}))}$$

be the rational functions of the affine coordinates of the plane σ. So, let $\mathbb{K}(u, v)$ be the rational function field of the curve $\psi(\mathcal{E})$ and $\psi^* : \mathbb{K}(u, v) \to \mathbb{K}(\mathcal{E})$ denote the pullback of ψ. Let

$$\xi_j = L_j(1, \phi_1, \phi_2, \ldots, \phi_N), \quad j = 0, 1, 2. \tag{4.14}$$

Then clearly

$$\psi^*(u) = \frac{L_1(1, \phi_1, \phi_2, \ldots, \phi_N)}{L_0(1, \phi_1, \phi_2, \ldots, \phi_N)} = \frac{\xi_1}{\xi_0}, \tag{4.15}$$

$$\psi^*(v) = \frac{L_2(1, \phi_1, \phi_2, \ldots, \phi_N)}{L_0(1, \phi_1, \phi_2, \ldots, \phi_N)} = \frac{\xi_2}{\xi_0}. \tag{4.16}$$

Proposition 4.22. *Let $R = \Phi_N^{-1}(\bar{R})$, then $\psi(R)$ is an $\mathbb{F}_q$-rational inflection point of $\psi(\mathcal{E})$.*

Proof. In order to show that $\psi(R)$ is an inflection point for $\psi(\mathcal{E})$ we need to show that a linear function in u, v has valuation equal to 3 at $\psi(R)$. Note that $W \subseteq \mathcal{H}_{\bar{R}} : f_{\bar{R}}(X_0, \ldots, X_N) = 0$ by construction and $\pi(\mathcal{H}_{\bar{R}})$ is a line of equation

$$\lambda L_0(X_0, \ldots, X_N) + \epsilon L_1(X_0, \ldots, X_N) + \eta L_2(X_0, \ldots, X_N) = 0.$$

Denote by β the rational function associated to $\pi(\mathcal{H}_{\bar{R}})$; thus

$$\beta = \lambda L_0(1, \phi_1, \phi_2, \ldots, \phi_N) + \epsilon L_1(1, \phi_1, \phi_2, \ldots, \phi_N) + \eta L_2(1, \phi_1, \phi_2, \ldots, \phi_N).$$

Taking into account (4.14),

$$\beta = \lambda \xi_0 + \epsilon \xi_1 + \eta \xi_2 = \xi_0 \left(\lambda + \epsilon \frac{\xi_1}{\xi_0} + \eta \frac{\xi_2}{\xi_0} \right).$$

As Φ_N is a birational map, $v_R(\beta) = v_{\bar{R}}(\Phi_N^{*-1}(\beta)) = 3$ by (4.12); also, as ψ is a birational map, from $\bar{R} \notin W^{(0)}$ and taking into account (4.15)-(4.16), it follows

$$3 = v_R(\beta) = v_R(\xi_0) + v_R \left(\lambda + \epsilon \frac{\xi_1}{\xi_0} + \eta \frac{\xi_2}{\xi_0} \right) = v_R \left(\lambda + \epsilon \frac{\xi_1}{\xi_0} + \eta \frac{\xi_2}{\xi_0} \right) =$$

$$= v_{\psi(R)}\left(\psi^{*-1}\left(\lambda + \epsilon\frac{\xi_1}{\xi_0} + \eta\frac{\xi_2}{\xi_0}\right)\right) = v_{\psi(R)}(\lambda + \epsilon u + \eta v).$$

In conlusion $\lambda + \epsilon u + \eta v$ is a linear function whose valuation at $\psi(R)$ is equal to 3. □

4.2.2. Complete Arcs in $PG(N, q)$. Let $(\tilde{G}, \oplus)$ be the abelian group on the set of the $\mathbb{F}_q$-rational points of $\psi_i(\mathcal{E})$, having as neutral element $O_{\psi_i(\mathcal{E})} := \psi_i(R)$, for $i = 1, 2, 3$, where R is uniquely determined in Section 4.2.1. Let $\tilde{\psi_i}$ be the following map

$$\begin{array}{ll} \tilde{\psi_i} : \mathcal{E} & \to PG(2, q) \\ \quad P & \mapsto \tilde{\psi_i}(P) := \psi_i(P \oplus R); \end{array}$$

then $\tilde{\psi_i}(O) = \psi_i(R)$ and consequently, $\tilde{\psi_i}$ is a birational map and also an isogeny.

Let S be as in Proposition 4.1; note that by (4.13), $S \ominus R$ is a coset that does not contain the neutral element $O \in \mathcal{E}$. Thus, the following Proposition holds.

Proposition 4.23. *The set $\tilde{\psi_i}(S \ominus R) = \psi_i(S)$ is an arc, for $i = 1, 2, 3$.*

Consequently, $\psi_i(S \setminus \{P\})$ is an arc as well and, by [**3**, Theorem 4], the following assertion holds.

Theorem 4.24. *Under the assumptions of Propositions* 2.23 *and* 4.18*, let T be as in Proposition* 4.18*. Then a complete arc in $PG(N, q)$ can be obtained from T by adding at most $N - 1$ points. In particular, there exists a complete arc in $PG(N, q)$ of size at most*

$$(\lceil (N + 1)/2 \rceil - 1)(|S| - 1) + 2\frac{m + 1}{N - 1} + N - \frac{5}{2}.$$

Proof. As T is a maximal $(N + 1)$-independent subset, every point in $\mathcal{X} \setminus T$ belongs to some hyperplane generated by N points of T.

