UNIVERSITÀ DEGLI STUDI FIRENZE

UNIVERSITÀ DEGLI STUDI DI PERUGIA

iNδAM Istituto Nazionale di Alta Matematica

Università di Firenze, Università di Perugia, INdAM consorziate nel CIAFM

**DOTTORATO DI RICERCA**
**IN MATEMATICA, INFORMATICA, STATISTICA**

CURRICULUM IN MATEMATICA
CICLO XXIX

**Sede amministrativa Università degli Studi di Firenze**
Coordinatore Prof. Graziano Gentili

# Maximal curves over finite fields and related objects

Settore Scientifico Disciplinare MAT/03

**Dottorando**:
Giovanni Zini
Giovanni Zini

**Tutore**
Prof. Massimo Giulietti
Massimo Giulietti

**Coordinatore**
Prof. Graziano Gentili

Anni 2013/2016

# Contents

# Introduction

The foundation of the theory of complex algebraic curves goes back to the Nineteenth century, and most of this theory remains valid for curves defined over a field of zero characteristic. Instead, there are significant differences between zero and positive characteristic, especially in the properties of automorphism groups but also in the behavior of the fundamental groups. Furthermore, when the constant field if finite, new aspects of the algebraic curves arise depending on their $\mathbb{F}_q$-rational points, where $\mathbb{F}_q$ is a finite extension of the constant field. For instance, this gives rise to a generalization of the Riemann zeta function which leads to an analogue of the Riemann hypothesis. The intrinsic theoretical interest towards algebraic curves over finite fields is boosted by interactions with Number Theory and Finite Geometry as well as relevant applications to error-correcting codes and cryptography.

Most of the results of the present work concern maximal curves over a finite field, their automorphism groups, and applications to Algebraic-Geometric codes.

The fundamental result in this area is the Hasse-Weil bound on the number $N_q$ of $\mathbb{F}_q$-rational points of a curve $\mathcal{X}$ of genus $g$ defined over $\mathbb{F}_q$,

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

Hasse proved the above bound for elliptic curves, although it was Artin to point out the number of solutions of the congruence

$$y^2 \equiv f(x) \pmod{p}$$

should satisfy the Hasse-Weil bound. For the general case the Hasse-Weil bound was proved by Weil.

The curve $\mathcal{X}$ is $\mathbb{F}_q$-maximal if it attains the Hasse-Weil upper bound, that is, $N_q = q + 1 + 2g\sqrt{q}$; this requires $q$ to be a square.

Computing the possible genera of $\mathbb{F}_q$-maximal curves is an open problem, and their spectrum is well understood only for large genera with respect to $q$.

By a result of Serre, a curve covered by an $\mathbb{F}_q$-maximal curve through an $\mathbb{F}_q$-rational morphism is still $\mathbb{F}_q$-maximal; in particular, automorphism groups defined over $\mathbb{F}_q$ produce quotient curves which are $\mathbb{F}_q$-maximal. This gives a strong motivation for the study of automorphism groups of $\mathbb{F}_q$-maximal curves.

For applications to Coding Theory, explicit equations of $\mathbb{F}_q$-maximal curves are needed. This may be challenging, and tools from Finite Field Theory and Combinatorics are often required.

The present thesis consists of four chapters.

Chapter 1 collects the basic definitions and results about curves over a finite field and their function fields. The background on Algebraic-Geometric codes is also given in Section 1.1. In Section 1.2 remarkable examples of maximal curve over finite fields are presented. They include classical examples such as the Deligne-Lusztig curves (Hermitian, Suzuki, and Ree curves), as well as recent examples, namely the Giulietti-Korchmáros, the Garcia-Güneri-Stichtenoth, and the Garcia-Stichtenoth curves.

Chapter 2 contains our original contributions to maximal curves. In Section 2.1 we construct Galois subcovers of the Giulietti-Korchmáros curves; we determine the corresponding Galois groups and compute explicits equations. We also show that some of such Galois subcovers are not isomorphic to a Galois subcover (in some cases, to any subcover) of the Hermitian curve. Sections 2.2 and 2.3 are about the Garcia-Güneri-Stichtenoth and Garcia-Stichtenoth curves, and the smallest Suzuki and Ree curves. We show that they are not isomorphic to a Galois subcover of the Hermitian curve. We heavily rely on deeper results on the structure of the linear group $\mathrm{PGU}(3,q)$ and the simple Suzuki and Ree groups. Section 2.4 is concerned especially with certain cyclic covers $\tilde{\mathcal{S}}_q$ and $\tilde{\mathcal{R}}_q$ of the Suzuki and Ree curves. We show that they are not Galois covered by the Hermitian curves $\mathcal{H}_{q^2}$ and $\mathcal{H}_{q^3}$ respectively, and determine their full automorphism groups. The contents of this chapter are also found in [54, 56, 92, 55].

Chapter 3 contains our original contributions to Algebraic-Geometric codes. Section 3.1 deals with Kummer extensions of the rational function field; we extend known results on the Weierstrass semigroup at many totally ramified points, and provide new families of so-called pure gaps at these points; this is then applied to obtain Algebraic-Geometric codes with good parameters. In Section 3.2 we construct Algebraic-Geometric codes from the Giulietti-Korchmáros curves and compute their parameters. Our idea is to consider divisors left invariant by a large automorphism group. This choice provides indeed codes with large automorphism groups, hence useful for the applications. The contents of this chapter are also found in [8, 9].

Chapter 4 contains our original contributions regarding applications of curves in related areas, namely Finite Geometry and Permutation Polynomials. Sections 4.1 and 4.2 deals with $(k,r)$-arcs in $\mathrm{PG}(2,q)$. For $r \in \{3,4\}$, we construct $(k,r)$-arcs from $\mathbb{F}_q$-rational points of a rational plane curve of degree $r+1$. Their sizes turn out to be less than $q$; this significantly distinguishes them from the previously known families. Section 4.3 provides constructions and characterizations of certain Complete Permutation Polynomials over a finite field. The characteristic 2 case is useful in Cryptography as they give rise to Bent-Negabent functions. We characterize Complete Permutation Polynomials of $\mathbb{F}_{q^n}$ of type $f_a(x) = ax^d$ with $d = (q^n - 1)/(q - 1) + 1$ in the case of $n + 1$ prime, using the known partial classifications of exceptional polynomials. The contents of this chapter are the object of three published papers [6, 7, 5] and one submitted paper [10].

Finally, I wish to thank my supervisor, Professor Massimo Giulietti, for his guidance at each step of my PhD program. This work, as well as many other things in these years, would not have been possible without his support.

# Chapter 1

# Preliminary notions on curves over a finite field and AG codes

## 1.1 Algebraic function fields and curves

### 1.1.1 Algebraic function fields

In this section we summarize some basic concepts about the theory of function fields. For the proofs and a more detailed exposition, we refer to [107, Chapters 1–4].