Let D be a point off $\mathcal{X}$. If there exists $\bar{i} \in \{1, 2, 3\}$ such that $\pi_{\bar{i}}(D) \notin \psi_{\bar{i}}(\mathcal{E})$ then, by a consequence of Proposition 2.23 applied to the arc $\psi_{\bar{i}}(S \setminus \{P\})$, there exist two points V_1, $V_2 \in \psi_{\bar{i}}(S \setminus \{P\})$ collinear with $\pi_{\bar{i}}(D)$. Let $\bar{R}_1$, $\bar{R}_2$ be their counterimages by $\pi_{\bar{i}}$; then $D \in < \bar{P}_1, \ldots, \bar{P}_{N-3}, \bar{Q}_{\bar{i}}, \bar{R}_1, \bar{R}_2 >$, where $< \bar{P}_1, \ldots, \bar{P}_{N-3}, \bar{Q}_{\bar{i}}, \bar{R}_1, \bar{R}_2 >$ is a hyperplane, generated by N points of T.

Otherwise, if $\pi_i(D) \in \psi_i(\mathcal{E})$, for $i = 1, 2, 3$, note that for $i \neq j$, the subspaces $< W_i, W_j, D >$ of $PG(N, q)$ are hyperplanes that contain at least $N - 1$ points of T. Also, there exists $\bar{R}_i \in \mathcal{X}$ such that $\pi_i(D) = \pi_i(\bar{R}_i)$, for $i = 1, 2, 3$. Consequently, such points $\bar{R}_i$ of $\mathcal{X}$ are such that

$$\bar{R}_i, \bar{R}_j \in < W_i, W_j, D > \text{, for } i \neq j.$$

Thus, by Proposition 4.2, the following relations hold

$$\bar{R}_i \oplus \bar{R}_j \oplus \bar{Q}_i \oplus \bar{Q}_j \oplus \bar{P}_1 \ldots \oplus \bar{P}_{N-3} = \bar{O}, \text{ for } i \neq j,$$

from which

$$2\bar{R}_i = \ominus 2\bar{Q}_i \ominus \bar{P}_1 \ldots \ominus \bar{P}_{N-3}, \text{ for } i = 1, 2, 3.$$

As the size of $\bar{G}$ is odd, the $\bar{R}_i$'s are uniquely determined by the W_i's and $D \in \bigcap_{i=1,2,3} < W_i, \bar{R}_i >$, which is a subspace of dimension at most $N-2$. So, in order to cover the point D it would be necessary to add at most $N-1$ points of such a subspace to T. □

Corollary 4.25. *Let m be a prime divisor of $q-1$ with $7 < m < \frac{1}{8}\sqrt[4]{q}$. Assume that $m > \max\{\frac{(N-1)^3}{2}, \frac{3N^2+5N-10}{2}\}$. Then for some integer i_0, with*

$$1 \leq i_0 - \lfloor \frac{q - 2\sqrt{q} + 1}{m} \rfloor \leq 31,$$

there exists a complete arc in $PG(N,q)$ with size at most

$$(\lceil (N+1)/2 \rceil - 1)(i_0 - 1) + 2\frac{m+1}{N-1} + N - \frac{5}{2}. \tag{4.17}$$

Proof. It has been shown in [**3**, Section 1, p. 389] that for a prime divisor m of $q-1$ such that $7 < m < \frac{1}{8}\sqrt[4]{q}$ there exist an integer i_0 not divisible by m in the interval

$$\Big[\lfloor \frac{q - 2\sqrt{q} + 1}{m} \rfloor + 1, \lfloor \frac{q - 2\sqrt{q} + 1}{m} \rfloor + 31\Big],$$

and an elliptic curve $\mathcal{E}$, such that the size of the set $\mathcal{E}(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points is $i_0 m$ and the associated group $(\mathcal{E}(\mathbb{F}_q), \oplus)$ is cyclic. Let K be the subgroup of G of size i_0. As i_0 and m are coprime, G is isomorphic to $\mathbb{Z}_m \times K$. Then the claim follows from Theorem 4.24. □

4.2.3. Comparison with previous results. In conclusion, we have obtained a complete arc of of size n in $PG(N,q)$ with $q^{3/4} < n < \frac{q}{N^2}$, for dimensions N greater than 2 and as large as $\sqrt[12]{q}$. We note that the order of magnitude of n only depends on the factorization of the integer $q-1$ into prime factors. In particular, whenever $q-1$ has a prime divisor less than $\frac{1}{8}\sqrt[4]{q}$ but of the same order of magnitude as $\sqrt[4]{q}$, complete arcs with roughly $q^{3/4}$ points are obtained.

We briefly compare this results with the few constructions of complete arcs for $N > 2$ available in the literature. In [**65**] the author investigates the existence of small complete arcs in projective spaces $PG(N,q)$ having many points in common with a normal rational curve. All the complete arcs in $PG(N,q)$ constructed in [**65**] have size $n \gtrapprox q/N$ [**65**, Theorems 3.1, 3.2, 3.3, 3.4, 5.2, 5.3, 5.4, 5.5]; clearly this can be close to our bound (4.17) only for very large geometrical dimensions N, namely $N \gtrapprox q^{1/4}$. In [**66, 67**] the authors investigate the largest possible intersection of an arc with the normal rational curves in $PG(N, q)$. If q is odd and the dimension is three, they find a subset K of the normal rational curve L of size roughly $q/2$ that can be completed only adding some points of $L \cup \ell$, where ℓ is a real or an imaginary bisecant of L; see [**66**, Theorem 3.8]. For large q's, they also describe arcs in $PG(N, q)$ with $4 \leq N \leq 0.09q + 2.59$ if q is even, $3 \leq N \leq 0.09q + 2.09$ if q is odd, having at least $0.41q + N - 1.59$ points in common with a given normal rational curve; see [**66**, Theorem 4.1] and [**67**, Theorem 4.1].