**Definition 1.1.1.** *Let $K$ be a perfect field. A* function field *$F$ over $K$ is a transcendental field extension $F$ of $K$ such that $F$ is a finite extension of $K(x)$, for some (and hence for any) $x \in F$ which is transcendental over $K$. The* constant field *of $F$ is the subfield of the elements of $F$ which are algebraic over $K$.*

Throughout this section, $F$ will denote a function field over a perfect field $K$ of characteristic $p \geq 0$, with constant field $K$.

Note that, if $K$ is algebraically closed, then $K$ is the constant field of $F$; if $K$ is a finite field $\mathbb{F}_q$, then $K$ is the algebraic closure $\overline{\mathbb{F}}_q = \cup_{i=1}^{\infty}\mathbb{F}_{q^i}$.

**Definition 1.1.2.** *A* valuation ring *of $F$ is a ring $\mathcal{O} \subsetneq F$ such that $K \subsetneq \mathcal{O}$ and, for every $z \in F$, we have $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.*

A valuation ring $\mathcal{O}$ of $F$ is a local principal ideal domain, and not a field; hence, the following definition is well-posed.

**Definition 1.1.3.** *A* place *of $F$ is the unique maximal ideal $P$ of some valuation ring $\mathcal{O}_P$ of $F$. Any generator of $P$ is called a* local parameter *at $P$. We denote by $\mathbb{P}(F)$ the set of places of $F$.*

Note that $\mathcal{O}_P$ is uniquely determined by its maximal ideal $P$. Note also that each $z \in F \setminus \{0\}$ has a unique representation of the form $z = t^n u$, where $n \in \mathbb{Z}$, $t$ is a local parameter at $P$, and $u \in \mathcal{O} \setminus P$; the integer $n$ does not depend on the choice of $u$.

Being a local PID, $\mathcal{O}_P$ is also a discrete valuation ring (DVR); the discrete valuation of $F$ associated with $\mathcal{O}_P$ is the map $v_P : F \to \mathbb{Z} \cup \{\infty\}$ defined by

$$0 \mapsto \infty, \quad 0 \neq z = t^n u \mapsto n,$$

where $t$ is a local parameter at $P$ and $u \in \mathcal{O}\setminus P$. The discrete valuation $v_P$ satisfies the following properties, for all $x, y \in F$ and $\lambda \in K$:

- $v_P(xy) = v_P(x) + v_P(y)$.
- $v_P(x + y) \geq \min\{v_P(x), v_P(y)\}$.
- If $v_P(x) \neq v_P(y)$, then $v_P(x + y) = \min\{v_P(x), v_P(y)\}$.
- $v_P(\lambda) = 0$.

The local parameters at $P$ are exactly the elements $t \in F$ such that $v_P(t) = 1$, while $\mathcal{O}_P = \{z \in F \mid v_P(z) \geq 0\}$.

**Definition 1.1.4.** *The* residue class field *of a place $P \in \mathbb{P}(F)$ is the field $F_P := \mathcal{O}_P/P$. The* degree *of $P$ is defined as* $\deg(P) = [F_P : K]$. *If* $\deg(P) = 1$, *then $P$ is said to be a $K$-*rational *(or simply* rational*) place.*

For any $z \in \mathcal{O}_P$, we denote by $z(P)$ the canonical image $z + P$; if $z \in F \setminus \mathcal{O}_P$, we set $z(P) := \infty$. Since $K \subset \mathcal{O}_P$ and $K \cap P = \{0\}$, $K$ is canonically embedded in $F_P$.

**Remark 1.1.5.** ([107, Prop. 1.1.15]) *If $P$ is a place of $F$ and $0 \neq x \in P$, then*

$$\deg(P) \leq [F : K(x)] \in \mathbb{N}.$$

*In particular,* $\deg(P)$ *is finite.*

If $K$ is algebraically closed, then all places of $F$ are rational, and for any $z \in F$ the map $P \mapsto z(P)$ is a function $\mathbb{P}(F) \to K \cup \{\infty\}$.

We define zeros and poles of a non-zero function $z \in F$.

**Definition 1.1.6.** *Let $z \in F \setminus \{0\}$ and $P \in \mathbb{P}(F)$. If $v_P(z) = m > 0$, then $P$ is a* zero *of $z$ of* order *(or* multiplicity*) $m$; if $v_P(z) = -m < 0$, then $P$ is a* pole *of $z$ of* order *(or* multiplicity*) $m$;*

**Example 1.1.7.** *An example of function field is the* rational function field, *that is, the extension $F = K(x)$ of $K$ where $x$ is transcendental over $K$. For any irreducible monic polynomials $p(x) \in K[x]$ we have a valuation ring, namely,*

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

*whose associated place is*

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} \in \mathcal{O}_{p(x)} \mid p(x) \mid f(x) \right\};$$

*we also have the valuation ring*

$$\mathcal{O}_{\infty} = \left\{ \frac{f(x)}{g(x)} \mid f, g \in K[x], \deg(f) \leq \deg(g) \right\},$$

*whose associated place is*

$$P_{\infty} = \left\{ \frac{f(x)}{g(x)} \mid f, g \in K[x], \deg(f) < \deg(g) \right\}.$$

*The so-called* infinite *place $P_\infty$ is the only pole of $x$. The place $P_{p(x)}$ has degree $1$ if and only if $p(x) = x - \alpha$ with $\alpha \in K$; this happens in particular when $K$ is algebraically closed. Hence, the places of degree $1$ are in one-to-one correspondence with $K \cup \{\infty\}$, that is, with the projective line $\mathrm{PG}(1, K)$.*

In order to state the Riemann-Roch Theorem, we start by defining the divisors of $F$.

**Definition 1.1.8.** *A* divisor *$D$ of $F$ is an element of the free abelian group $\mathrm{Div}(F)$ generated by the places of $F$, written additively. Namely,*

$$D = \sum_{P \in \mathbb{P}(F)} n_P P, \qquad \text{with } n_P \in \mathbb{Z},\ n_P = 0 \text{ for almost all } P \in \mathbb{P}(F).$$

*The* support *of $D$ is $\mathrm{supp}(D) := \{P \in \mathbb{P}(F) \mid n_P \neq 0\}$; the* degree *of $D$ is*

$$\deg(D) := \sum_{P \in \mathbb{P}(F)} n_P \cdot \deg(P).$$

*Let $v_P(D) := n_P$ be the* weight *(or* multiplicity*) of $P$ in $D$. Then the relation*

$$D_1 \leq D_2 \iff v_P(D_1) \leq v_P(D_2) \text{ for all } P \in \mathbb{P}(F)$$

*defines a partial ordering on $\mathrm{Div}(F)$. A divisor $D$ is called* effective *(or* positive*) if $D \geq 0$.*

Any non-zero rational function $z \in F$ has a finite number of zeros and poles. Then the following definition is well-posed.