4.3. Complete arcs and MDS elliptic codes

In this section we keep the notation of Section 1.5 and we will use the well-known connection between finite geometries and MDS codes, in order to present the main result of this chapter in the language of covering codes. The geometric problem of finding an n-arc of $PG(s-1, q)$ can be looked at as the problem of finding an $[n, n-s, s+1]$ MDS code. The coordinates of the points of the arc are the columns of a parity check matrix for the code. Since the covering radius ρ is the least integer such that every syndrome is a linear combination of some ρ or fewer columns of the parity check matrix, we have that $\rho = s-1$ holds precisely when the arc is complete, (see Definition 2.1).

First we briefly introduce elliptic codes.

We keep the notation at the beginning of Chapter 4. Let $P_1, P_2, \ldots, P_n$ be $\mathbb{F}_q$-rational points of $\mathcal{E}$, and let D be the divisor $P_1 + P_2 + \ldots + P_n$. For an integer $N \geq 2$, the AG code $C(D, (N+1)O)$ of length n over $\mathbb{F}_q$ is the image of the linear map $\alpha : L((N+1)O) \to \mathbb{F}_q^n$ defined by $\alpha(f) = (f(P_1), f(P_2), \ldots, f(P_n))$. If n is bigger than $N+1$, then α is an embedding, and the dimension of $C(D, (N+1)O)$ is equal to $N+1$. The dual code $C^{\perp}(D, (N+1)O)$ of $C(D, (N+1)O)$ is an AG code with dimension $n - (N+1)$.

As a matter of terminology, we give the following definition.

DEFINITION 4.26. The code $C^{\perp}(D, (N+1)O)$ is called an (n, N)-*elliptic code* associated to $\mathcal{E}$.

A parity check matrix M of an (n, N)-elliptic code is

$$M_{P_1,\ldots,P_n} = \begin{pmatrix} \phi_0(P_1) & \ldots & \phi_0(P_n) \\ \vdots & \ldots & \vdots \\ \phi_N(P_1) & \ldots & \phi_N(P_n) \end{pmatrix}, \tag{4.18}$$

where $\phi_0, \phi_1, \ldots, \phi_N$ form an $\mathbb{F}_q$-basis of $L((N+1)O)$. Throughout this section, we will assume that this basis coincides with the coordinates of the morphism Φ_N, defined in (4.2). As a consequence of Proposition 4.2, the following characterization of MDS elliptic codes holds (see also [**49**, Sect. 2]).

Corollary 4.27. *An (n, N)-elliptic code with parity check matrix $M_{P_1,\ldots,P_n}$ is an MDS code if and only if for every $1 \leq i_1 < i_2 < \ldots < i_{N+1} \leq n$,*

$$P_{i_1} \oplus \ldots \oplus P_{i_{N+1}} \neq O.$$

In the case where the point set $\{P_1, \ldots, P_n\}$ coincides with the arc S of Proposition 4.1, we have the following result, which is equivalent to Proposition 4.3, translated into the language of codes and a direct consequence of Corollary 4.27 and Proposition 4.2.

Proposition 4.28. *The (n, N)-elliptic code associated to the points of S is an MDS code.*

In the case where the point set $\{P_1, \ldots, P_n\}$ coincides with the subset T of $\bar{G}$ of Proposition 4.18, the (n, N)-elliptic code associated to the points of T is an MDS code too. We note that the MDS code associated to the complete arc in Theorem 4.24, is obtained from the $(|T|, N)$-elliptic code associated to T by applying a lengthening procedure not more than $N - 1$ times.

Taking into account the above discussion, we can reformulate Corollary 4.25 into the language of covering codes. In particular, to find a complete arc of of size n in $PG(N, q)$ with $q^{3/4} < n < \frac{q}{N^2}$, where the dimension N is greater than 2 and as large as $\sqrt[12]{q}$, is equivalent to find some MDS elliptic codes that give rise to MDS codes with covering radius $\rho = N$, and a length n roughly $q^{3/4} < n < \frac{q}{N^2}$. More precisely, our main result is the following.

Theorem 4.29. *Let $q = p^h$, with $p > 3$ a prime. Let m be a prime divisor of $q - 1$ with $7 < m < \frac{1}{8}\sqrt[4]{q}$. Assume that $m > \max\{\frac{(N-1)^3}{2}, \frac{3N^2+5N-10}{2}\}$. Then there exists an MDS code over $\mathbb{F}_q$ with redundancy $N + 1$, covering radius N, and length n with*

$$\lfloor \frac{q - 2\sqrt{q} + 1}{m} \rfloor \leq n \leq (\lceil (N + 1)/2 \rceil - 1)(\lfloor \frac{q - 2\sqrt{q} + 1}{m} \rfloor + 30) + 2\frac{m + 1}{N - 1} + N - \frac{5}{2}.$$

In terms of the length function $l(N+1, N; q)_{N+2}$ introduced in Section 1.5, Theorem 4.29 can be read as follows.