**Definition 1.1.9.** *Let $0 \neq z \in F$, and let $Z_1$ and $Z_2$ denote the set of its zeros and poles, respectively. Then we define*

$$(z)_0 := \sum_{P \in Z_1} v_P(z)P, \quad (z)_\infty := \sum_{P \in Z_2} (-v_P(z))P, \quad div(z) = (z) := (z)_0 - (z)_\infty,$$

*which are called respectively the zero divisor, the pole divisor, and the principal divisor of $z$.*

The number of zeros of $z$ is equal to the number of poles of $z$, both counted with multiplicity; in particular, $\deg(z)_0 = \deg(z)_\infty = [F : K(z)]$ ([107, Th. 1.4.11]). Therefore, $div(z)$ has degree zero.

The *principal divisors* of $F$ are the elements of the normal subgroup

$$\mathrm{Princ}(F) := \{div(z) \mid z \in F, z \neq 0\}$$

of $\mathrm{Div}(F)$. The *divisor class group* of $F$ is the quotient group

$$\mathrm{Cl}(F) := \mathrm{Div}(F)/\mathrm{Princ}(F).$$

Two divisors $D_1, D_2 \in \mathrm{Div}(F)$ are said to be *equivalent*, $D_1 \sim D_2$, if $[D_1] = [D_2] \in \mathrm{Cl}(F)$.

**Definition 1.1.10.** *For a divisor $A \in \mathrm{Div}(F)$, the* Riemann-Roch space *associated to $A$ is the $K$-vector space*

$$\mathcal{L}(A) := \{z \in F \mid div(z) \geq -A\} \cup \{0\}.$$

*The dimension of $\mathcal{L}(A)$ over $K$ is denoted by $\ell(A)$.*

In other words, the function $z \in F$ is an element of $\mathcal{L}(A)$ if and only if any pole $P$ of $z$ is in the support of $A$ and the order of $z$ at $P$ is less than or equal to $v_P(A)$. The following properties hold (see [107, Sec. 1.4]):

- If $A \sim B$, then $\mathcal{L}(A) \cong \mathcal{L}(B)$.
- If $\deg(A) < 0$, then $\ell(A) = 0$.
- If $A \leq B$, then $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ and $\dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq \deg(B) - \deg(A)$.

It can be shown ([107, Prop. 1.4.14]) that for any $A \in \mathrm{Div}(F)$ we have $\deg(A) + 1 - \ell(A) \leq m$ for some $m \in \mathbb{N}$ independent from $A$. Hence, the genus of $F$ is well-defined as follows.

**Definition 1.1.11.** *The* genus *of $F$ is*

$$g(F) := \max\{\deg(A) + 1 - \ell(A) \mid A \in \mathrm{Div}(F)\} \geq 0.$$

**Remark 1.1.12.** *The rational function field $K(x)$ has genus zero.*

We show how the genus of $F$ is related to the divisors of $F$; see [107, Sect. 1.5] for more details. Let $\Omega_F$ be the differential module of $F$, that is, $\Omega_F := \{zdx \mid z \in F\}$, where $dx$ is the differential of a separating element $x \in F$. For any $\omega \in \Omega_F$ and $P \in \mathbb{P}(F)$ we can define the valuation $v_P(\omega)$ of $\omega$ at $P$, and consequently the well-defined divisor

$$div(\omega) = \sum_{P \in \mathbb{P}(F)} v_P(\omega)P \ \in \mathrm{Div}(F).$$

The divisor $div(\omega)$ is a so-called *canonical divisor.*

**Proposition 1.1.13.** ([107, Cor. 1.5.16]) *For any canonical divisor $W$ of $F$,*

$$\deg(W) = 2g(F) - 2.$$

**Riemann-Roch Theorem.** ([107, 1.5.15]) *Let $W$ a canonical divisor of $F$. Then, for any $A \in \mathrm{Div}(F)$,*

$$\ell(A) = \deg(A) + 1 - g(F) + \ell(W - A).$$

One of the consequences of the Riemann-Roch Theorem is the Weierstrass Gap Theorem about the divisors supported at one rational place.

**Definition 1.1.14.** *Let $P$ be a place of $F$. The subsemigroup*

$$H(P) := \{n \in \mathbb{N} \mid \ \textit{there exists} \ \ z \in F \ \ \textit{with} \ \ (z)_\infty = nP\}$$

*of $\mathbb{N}$ is called the* Weierstrass semigroup *at $P$. The elements of $H(P)$ and $G(P) := \mathbb{N} \setminus H(P)$ are called* non-gaps *and* gaps *at $P$, respectively.*

**Weierstrass Gap Theorem.** *Let $g$ be the genus of $F$ and $P$ be a rational place of $F$. Then there are exactly $g$ gaps at $P$. The smallest gap is $1$, and the greatest gap is strictly smaller than $2g$.*

Now we recall some basic properties of extensions of function fields. In the following, $F'$ denotes another function field over $K$ such that $F \subseteq F'$ and $F'/F$ is an algebraic extension.

**Definition 1.1.15.** *Let $P$ and $P'$ be places of $F$ and $F'$, respectively. If $P \subseteq P'$, we say that $P$* lies under *$P'$ and $P'$* lies over *$P$; in symbols, $P' \mid P$. In this case, the* relative degree *of $P'$ over $P$ is $f(P'|P) := [F'_{P'} : F_P]$.*

The following properties hold (see [107, Sec. 3.1]):

- For any $P' \in \mathbb{P}(F')$, there exists exactly one place $P \in \mathbb{P}(F)$ lying under $P'$.
- If $P' \in \mathbb{P}(F')$ lies over $P \in \mathbb{P}(F)$, then there exists a positive integer $e(P'|P)$, called the *ramification idex* of $P'$ over $P$, such that $v_{P'}(z) = e(P'|P) \cdot v_P(z)$ for all $z \in F$.
- If $F''$ is another function field over $K$ which is an algebraic extension of $F'$ and $P'' \in \mathbb{P}(F'')$ lies over $P'$, then

$$e(P''|P) = e(P''|P') \cdot e(P'|P), \quad f(P''|P) = f(P''|P') \cdot f(P'|P).$$

The ramification of places is related to the degree of the extension.

**Fundamental Equality.** ([107, Th. 3.1.11]) *If $F'$ is a finite extension of $F$, $P$ is a place of $F$, and $P'_1, \dots, P'_m$ are all the places of $F'$ lying over $P$, then*

$$\sum_{i=1}^{m} e(P'_i|P) \cdot f(P'_i|P) = [F' : F].$$

**Definition 1.1.16.** *Let $[F' : F] = n \in \mathbb{N}$. The place $P \in \mathbb{P}(F)$ is* unramified *(or* splits completely*) in $F'/F$ if there are exactly $n$ distinct places of $F'$ lying over $P$, with ramification index $1$; $P$ is* totally ramified *in $F'/F$ if there is just one place of $F'$ lying over $P$, with ramification index $n$.*

The genera of $F$ and $F'$ can be related by the Riemann-Hurwitz genus formula. To this aim, we start by the definition of the Different divisor.