Corollary 4.30. *Let $q = p^h$, with $p > 3$ a prime, and $N > 2$ an integer. Let m be a prime divisor of $q - 1$ with $7 < m < \frac{1}{8}\sqrt[4]{q}$ and $m > \max\{\frac{(N-1)^3}{2}, \frac{3N^2+5N-10}{2}\}$. Then*

$$l(N + 1, N; q)_{N+2} \leq (\lceil (N + 1)/2 \rceil - 1)(\lfloor \frac{q - 2\sqrt{q} + 1}{m} \rfloor + 30) + 2\frac{m + 1}{N - 1} + N - \frac{5}{2}.$$

CHAPTER 5

Complete caps in $AG(3,q)$ from elliptic curves

Since the 80's, elliptic curves, and more generally cubic curves, have played an important role in the construction of small complete caps, both in the plane [**26, 71, 72, 68, 75, 78**] and in higher dimensions via inductive constructions [**1, 2, 3, 27, 28, 32**]. Let $AG(3,q)$ be the three-dimensional affine space over $\mathbb{F}_q$. Here we show that the set $\mathcal{X}$ of $\mathbb{F}_q$-rational affine points of an elliptic curve in $AG(3,q)$ is a cap. By using arguments from algebraic geometry, we are able to provide a significant lower bound on the number of points of $AG(3,q)$ that are collinear with two points of $\mathcal{X}$; see Proposition 4.1. Interestingly, $\mathcal{X}$ can be extended to a (larger) cap of size $2q$ by adding the $\mathbb{F}_q$-rational affine points of another elliptic curve, called its *quadratic twist*; see Proposition 5.2. For $q \leq 349$ these caps are not complete; however, by adding some extra points they can be extended to complete caps in $AG(3,q)$ of size with the same order of magnitude as the trivial lower bound. For $97 < q \leq 349$ these are the smallest complete caps in $AG(3,q)$ known in the literature (for $q \leq 97$ smaller examples were obtained in [**15, 50**]).

5.1. The construction

Let (X,Y,Z) denote the coordinates of the Galois affine space $AG(3,q)$, where $q=p^h$ and $p \neq 2$ is a prime. Let $\mathcal{C} : X^2 - Z = 0$ be a cone of $AG(3,q)$ and $\mathcal{F}$ be the family of lines of $AG(3,q)$

$$\mathcal{F} = \{\ell_k \mid k \in \mathbb{F}_q\},$$

where ℓ_k has equations $X=k, Z=k^2$. Clearly, $\mathcal{C}$ can be viewed as the union of the (pairwise disjoint) lines in $\mathcal{F}$.

Lemma 5.1. *Let S be a subset of $\mathcal{C}$. If every line of $\mathcal{F}$ contains at most two points of S, then S is a cap.*

Proof. Assume on the contrary that there exists a line $\ell \notin \mathcal{F}$ containing three distinct points $P_i = (x_i, y_i, x_i^2) \in S$, for $i = 1,2,3$. Note that $x_1 \neq x_2$, otherwise ℓ has equations $X = x_1, Z = x_1^2$ and belongs to $\mathcal{F}$. Therefore, ℓ is the only line through P_1 and P_2, and hence it is contained in the plane with equation

$$(X - x_1)/(x_2 - x_1) = (Z - x_1^2)/(x_2^2 - x_1^2).$$

From $P_3 \in \ell$ it follows

$$(x_3 - x_1)/(x_2 - x_1) = (x_3^2 - x_1^2)/(x_2^2 - x_1^2),$$

which holds if and only if $x_1 = x_3$ or $x_2 = x_3$, as $x_1 \neq x_2$ by assumptions. But then ℓ has equations $X = x_2, Z = x_2^2$ or $X = x_3, Z = x_3^2$, a contradiction. □

Fix $A, B \in \mathbb{F}_q$ with $4A^3+27B^2 \neq 0$ and such that the polynomial $T^3+AT+B \in \mathbb{F}_q[T]$ has no roots in $\mathbb{F}_q$. Let $\mathcal{E}$ be the plane elliptic curve with affine equation $\mathcal{E} : Y^2 - X^3 - AX - B = 0$. Fix a non-square C in $\mathbb{F}_q$ and let $\mathcal{E}^T : Y^2 - C(X^3 + AX + B) = 0$ be a quadratic twist of $\mathcal{E}$. We define the following subsets of $\mathcal{C}$:

$$\mathcal{X} := \{(x, y, x^2) \in AG(3, q) \mid (x, y) \in \mathcal{E}\},$$

$$\mathcal{X}^T := \{(x, y, x^2) \in AG(3, q) \mid (x, y) \in \mathcal{E}^T\}.$$

Note that $\mathcal{X} \cap \mathcal{X}^T = \{(x, 0, x^2) \in AG(3, q) \mid x^3+Ax+B = 0\}$; as $T^3+AT+B \in \mathbb{F}_q[T]$ has no roots in $\mathbb{F}_q$, $\mathcal{X}$ and $\mathcal{X}^T$ are disjoint.

Proposition 5.2. *The set $S = \mathcal{X} \cup \mathcal{X}^T$ is a cap of size $2q$.*

Proof. Since S is a subset of $\mathcal{C}$, by Lemma 5.1 it is enough to show that every line in $\mathcal{F}$ contains exactly two points in S. The intersection of a line ℓ_k and S consists of points (k, t, k^2) where t is such that either

$$t^2 - (k^3 + Ak + B) = 0, \quad \text{or} \tag{5.1}$$

$$t^2 - C(k^3 + Ak + B) = 0. \tag{5.2}$$

Recall that by construction $k^3+Ak+B \neq 0$ for each $k \in \mathbb{F}_q$. Also, when k^3+Ak+B is a square in $\mathbb{F}_q$, then (5.1) holds for two values of $t \in \mathbb{F}_q$ and (5.2) has no solutions. Similarly, when $k^3 + Ak + B$ is a non-square in $\mathbb{F}_q$, then (5.1) holds for no values of $t \in \mathbb{F}_q$, whereas (5.2) has two solutions. In either case, $\#S \cap \ell_k = 2$. □