**Definition 1.1.17.** (see [107, Sections 3.4, 4.3]) *Let $P \in \mathbb{P}(F)$ and $P' \in \mathbb{P}(F')$ with $P' \mid P$. The* Different exponent *of $P'$ over $P$ is defined by*

$$d_{P'} = d(P'|P) := -v_{P'}\left(\frac{dt}{dt'}\right),$$

*where $t$ and $t'$ are local parameters at $P$ and $P'$, respectively. We have that $d(P'|P) \geq 0$, and $d(P'|P) = 0$ for almost all $P \in \mathbb{P}(F)$. Therefore, the effective* Different divisor *of $F'/F$ is well-defined by*

$$\mathrm{Diff}(F'/F) := \sum_{P' \in \mathbb{P}(F')} d_{P'} P'.$$

The Different exponent $d(P'|P)$ satisfies the following properties, known as *Dedekind's Different theorem* ([107, Th. 3.5.1]):

1. $d(P'|P) = e(P'|P) - 1$ if and only if $p \nmid e(P'|P)$;
2. $d(P'|P) \geq e(P'|P)$ if and only if $p \mid e(P'|P)$.

In Case 1 $P'|P$ is said to be *tamely ramified*, in Case 2 $P'|P$ is *wildly ramified.*

**Riemann-Hurwitz genus formula.** ([107, Th. 3.4.13])

$$2g(F') - 2 = [F' : F](2g(F) - 2) + \deg(\mathrm{Diff}(F'/F)).$$

Now we define Galois extensions of function fields. Let $G$ be the subgroup

$$G := \mathrm{Aut}(F'/F) = \{\sigma : F' \to F' \text{ automorphism} \mid \sigma(z) = z \;\text{ for all }\; z \in F'\}$$

of the $K$-automorphism group $\mathrm{Aut}(F)$ of $F$. The extension $F'/F$ is *Galois* if $G$ has finite order $[F' : F]$. In this case we write $F = Fix(G) = F'^G$ for the fixed field of $G$ and $Gal(F'/F) := G$ for the Galois group of $F'/F$.

If $p \nmid |G|$, $F'/F$ is said to be a *tame* extension; otherwise, a *wild* extension.

**Remark 1.1.18.** ([107, Th. 3.7.1, Cor. 3.7.2]) *The Galois group $Gal(F'/F)$ acts naturally on the places of $F'$. For any place $P$ of $F$, $Gal(F'/F)$ acts transitively on the places of $F'$ lying over $P$, and $v_{\sigma(P)}(z) = v_P(\sigma^{-1}(z))$ for all $\sigma \in Gal(F'/F)$, $z \in F'$. This implies that places of $F'$ lying over the same place of $F$ have the same ramification index and Different exponent.*

**Definition 1.1.19.** *Let $F'/F$ be a Galois extension with Galois group $G$, and $P'$ be a place of $F'$. For every $i \in \mathbb{N}$ the $i$-*th ramification group *of $P'$ is*

$$G_{P'}^{(i)} := \{\sigma \in G \mid v_{P'}(\sigma(z) - z) \geq i + 1 \;\textit{ for all }\; z \in \mathcal{O}_{P'}\}.$$

*The $0$-th ramification group $G_{P'} := G_{P'}^{(0)}$ is the* stabilizer *of $P'$ in $G$.*

For the higher ramification groups the following hold ([107, Prop. 3.8.5]):

- $G_{P'}$ has order $|G_{P'}| = e(P'|P)$.
- $G_{P'}^{(i)} \subseteq G_{P'}^{(j)}$ for $i \geq j$, and $G_{P'}^{(k)} = \{id\}$ for $k$ sufficiently large.
- For any $i \geq 0$, $G_{P'}^{(i+1)}$ is a normal subgroup of $G_{P'}^{(i)}$.
- $G_{P'}^{(1)}$ is a $p$-group, and $G_{P'}^{(0)} = G_{P'}^{(1)} \rtimes H$, where $H$ is a cyclic group of order coprime to $p$.

- For any $i \geq 1$, $G_{P'}^{(i)}/G_{P'}^{(i+1)}$ is isomorphic to an additive subgroup of $F'_{P'}$; hence, if $p > 0$, then $G_{P'}^{(i)}/G_{P'}^{(i+1)}$ is an elementary abelian $p$-group.

The Different exponent is related to the ramification groups as follows.

**Hilbert's Different formula.** ([107, Th. 3.8.7]) *Let $F'/F$ be a Galois extension with Galois group $G$, and $P'$ be a place of $F'$. Then*

$$d_{P'} = \sum_{i=0}^{\infty} \big(|G_{P'}^{(i)}| - 1\big), \textit{ and hence } \quad \deg(\mathrm{Diff}(F'/F)) = \sum_{P' \in \mathbb{P}(F')} \sum_{i=0}^{\infty} \big(|G_{P'}^{(i)}| - 1\big).$$

In particular, for tame extensions, we have

$$\deg(\mathrm{Diff}(F'/F)) = \sum_{P' \in \mathbb{P}(F')} \big(|G_{P'}| - 1\big).$$

We present two special types of Galois extensions of function fields.

**Kummer extensions.** ([107, Prop. 3.7.3]) *Let $F$ be a function field over $K$, where $K$ contains a primitive $n$-th root of unity, with $n > 1$ and $n$ coprime to $p$. Suppose that $u \in F$ is an element satisfying*

$$u \neq w^d \;\textit{ for all }\; w \in F \;\textit{ and all divisors }\; d > 1 \;\textit{ of }\; n.$$

*Let*

$$F' = F(y) \quad \textit{with} \quad y^n = u.$$

*Then $F'$ is said to be a* Kummer *extension of $F$. Moreover,*

- *$T^n - u \in F[T]$ is the minimal polynomial of $y$ over $F$; hence $[F' : F] = n$. The extension $F'/F$ is Galois, with cyclic Galois group generated by $\sigma : y \mapsto \zeta y$, where $\zeta$ is a primitive $n$-th root of unity.*
- *If $P' \in \mathbb{P}(F')$ lies over $P \in \mathbb{P}(F)$, then*

$$e(P'|P) = \frac{n}{r_P} \;\textit{ and }\; d(P'|P) = \frac{n}{r_P} - 1, \;\textit{ where }\; r_P := \gcd(n, v_P(u)) > 0.$$

- *The genus of $F'$ is*

$$g(F') = 1 + n\left(g(F) - 1 + \frac{1}{2}\sum_{P \in \mathbb{P}(F)} \Big(1 - \frac{\gcd(n, v_P(u))}{n}\Big) \cdot \deg(P)\right).$$