Let $(G, \oplus)$ denote the abelian group of the $\mathbb{F}_q$-rational points of $\mathcal{E}$, defined by choosing the only ideal point O of $\mathcal{E}$ as the neutral element. Here we repeat the construction of Chapter 4, for $N = 3$. Let ϕ be the rational map on $\mathcal{E}$ defined as in (4.2), with affine coordinates $\phi(x, y) = (x, y, x^2)$, and $\phi(O) = Z_\infty$, where Z_∞ is the ideal point of the Z-axis. Also, let $\tilde{\mathcal{X}}$ be the union of $\mathcal{X}$ and $\{Z_\infty\}$; then the restriction $\phi_{|G} : G \to \tilde{\mathcal{X}}$ of the map ϕ to the set G of the $\mathbb{F}_q$-rational points of $\mathcal{E}$ is clearly a bijection. Next proposition is Proposition 4.2, for $N = 3$.

Proposition 5.3. *Let $P_1, P_2, P_3, P_4 \in \mathcal{E}$, then*

$$\phi(P_1), \phi(P_2), \phi(P_3), \phi(P_4) \text{ are coplanar } \Leftrightarrow P_1 \oplus P_2 \oplus P_3 \oplus P_4 = O.$$

Proposition 5.4. *Any point P off $\mathcal{X}$ belongs to at most 2 distinct secants of $\mathcal{X}$.*

PROOF. Assume by contradiction that there exist three distinct secants r_j of $\mathcal{X}$ passing through P, for $j = 1, 2, 3$, i.e., there exist six distinct points P_i in G such that $P, \phi(P_1), \phi(P_2) \in r_1$, $P, \phi(P_3), \phi(P_4) \in r_2$ and $P, \phi(P_5), \phi(P_6) \in r_3$. Then by Proposition 5.3

$$\begin{cases} P_1 \oplus P_2 \oplus P_3 \oplus P_4 = O \\ P_3 \oplus P_4 \oplus P_5 \oplus P_6 = O \\ P_1 \oplus P_2 \oplus P_5 \oplus P_6 = O \end{cases},$$

whence,

$$\begin{cases} 2(P_1 \oplus P_2) = O \\ 2(P_3 \oplus P_4) = O \\ 2(P_5 \oplus P_6) = O \end{cases}.$$

Note that in G there is no point with $Y = 0$. This implies that in G there is no involution, and hence for each $i \in \{1, 3, 5\}$ we have $P_i \oplus P_{i+1} = O$. By the definition of the group operation $\oplus$, this implies $\phi(P_i) = (\tilde{x}_i, \tilde{y}_i, \tilde{x}_i^2)$ and $\phi(P_{i+1}) = (\tilde{x}_i, -\tilde{y}_i, \tilde{x}_i^2)$, for some $\tilde{x}_i, \tilde{y}_i \in \mathbb{F}_q$; whence, for $j = (i+1)/2$ the line r_j is actually the line $\ell_{\tilde{x}_i} \in \mathcal{F}$. This contradicts $P \in r_j$ for each j, as the lines in $\mathcal{F}$ are pairwise disjoint. □

By a standard double-counting argument Proposition 5.4 yields that the number of points in $AG(3, q)$ belonging to some secant of $\mathcal{X}$ is at least $q\#\mathcal{X}(\#\mathcal{X} - 1)/4$. Actually a stronger result can be proved.

PROPOSITION 5.5. *At least*

$$\#\mathcal{X} + \frac{1}{2}\#\mathcal{X}(\#\mathcal{X} - 1)\left(q - 2 - \frac{\#\mathcal{X} - 2}{4}\right)$$

points of $AG(3, q)$ are collinear with two points of $\mathcal{X}$.

PROOF. Let c denote the number of points in $AG(3, q)$ belonging to some secants of $\mathcal{X}$. For $i = 1, 2$, let $\mathcal{A}_i$ be the set of ordered pairs (P, r) such that r is a secant of $\mathcal{X}$, P is a point on $r \setminus \mathcal{X}$, and i is the number of secants of $\mathcal{X}$ through P. Then clearly

$$c = \#\mathcal{X} + \#\mathcal{A}_1 + \frac{1}{2}\#\mathcal{A}_2.$$

For a secant r of $\mathcal{X}$ let $N(r)$ be the number of points of $r \setminus \mathcal{X}$ belonging to two secants of $\mathcal{X}$. Then

$$\#\mathcal{A}_1 = \sum_{r \text{ secant of } \mathcal{X}} (q - 2 - N(r)), \qquad \#\mathcal{A}_2 = \sum_{r \text{ secant of } \mathcal{X}} N(r),$$

and hence

$$c = \#\mathcal{X}\left(1 + \frac{q-2}{2}(\#\mathcal{X} - 1)\right) - \frac{1}{2}\sum_{r \text{ secant of } \mathcal{X}} N(r).$$

To prove the assertion we show that $N(r) \leq (\#\mathcal{X} - 2)/2$ for each secant r of $\mathcal{X}$. Let $\phi(P_1)$ and $\phi(P_2)$ be the two points of $\mathcal{X} \cap r$, and let R be the opposite of $P_1 \oplus P_2$ in G. If a point $Q \in r$ belongs to another secant of $\mathcal{X}$, then there exist $P_3, P_4 \in G$ such that the points $\phi(P_3)$ and $\phi(P_4)$ are collinear with Q. Then $\phi(P_1)$, $\phi(P_2)$, $\phi(P_3)$, and $\phi(P_4)$ are coplanar. By Proposition 5.3 $P_3 \oplus P_4 = R$; clearly, this happens for $(\#\mathcal{X} - 2)/2$ unordered pairs $\{P_3, P_4\}$ with $P_3, P_4 \in G \setminus \{P_1, P_2, O\}$, $P_3 \neq P_4$. □

COROLLARY 5.6. *At least*

$$q + \frac{3}{8}q(q-1)(q-2)$$

points of $AG(3,q)$ *are collinear with two points of* $\mathcal{X} \cup \mathcal{X}^T$.

PROOF. If $\#\mathcal{X} \geq q$, then the claim follows from Proposition 5.5. Otherwise it is enough to apply the same argument to $\#\mathcal{X}^T$, since $\#\mathcal{X}^T = 2q - \#\mathcal{X} > q$. □

5.2. New examples of complete caps

For $q \leq 349$ the cap $\mathcal{X} \cup \mathcal{X}^T$ has been extended to a complete cap by computer. Our rough algorithm can be described as follows: set $K := \mathcal{X} \cup \mathcal{X}^T$; then check every point P of $AG(3,q) \setminus (\mathcal{X} \cup \mathcal{X}^T)$, and let $K := K \cup \{P\}$ whenever P is not covered by a secant of K. Clearly such an approach is not effective for large values of q's. We were able to go as far as $q = 349$, because we used some geometrical remarks in order to speed up the test of collinearity of P and two distinct points in $\mathcal{X} \cup \mathcal{X}^T$. The GAP programme that we used can be downloaded from `http://goo.gl/4RyvM9`.

In the following table we describe the new complete caps that we obtained. The column n indicates the size of the complete cap in $AG(3,q)$ obtained from the elliptic curve $\mathcal{E}$ defined over $\mathbb{F}_q$ with affine equation $Y^2 = X^3 + \omega^i X + \omega^j$, where ω is the primitive element of $\mathbb{F}_q$ chosen by GAP, and q, i and j can be read from the table. In the equation of $\mathcal{E}^T$, $C = \omega$ is chosen. As a matter of notation, here we put $\omega^{-\infty} = 0$.

q	i	j	n
5	0	0	14
7	$-\infty$	1	24
9	0	1	33
11	0	2	39
13	$-\infty$	1	46
17	0	1	61
19	$-\infty$	1	73
23	0	4	88
25	$-\infty$	1	96
27	15	2	110
29	0	2	116
31	$-\infty$	1	126
37	$-\infty$	1	152
41	0	0	169
43	$-\infty$	1	180
47	0	8	198
49	$-\infty$	1	208
53	0	3	225
59	0	0	258
61	$-\infty$	1	263
67	$-\infty$	1	296
71	0	0	319
73	$-\infty$	1	330
79	$-\infty$	1	359
81	2	2	367
83	0	3	374
89	0	2	404

q	i	j	n
97	$-\infty$	1	450
101	0	0	463
103	$-\infty$	1	476
107	0	0	499
109	$-\infty$	1	514
113	0	0	529
121	$-\infty$	1	569
125	2	2	591
127	$-\infty$	1	602
131	0	3	619
137	0	2	650
139	$-\infty$	1	667
149	0	7	710
151	$-\infty$	1	733
157	$-\infty$	1	759
163	$-\infty$	1	790
167	0	3	817
169	$-\infty$	1	810
173	0	4	844
179	0	2	882
181	$-\infty$	1	883
191	0	0	936
193	$-\infty$	1	954
197	0	2	973
199	$-\infty$	1	983
211	$-\infty$	1	1052

q	i	j	n
223	$-\infty$	1	1121
227	0	3	1132
229	$-\infty$	1	1148
233	0	0	1160
239	0	3	1196
241	$-\infty$	1	1215
243	125	4	1219
251	0	2	1259
257	0	0	1298
263	0	2	1334
269	0	3	1362
271	$-\infty$	1	1369
277	$-\infty$	1	1414
281	0	0	1425
283	$-\infty$	1	1450
289	$-\infty$	1	1478
293	0	2	1492
307	$-\infty$	1	1570
311	0	0	1601
313	$-\infty$	1	1603
317	0	0	1637
331	$-\infty$	1	1704
337	$-\infty$	1	1743
343	$-\infty$	2	1765
347	0	3	1802
349	$-\infty$	1	1809

Bibliography

[1] N. Anbar, D. Bartoli, M. Giulietti and I. Platoni. 'Small complete caps from singular cubics'. *J. Combin. Des.*, 22 (10) : 409–424, 2014. DOI: 10.1002/jcd.21366.

[2] N. Anbar, D. Bartoli, M. Giulietti and I. Platoni. 'Small complete caps from singular cubics, II'. *J. Algebraic Combin.*, in press, 2014. DOI: 10.1007/s10801-014-0532-7.

[3] N. Anbar and M. Giulietti. 'Bicovering arcs and small complete caps from elliptic curves'. *J. Algebraic Combin.*, 38 : 371–392, 2013.

[4] S. Ball. 'On small complete arcs in a finite plane'. *Discrete Math.*, 174 : 29–34, 1997.

[5] D. Bartoli, M. Giulietti and I. Platoni. 'On the covering radius of MDS Codes', submitted to *IEEE Trans. Inf. Theory.*

[6] D. Bartoli, G. Faina and M. Giulietti. 'Small complete caps in three-dimensional Galois spaces'. *Finite Fields Appl.*, 24 : 184–191, 2013.

[7] A. Blokhuis. 'Note on the size of a blocking set in $PG(2, p)$'. *Combinatorica*, 14 : 111–114, 1994.