**Generalized Artin-Schreier extensions.** ([107, Prop. 3.7.10]) *Let $F$ a function field over $K$ with $p>0$. Let $a(T)\in K[T]$ be an additive separable polynomial of degree $p^n$ having all its roots in $K$. Let $u\in F$. Suppose that for each $P\in\mathbb{P}(F)$ there is an element $z_P\in F$ such that*

$$v_P(u-a(z_P))\geq 0,\quad \textit{or}\quad v_P(u-a(z_P))=-m\ \ \textit{with}\ \ m>0\ \ \textit{and}\ \ p\nmid m.$$

*Define $m_P:=-1$ in the former case, $m_P:=m$ in the latter case. Then $m_P$ is well-defined. Let*

$$F'=F(y)\qquad \textit{with}\qquad a(y)=u.$$

*If there exists $Q\in\mathbb{P}(F)$ with $m_Q>0$, then $F'$ is said to be a* generalized Artin-Schreier *extension of $F$. Moreover,*

- *$a(T)-u\in F[T]$ is the minimal polynomial of $y$ over $F$; hence $[F':F]=p^n$. The extension $F'/F$ is Galois, and the Galois group is an elementary abelian $p$-group isomorphic to the additive group of roots of $a(T)$.*
- *Each $P\in\mathbb{P}(F)$ with $m_P=-1$ is unramified in $F'/F$.*
- *Each $P\in\mathbb{P}(F)$ with $m_P>0$ is totally ramified in $F'/F$, and*

$$d(P'|P)=(p^n-1)(m_P-1).$$

- *The genus of $F'$ is*

$$g(F')=p^n\cdot g(F)+\frac{p^n-1}{2}\left(-2+\sum_{P\in\mathbb{P}(F)}(m_P+1)\cdot\deg(P)\right).$$

### 1.1.2 Algebraic curves

In this section we recall some elementary facts about algebraic curves, and relate them to function fields. For the proofs and a general exposition, we refer to [40, 67].

Let $K$ be a perfect field, $\overline{K}$ be its algebraic closure, and $\mathrm{PG}(n,\overline{K})$ be the $n$-dimensional projective space over $\overline{K}$. Let $V\subseteq\mathrm{PG}(n,\overline{K})$ be a *projective algebraic set*, that is, $V$ is the set of points of $\mathrm{PG}(n,\overline{K})$ on which a certain subset of $\overline{K}[X_0,X_1,\ldots,X_n]$ vanishes. The *ideal* $I(V)$ of $V$ is the homogeneous ideal of $\overline{K}[X_0,\ldots,X_n]$ generated by all homogeneous polynomials vanishing on $V$. The set $V$ is *irreducible over* $\overline{K}$ if and only if $I(V)$ is a prime ideal in $\overline{K}[X_0,\ldots,X_n]$; being $\overline{K}$ algebraically closed, we also say that $V$ is *absolutely irreducible* or *geometrically irreducible*. If $V$ is an absolutely irreducible projective algebraic set, then $V$ is called a (absolutely irreducible, projective, algebraic) *variety*.

**Definition 1.1.20.** *If $I(V)$ can be generated by polynomials in $K[X_0,\dots,X_n]$, then the variety $V$ is said to be* defined over $K$*. The $K$-*rational points *of $V$ are the points of $V$ whose homogeneous coordinates can be chosen in $K$.*

In the following, $V$ will denote a variety over $K$ in $\mathrm{PG}(n,\overline{K})$.

**Definition 1.1.21.** *The* homogeneous coordinate ring $\overline{K}[V]$ *of $V$ is defined as $\overline{K}[X_0,\dots,X_n]/I(V)$, and the* function field $\overline{K}(V)$ *of $V$ is the subfield of the field of fractions of $\overline{K}[V]$ defined by*

$$\overline{K}(V) := \left\{ \frac{F+I(V)}{G+I(V)} \mid F,G \textit{ are homogeneous}, \deg(F)=\deg(G), G\notin I(V) \right\}.$$

Let $f\in\overline{K}(V)$, $f:=(F+I(V))/(G+I(V))$, and $P\in V$. If $G(P)\neq 0$, then $f(P):=F(P)/G(P)\in\overline{K}$ and $f$ is *regular* at $P$; the *local ring* of $V$ at $P$ is

$$\overline{K}[V]_P := \{f\in\overline{K}(V) \mid f \text{ is regular at } P\}.$$

It is a local ring with maximal ideal $M_P := \{f\in\overline{K}[V]_P \mid f(P)=0\}$. The *$K$-rational function field* of $V$ can be defined in a similar way.

Let $\mathrm{AG}(n,\overline{K})$ be the $n$-dimensional affine space over $\overline{K}$ with coordinates $X_1/X_0$, …, $X_n/X_0$. Then we can define in a similar way affine varieties of $\mathrm{AG}(n,\overline{K})$, their coordinate rings, local rings, and function fields. If $V_a$ is the affine variety associated with $V$ and $P_a\in V_a$ is the affine point corresponding to $P\in V$, then there is a natural isomorphism $\overline{K}(V_a)\cong\overline{K}(V)$ which induces an isomorphism $\overline{K}[V_a]_{P_a}\cong\overline{K}[V]_P$.

The *dimension* of $V$ is the transcendence degree of $\overline{K}(V)/\overline{K}$; if $V$ has dimension 1, it is a *curve*. Hereafter, $\mathcal{X}$ denotes a curve in $\mathrm{PG}(n,\overline{K})$ defined over $K$; we also require that $\mathcal{X}$ is non-degenerate, that is, $\mathcal{X}$ is not contained in any hyperplane of $\mathrm{PG}(n,\overline{K})$.

Clearly, $\overline{K}(\mathcal{X})$ is generated over $\overline{K}$ by $x_1,\dots,x_n$, where $x_i:=(X_i+I(V))/(X_0+I(V))$ is the *$i$-th coordinate function*. By [80, Th. X.1] there is a $j\in\{1,\dots,n\}$ such that the extension $\overline{K}(\mathcal{X})/\overline{K}(x_j)$ is finite and separable. By the Theorem of the Primitive Element ([67, Th. A.1]) we have $\overline{K}(\mathcal{X})=\overline{K}(x_j,y)$, where $y\in\overline{K}(\mathcal{X})$ satisfies $F(x_j,y)=0$ with $F\in\overline{K}[X,Y]$ such that $F(x_j,T)\in\overline{K}(x_j)[T]$ is separable; since $\mathcal{X}$ is defined over $K$, we can also assume $F\in K[X,Y]$.

Note that $\overline{K}(\mathcal{X})$ is a function field over $\overline{K}$, in the sense of Definition 1.1.1. Conversely, given a function field F over $\overline{K}$, we argue as above to conclude that $F=\overline{K}(x,y)$, where $x$ is transcendent over $\overline{K}$ and $y$ satisfies $F(x,y)=0$ for some $F\in\overline{K}[X,Y]$ separable in $Y$; hence, $F$ is isomorphic to the function field of the plane curve $\mathcal{X}$ defined by $F(X,Y)=0$.