[8] E. Boros and T. Szőnyi. 'On the sharpness of a theorem of B. Segre'. *Combinatorica*, 6 : 261–268, 1986.

[9] R. A. Brualdi, S. Litsyn and V. S. Pless. 'Covering radius'. *Handbook of Coding Theory*, V.S. Pless, W.C. Huffman, and R.A. Brualdi, Eds. Amsterdam, The Netherlands: Elsevier, 1 : 755–826, 1998.

[10] R. A. Brualdi, V.S. Pless and R. M. Wilson. 'Short codes with a given covering radius'. *IEEE Trans. Inform. Theory*, 35 (1) : 99–109, 1989.

[11] A.A. Bruen, J.W.P. Hirschfeld and D.L. Wehlau. 'Cubic curves, finite geometry and cryptography'. *Acta Appl. Math.*, 115 (3) : 265–278, 2011.

[12] G. D. Cohen, I. Honkala, S. Litsyn and A. C. Lobstein. *Covering Codes.* Amsterdam, The Netherlands: Elsevier, 1997.

[13] G. D. Cohen, M. G. Karpovsky, H. F. Mattson Jr. and J. R. Schatz. 'Coverig radius - Survey and recent results '. *IEEE Trans. Inf. Theory*, 31 (3) : 328–343, 1985.

[14] G. D. Cohen, A. C. Lobstein and N. J. A. Sloane. 'Further results on the covering radius of codes'. *IEEE Trans. Inform. Theory*, 32 (5) : 680–694, 1986.

[15] A. A. Davydov, G. Faina, S. Marcugini, and F. Pambianco. 'On sizes of complete caps in projective spaces $\mathrm{PG}(n, q)$ and arcs in planes $\mathrm{PG}(2, q)$'. *J. Geom.*, 94 (1-2) : 31–58, 2009.

[16] A.A. Davydov, M. Giulietti, S. Marcugini, and F. Pambianco. 'New inductive constructions of complete caps in $\mathrm{PG}(N, q)$, q even'. *J. Combin. Des.*, 18 (3) : 177–201, 2010.

[17] A.A. Davydov, M. Giulietti, S. Marcugini, and F. Pambianco. 'Linear non-binary covering codes and saturating sets in projective spaces'. *Advances in Mathematics of Communications*, 5 (1) : 119–147, 2011.

[18] A.A. Davydov and P.R.J. Östergård. 'Recursive constructions of complete caps'. *J. Statist. Plann. Inference*, 95 (1-2) : 167–173, 2001. Special issue on design combinatorics: in honor of S. S. Shrikhande.

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

[20] E. Gabidulin, T. Klove. 'The newton radius of mds codes'. in *Information Theory Whorkshop*, June 1998 : 50–51, 1998.

[21] G. Faina. 'Complete caps having less than $(q^2+1)/2$ points in common with an elliptic quadric of $PG(3,q)$, q odd'. *Rend. Mat. Appl. (7)*, 8 (2) : 277–281, 1988.

[22] G. Faina and F. Pambianco. 'A class of complete k-caps in $PG(3,q)$ for q an odd prime'. *J. Geom.*, 57 (1-2) : 93–105, 1996.

[23] G. Faina, F. Pasticci, and L. Schmidt. 'Small complete caps in Galois spaces'. *Ars Combin.*, 105 : 299–303, 2012.

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

[25] J. C. Fisher, J.W.P Hirschfeld and J.A. Thas. 'Complete arcs in planes of square order'. *Ann. Discrete Math.*, 30 : 243–250, 1986.

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

[27] M. Giulietti. 'On the extendibility of Near-MDS Elliptic Codes'. *AAECC - Applicable Algebra in Engineering, Communication and Computing*, 15(1) : 1–11, 2004.

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

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

[30] M. Giulietti. 'The geometry of covering codes: small complete caps and saturating sets in Galois spaces'. In *Surveys in Combinatorics 2013 - London Mathematical Society Lecture Note Series 409*, Cambridge University Press, 51–90, 2013.

[31] M. Giulietti and F. Pasticci. 'Quasi-Perfect Linear Codes With Minimum Distance 4'. *IEEE Trans. Inform. Theory*, 53 (5) : 1928–1935, 2007.

[32] M. Giulietti and F. Pasticci. 'On the completeness of certain n-tracks arising from elliptic curves'. *Finite Fields Appl.*, 13 (4) : 988–1000, 2007. DOI: 10.1016/j.ffa.2006.09.007.

[33] É. Hadnagy. 'Small Complete Arcs in $PG(2,p)$'. *Finite Fields Appl.*, 5 : 1–12, 1999.

[34] J.W.P. Hirschfeld. *Finite projective spaces of three dimensions.* Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, 1985. Oxford Science Publications.

[35] J.W.P. Hirschfeld. 'Algebraic curves, arcs, and caps over finite fields'. Quaderni dal Dipartimento di Matematica dell'Universit del Salento 5, Dipartimento di Matematica, Universit del Salento, Lecce, 1986.

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

[37] J.W.P. Hirschfeld, G. Korchmáros, and F. Torres. *Algebraic curves over a finite field.* Princeton University Press, Princeton and Oxford, 2008.

[38] J.W.P. Hirschfeld, G. Korchmáros. 'On the embedding of an arc into a conic in a finite plane'. *Finite Fields Appl.*, 2 : 247–292, 1996.

[39] J.W.P. Hirschfeld, G. Korchmáros. 'On the number of rational points on an algebraic curve over a finite field'. *Bull. Belg. Math. Soc. Simon Stevin*, 5 : 313–340, 1998.

[40] J.W.P. Hirschfeld and L. 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).