The points of $\mathcal{X}$ are related to the places of its function field.

**Definition 1.1.22.** *A point $P \in \mathcal{X}$ is called* non-singular *(or* simple*) if the local ring $\overline{K}[\mathcal{X}]_P$ is a discrete valuation ring of $\overline{K}(\mathcal{X})$.*

Definition 1.1.22 is consistent with the Jacobi-criterion for plane curves and with the usual definition of singularity. Moreover, the following holds.

**Proposition 1.1.23.** [67, Th. 4.32] *For any DVR $\mathcal{O}$ of $\overline{K}(\mathcal{X})$, there exists exactly one point $P \in \mathcal{X}$ (called the* center *of $\mathcal{O}$) such that $\overline{K}[\mathcal{X}]_P \subseteq \mathcal{O}$ and the maximal ideal of $\overline{K}[\mathcal{X}]_P$ is the restriction to $\overline{K}[\mathcal{X}]_P$ of the place of $\mathcal{O}$.*

Proposition 1.1.23 implies that the points of a non-singular curve are in $1-1$ correspondence with the places of its function field. We shall always identify a simple point $P$ of $\mathcal{X}$ with the place of $\overline{K}(\mathcal{X})$ centered at $P$. If a point is singular with multiplicity $m$ (in the usual sense), then it is the center of at most $m$ places ([67, Th. 4.36]).

**Remark 1.1.24.** [67, Th. 8.29, 8.31] *If a place is $K$-rational (i.e., it has degree $1$ over $K$), then its center is $K$-rational; conversely, if a point is simple and $K$-rational, then the corresponding place is $K$-rational.*

**Definition 1.1.25.** *The set of $K$-rational places of $\mathcal{X}$ is denoted by $\mathcal{X}(K)$.*

If $\mathcal{X}$ is a plane curve and $\mathcal{C}$ is another plane curve (eventually reducible), then we can define in a standard way the *intersection multiplicity* $\mathcal{I}(\mathcal{X} \cap \mathcal{C}, P)$ of $\mathcal{X}$ and $\mathcal{C}$ at a point $P \in \mathrm{PG}(2, \overline{K})$; see [67, Chapt. 3.1].

**Proposition 1.1.26.** ([67, Th. 4.36]) *Suppose that $\mathcal{X} : F(X,Y) = 0$ is a plane curve, $P$ is a simple point of $\mathcal{X}$, and $\alpha = \frac{G(x,y)}{H(x,y)} \in \overline{K}(\mathcal{X})$. Let $\mathcal{G}$ and $\mathcal{H}$ be the plane curves defined by $G(X,Y) = 0$ and $H(X,Y) = 0$, respectively. Then*

$$v_P(\alpha) = \mathcal{I}(\mathcal{X} \cap \mathcal{G}, P) - \mathcal{I}(\mathcal{X} \cap \mathcal{H}, P).$$

Recall that the *order* (or *degree*) of $\mathcal{X}$ is the number of intersections (counted with multiplicity) of $\mathcal{X}$ with an hyperplane of $\mathrm{PG}(n, \overline{K})$; if $\mathcal{X}$ is a plane curve defined by $F \in \overline{K}[X,Y]$, then the order of $\mathcal{X}$ coincides with the degree of $F$.

**Bézout's Theorem.** ([67, Th. 3.14]) *If $\mathcal{Y}$ and $\mathcal{Z}$ are two (eventually reducible) plane curves of order $d_1$ and $d_2$, then*

$$\sum_{P \in \mathrm{PG}(2,\overline{K})} \mathcal{I}(\mathcal{Y} \cap \mathcal{Z}, P) = d_1 d_2.$$

The *genus* $g(\mathcal{X})$ of $\mathcal{X}$ is defined to be the genus of its function field $\overline{K}(\mathcal{X})$.

**Proposition 1.1.27.** ([67, Th. 5.57]) *Let $\mathcal{X}$ be a plane curve of order $d$. Let $P_1, \dots, P_k$ be the singular points of $\mathcal{X}$ with multiplicities $m_1, \dots, m_k$. Then*

$$g(\mathcal{X}) \leq \frac{(d-1)(d-2)}{2} - \frac{1}{2}\sum_{i=1}^{k} m_i(m_i - 1). \tag{1.1}$$

*Equality in* (1.1) *holds if and only if all singular points of $\mathcal{X}$ are ordinary, i.e. there are $m_i$ distinct tangent lines to $\mathcal{X}$ at $P_i$, $i = 1, \dots, k$.*

Now we define rationals maps between curves and show that they correspond to algebraic extensions of function fields.

**Definition 1.1.28.** *A* rational map *of $\mathcal{X}$ into* $\mathrm{PG}(r, \overline{K})$ *is an element*

$$\varphi = (F_0 : F_1 : \dots : F_r) \in \mathrm{PG}(r, \overline{K}(\mathcal{X})).$$

*If $\varphi \in \mathrm{PG}(r, K(\mathcal{X}))$, then $\varphi$ is said to be $K$-*rational *(or* defined over $K$*). The rational map $\varphi$ is* defined *(or* regular*) at $P \in \mathcal{X}$ if the image $\varphi(P)$ is defined, that is, there exists $\rho \in \overline{K}(\mathcal{X})^*$ such that $\rho F_i \in \overline{K}[\mathcal{X}]_P$ for all $i$ and $\rho F_i(P) \neq 0$ for some $i$; in this case, $\varphi(P)$ is well-defined. We write $\varphi(\mathcal{X})$ for $\{\varphi(P) \mid \varphi$ is defined at $P\}$. If $\varphi$ is defined at every point of $\mathcal{X}$, then $\varphi$ is a* morphism*.*

**Remark 1.1.29.** *A rational map $\varphi$ of $\mathcal{X}$ into* $\mathrm{PG}(3, \overline{K})$ *is defined at every simple point of $\mathcal{X}$* [67, Th. 5.17]*. If $\varphi$ is non-constant, then there exists a unique curve $\mathcal{Y}$ of* $\mathrm{PG}(r, \overline{K})$ *such that $\varphi(\mathcal{X}) \subseteq \mathcal{Y}$* [67, Th. 5.16]*; in this case, we write $\varphi : \mathcal{X} \to \mathcal{Y}$.*

**Definition 1.1.30.** *If $\varphi : \mathcal{X} \to \mathcal{Y}$ is a ($K$-)rational map, then we say that $\varphi$ is a* ($K$-)covering*, $\mathcal{X}$ is a* ($K$-)cover *of $\mathcal{Y}$, and $\mathcal{Y}$ is a* ($K$-)subcover *of $\mathcal{X}$.*

Let $\varphi = (F_0 : \dots : F_r) : \mathcal{X} \to \mathcal{Y}$ and $\psi = (G_0 : \dots : G_s) : \mathcal{Y} \to \mathcal{Z}$ be two rational maps. Then the *composition* is defined as

$$\psi \circ \varphi : \mathcal{X} \to \mathcal{Z}, \quad \psi \circ \varphi := (G_0(F_0, \dots, F_r) : \dots : G_s(F_0, \dots, F_r)).$$

Suppose that $F_0 \neq 0$. For $i = 1, \dots, r$, let $f_i := F_i/F_0$ and let $y_1, \dots, y_r$ be the coordinate functions of $\mathcal{Y}$. Then

$$\varphi^* : \overline{K}(\mathcal{Y}) \to \overline{K}(\mathcal{X}), \quad \varphi^*\left(\frac{g(y_1, \dots, y_r)}{h(y_1, \dots, y_r)}\right) := \frac{g(f_1/f_0, \dots, g_r/g_0)}{h(f_1/f_0, \dots, f_r/f_0)}$$

is a well-defined field $\overline{K}$-homomorphism, the *pull-back* of $\varphi$.

**Remark 1.1.31.** *Let $\mathcal{G}$ be the category of curves and rational maps, and $\mathcal{A}$ be the category of function fields and field homomorphisms. Then the pull-back is a controvariant functor of $\mathcal{G}$ into $\mathcal{A}$.*

**Definition 1.1.32.** *If $\varphi : \mathcal{X} \to \mathcal{Y}$ is an invertible morphism in the category $\mathcal{G}$ defined in Remark* 1.1.31*, then $\varphi$ is called a* birational map*, and the curves $\mathcal{X}$ and $\mathcal{Y}$ are said to be* birationally equivalent*; if the birational map $\varphi$ is a morphism, then $\mathcal{X}$ and $\mathcal{Y}$ are said to be* isomorphic.

**Corollary 1.1.33.** *The curves $\mathcal{X}$ and $\mathcal{Y}$ are birationally equivalent if and only if their function fields $\overline{K}(\mathcal{X})$ and $\overline{K}(\mathcal{Y})$ are $\overline{K}$-isomorphic.*

**Remark 1.1.34.** *Since every function field is $\overline{K}$-isomorphic to the function field of a plane curve, we have that every curve is birationally equivalent to a plane curve.*

*It can be also shown (*[67, Remark 8.30]*) that every curve is birationally equivalent to a non-singular curve (in some possibly higher dimensional space), which is said to be a non-singular model of the curve.*

If $\varphi : \mathcal{X} \to \mathcal{Y}$ is a rational map and $P_{\mathcal{X}}$ is a place of $\mathcal{X}$, then there is exactly one place $P_{\mathcal{Y}}$ of $\mathcal{Y}$ such that $\varphi^*(P_{\mathcal{Y}}) \subseteq P_{\mathcal{X}}$ ([67, Th. 5.18]). In this case, we define $\hat{\varphi}(P_{\mathcal{X}}) := P_{\mathcal{Y}}$.

Since no confusion arises, we will always indicate the maps $\varphi$, $\varphi^*$, and $\hat{\varphi}$ with the same symbol $\varphi$. We will also identify $\overline{K}(\mathcal{Y})$ with its $\overline{K}$-isomorphic image $\varphi^*(\overline{K}(\mathcal{Y})) \subseteq \overline{K}(\mathcal{X})$.

Therefore, the rational maps $\varphi : \mathcal{X} \to \mathcal{Y}$ will be studied through the theory of algebraic extensions $\overline{K}(\mathcal{X})/\overline{K}(\mathcal{Y})$ of function fields. In particular, the $\overline{K}$-automorphism group of the function field $\overline{K}(\mathcal{X})$ will be identified with the automorphism group $\mathrm{Aut}(\mathcal{X})$ of the curve.

**Definition 1.1.35.** *A rational map $\varphi : \mathcal{X} \to \mathcal{Y}$ is said to be a* Galois covering *if $\overline{K}(\mathcal{X})/\overline{K}(\mathcal{Y})$ is a Galois extension. If $\varphi : \mathcal{X} \to \mathcal{Y}$ is a Galois covering with Galois group $G$, then $\mathcal{Y}$ is called the* quotient curve *of $\mathcal{X}$ over $G$ and is denoted by $\mathcal{X}/G$.*

Clearly, if two automorphism groups $G, G' \leq \mathrm{Aut}(\mathcal{X})$ are conjugated in $\mathrm{Aut}(\mathcal{X})$, then the quotient curves $\mathcal{X}/G$ and $\mathcal{X}/G'$ are isomorphic.

The following lemma for curves over finite fields will be useful.

**Lemma 1.1.36.** *Let $\mathcal{C}$ be a curve defined over the finite field $\mathbb{F}_q$ and consider the function field $\mathbb{F}_q(\mathcal{C})$ with constant field $\mathbb{F}_q$. Suppose that $f \in \mathbb{F}_q(\mathcal{C})[T]$ is a polynomial irreducible over $\overline{\mathbb{F}}_q(\mathcal{C})[T]$ and $z$ is a root of $f$. Then $\mathbb{F}_q$ is the full constant field of $\mathbb{F}_q(\mathcal{C})(z)$.*

*Proof.* Let $\mathbb{F}_{q'}$ be the constant field of $\mathbb{F}_q(\mathcal{C})(z)$ over $\mathbb{F}_q$. Then

$$\mathbb{F}_q(\mathcal{C}) \subseteq \mathbb{F}_{q'}(\mathcal{C}) \subseteq \mathbb{F}_{q'}(\mathcal{C})(z) = \mathbb{F}_q(\mathcal{C})(z).$$

Since $f$ is irreducible over $\mathbb{F}_{q'}(\mathcal{C})$, then $[\mathbb{F}_{q'}(\mathcal{C})(z) : \mathbb{F}_{q'}(\mathcal{C})] = \deg(f) = [\mathbb{F}_q(\mathcal{C})(z) : \mathbb{F}_q(\mathcal{C})]$, hence $[\mathbb{F}_{q'}(\mathcal{C}) : \mathbb{F}_q(\mathcal{C})] = 1$ and $\mathbb{F}_{q'} = \mathbb{F}_q$ . □

### 1.1.3 Algebraic-Geometric codes

In this section we use the function field notation to introduce Algebric-Geometric codes, briefly AG codes. They generalize several previously known families of linear codes; see [117] for an introduction to coding theory. AG codes were firstly introduced by Goppa [57, 58], and thus are nowadays referred to also as Goppa codes; see [113] for a detailed introduction to AG codes.