[41] J.W.P. Hirschfeld and L. Storme. 'The packing problem in statistics, coding theory and finite projective spaces: update 2001'. In *Finite geometries*, volume 3 of *Dev. Math.*, pages 201–246. Kluwer Acad. Publ., Dordrecht, 2001.

[42] J.W.P. Hirschfeld and J.F. Thas. *General Galois Geometries*, Oxford Univ. Press, Oxford, 1991.

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

[44] B.C. Kestenband. 'A family of complete arcs in finite projective planes'. *Colloq. Math.*, 57 : 59–67, 1989.

[45] G. Korchmáros. 'New examples of complete k-arcs in $PG(2,q)$'. *European J. Combin.*, 4 (4) : 329–334, 1983.

[46] J.H. Kim and V.H. Vu. 'Small complete arcs in projective planes '. *Combinatorica*, 23 (2) : 311–363, 2003.

[47] R. Lidl and H. Niederreiter. *Finite Fields*, Enc. of Math. **20**, Addison-Wesley, Reading, 1983.

[48] L. Lombardo-Radice. 'Sul problema dei k-archi completi in $S_{2,q}$. ($q = p^t$, p primo dispari.)'. *Boll. Un. Mat. Ital. (3)*, 11 : 178–181, 1956.

[49] C. Munuera. 'On MDS elliptic codes'. *Discrete Math.*, 117 (1-3) : 279–286, 1993. DOI: 10.1016/0012-365X(93)90344-S

[50] P.R.J. Östergård. 'Computer search for small complete caps'. *J. Geom*, 69 : 172–179, 2000. DOI: 10.1007/BF01237484.

[51] F. Pambianco and L. Storme. Unpublished Manuscript, 1995.

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

[53] G. Pellegrino. 'On complete caps, not ovaloids, in the space $PG(3,q)$ with q odd'. *Rend. Circ. Mat. Palermo*, 47 : 141–168, 1998.

[54] I. Platoni. 'Complete caps in $AG(3,q)$ from elliptic curves'. J. Algebra Appl., 13 : 1450050 [8 pages], 2014; DOI: 10.1142/S0219498814500509.

[55] O. Polverino. 'Small blocking sets and complete k-arcs in $PG(2,p^3)$'. *Discrete Math.*, 208/209 : 469–476, 1999.

[56] R. Schoof. 'Nonsingular plane cubic curves over finite fields'. *J. Combin. Theory Ser. A*, 46 (2) : 183–211, 1987.

[57] B. Segre. 'Le geometrie di Galois'. *Ann. Mat. Pura Appl.*, 48 : 1–97, 1959.

[58] B. Segre. 'On complete caps and ovals in three-dimensional Galois spaces of characteristic two'. *Acta Arithm*, 5 : 315–332, 1959.

[59] B. Segre. 'Introduction to Galois geometries'. *Atti Accad. Naz. Lincei Mem. Cl. Sci. Fis. Mat. Natur. Sez. I (8)*, 8 : 133–236, 1967.

[60] B. 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.

[61] B. 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.

[62] B. Segre. 'Sui k-archi nei piani finiti di caratteristica due'. *Rev. Math. Pures Appl.*, 2 : 289–300, 1957.

[63] B. Segre and U. Bartocci. 'Ovali ed altre curve nei piani di Galois di caratteristica due'. *Acta Arith.*, 18 : 423–449, 1971.

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

[65] L. Storme. 'Small arcs in projective spaces'. *J. Geom.*, 58 (1-2) : 179–191, 1997.

[66] L. Storme and T. Szőnyi. 'Intersection of arcs and normal rational curves in spaces of odd characteristic'. In *Finite geometry and combinatorics (Deinze, 1992)*, ser. London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 191 : 359–378, 1993.

[67] L. Storme and T. Szőnyi. 'Intersection of arcs and normal rational curves in spaces of even characteristic'. *J. Geom.*, 51 (1-2) : 150–166, 1994.

[68] T. 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.

[69] T. 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.

[70] T. Szőnyi. 'Some applications of algebraic curves in finite geometry and combinatorics'. In *Surveys in combinatorics, 1997 (London)*, volume 241 of *London Math. Soc. Lecture Note Ser.*, pages 197–236. Cambridge Univ. Press, Cambridge, 1997.

[71] T. Szőnyi. 'Small complete arcs in Galois planes'. *Geom. Dedicata*, 18 (2) : 161–172, 1985.

[72] T. Szőnyi. 'Note on the order of magnitude of k for complete k-arcs in $\mathrm{PG}(2,q)$'. *Discrete Math.*, 66 (3) : 279–282, 1987.

[73] J. A. Thas. 'Complete arcs and algebraic curves in $PG(2,q)$'. *J. Algebra*, 106 : 451–464, 1987.

[74] J.F. Voloch. 'Arcs in projective planes over prime fields'. *J. Geom.*, 38 : 198–200, 1990.

[75] J.F. Voloch. 'A note on elliptic curves over finite fields'. *Bull. Soc. Math. France*, 116 : 455–458, 1988.

[76] J.F. Voloch. 'Complete arcs in Galois planes of non-square order'. *Advances in Finite Geometries and Designs*, (eds. J.W.P. Hirschfeld, D.R, Hughes, J.A. Thas), Oxford University Press, Oxford, 1991, 401–406, 1991.

[77] J.F. Voloch. 'On the completeness of certain plane arcs'. *European J. Combin.*, 8 : 453–456, 1987.

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

[79] W.G. Waterhouse. 'Abelian varieties over finite fields'. *Ann. Sci. Ecole Norm. Sup.*, 2 : 521–560, 1969.

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