**Definition 1.1.37.** *Let $\mathbb{F}_q$ be the finite field with $q$ elements. A* linear $[n, k, d]_q$-code *is an $\mathbb{F}_q$-vector subspace $C$ of $\mathbb{F}_q^n$. The elements of $C$ are called* codewords*, $n$ is the* length *of $C$, $k$ is the* dimension *of $C$ as an $\mathbb{F}_q$-vector space, and $d$ is the* minimum distance*. This means that $d$ is the minimum number of entries in which any two distinct codewords differ; equivalently, $d$ is the minimum number of entries in which a codeword is non-zero. The* Singleton defect *is the integer $\delta := n + 1 - k - d$. The* Singleton bound *$\delta \geq 0$ holds. The* dual code *$C^\perp$ of $C$ is the subspace of $\mathbb{F}_q^n$ orthogonal to $C$ with respect to the canonical inner product of $\mathbb{F}_q^n$.*

Let $F$ be a function field of genus $g$ over the finite field $\mathbb{F}_q$ with $q$ elements and characteristic $p > 0$. Let $P_1, \ldots, P_n \in \mathbb{P}(F)$ be $n$ distinct $\mathbb{F}_q$-rational places of $F$, $D$ be the divisor $P_1 + \ldots + P_n$, and $G$ be another $\mathbb{F}_q$-rational divisor such that $\mathrm{supp}(G) \cap \mathrm{supp}(D) = \emptyset$.

Consider the evaluation map

$$\begin{array}{rccl} e_D : & \mathcal{L}(G) & \to & \mathbb{F}_q^n \\ & f & \mapsto & e_D(f) = (f(P_1), f(P_2), \ldots, f(P_n)) \end{array} .$$

The map $e_D$ is $\mathbb{F}_q$-linear. The *functional AG code* is $C_{\mathcal{L}}(D, G) := e_D(\mathcal{L}(G))$.

**Proposition 1.1.38.** ([107, Th. 2.2.2, Cor. 2.2.3]) *The $[n, k, d]_q$-code $C_{\mathcal{L}}(D, G)$ satisfies the following properties:*

- *$k = \ell(G) - \ell(G - D)$, $d \geq n - \deg(G)$.*
- *If $n > \deg(G)$, then $e_D$ is injective and $k = \ell(G)$.*

- *If* $n > \deg(G) > 2g-2$, *then* $k = \deg(G) + 1 - g$.

The integer $d^* := n - \deg(G)$ is called the *designed minimum distance* of $C_{\mathcal{L}}(D,G)$. The *differential AG code* is

$$C_\Omega(D,G) := \{(res_{P_1}(\omega), \dots, res_{P_n}(\omega)) \mid \omega \in \Omega_F(G-D)\},$$

where $\Omega_F$ is the differential module of $F$, $\Omega_F(G-D) = \{\omega \in \Omega_F \mid div(\omega) \geq G-D\} \cup \{0\}$, and $res_P(\omega)$ is the residue of $\omega$ at $P$; see [107, Section 8.1].

**Proposition 1.1.39.** ([107, Th. 2.2.7, 2.2.8]) *The* $[\bar{n}, \bar{k}, \bar{d}]_q$*-code* $C_\Omega(D,G)$ *satisfies the following properties:*

- $C_\Omega(D,G) = C_{\mathcal{L}}(D,G)^\perp$.
- $\bar{k} = i(G-D) - i(G)$, *where* $i(A) = \ell(A) - \deg(A) + g - 1$.
- $\bar{d} \geq \bar{d}^* := \deg(G) - (2g-2)$.
- *If* $\deg(G) > 2g-2$, *then* $\bar{k} = i(G-D) \geq \bar{n} + g - 1 - \deg(G)$.
- *If* $n > \deg(G) > 2g-2$, *then* $\bar{k} = \bar{n} + g - 1 \deg(G)$.

In the construction of AG codes, the condition $\mathrm{supp}(D) \cap \mathrm{supp}(G) = \emptyset$ can be removed as follows; see [113, Sec. 3.1.1]. For any $P_i \in \mathrm{supp}(D)$ let $b_i$ be the weight of $P_i$ in $G$ and $t_i \in F$ be a local parameter at $P_i$. The map

$$\begin{array}{llll} e'_D: & \mathcal{L}(G) & \to & \mathbb{F}_q^n \\ & f & \mapsto & e'_D(f) = ((t^{b_1}f)(P_1), (t^{b_2}f)(P_2), \dots, (t^{b_n}f)(P_n)) \end{array}$$

is linear. The *extended AG code* is $C_{ext}(D,G) := e'(\mathcal{L}(G))$. Note that $e'_D$ is not well-defined since it depends on the choice of the local parameters; yet, different choices yield extended AG codes which are equivalent. The code $C_{ext}(D,G)$ is a lengthening of $C_{\mathcal{L}}(\hat{D},G)$, where $\hat{D}$ is the sum of the places in $\mathrm{supp}(D) \setminus \mathrm{supp}(G)$.

**Remark 1.1.40.** *For the* $[n', k', d']_q$*-code* $C_{ext}(D,G)$ *the following holds:*

- $k' = \ell(G) - \ell(G-D)$, $d' \geq n' - \deg(G)$.
- *If* $n' > \deg(G)$, *then* $e'_D$ *is injective and* $k' = \deg(G)$.
- *If* $n' > \deg(G) > 2g-2$, *then* $k' = \deg(G) + 1 - g$.

We present some results which improve the bounds on the parameters of the differential code $C_\Omega(D,G)$, through the concept of pure gaps at many places of $F$; see [21, 70] and the references therein. To this aim, we start by generalizing the notion of Weierstrass semigroup.

**Definition 1.1.41.** *Let $Q_1, \dots, Q_s$ be distinct $\mathbb{F}_q$-rational places of $F$. The* Weierstrass semigroup *at $Q_1 \dots, Q_s$ is the subsemigroup*

$$H(Q_1, \dots, P_s) := \{(n_1, \dots, n_s) \in \mathbb{N}^s \mid \exists z \in F \text{ with } (z)_\infty = n_1Q_1 + \cdots + n_sQ_s\}$$

*of $\mathbb{N}^s$, whose elements are the* non-gaps *at $Q_1 \dots, Q_s$; the elements of the complement $G(Q_1, \dots, Q_s) = \mathbb{N}^s \setminus H(Q_1, \dots, Q_s)$ are the* gaps *at $Q_1 \dots, Q_s$.*

From [21, Lemma 2.2], an $s$-tuple $(n_1, \dots, n_s) \in \mathbb{N}^s$ is a gap at $Q_1, \dots, Q_s$ if and only if $\ell\big(\sum_{i=1}^s n_iQ_i\big) = \ell\big((\sum_{i=1}^s n_iQ_i) - Q_j\big)$ for some $j \in \{1, \dots, s\}$.

For $s = 1$ there are exactly $g$ gaps at $Q_1$, by the Weierstrass Gap Theorem. For $s \geq 2$ the number of gaps may vary depending on the choice of the places. When $s = 2$ the size of $G(Q_1, Q_2)$ was given in [70] in terms of $G(Q_1)$ and $G(Q_2)$, as follows. Let $1 = a_1 < a_2 < \cdots < a_g$ and $1 = b_1 < b_2 < \cdots < b_g$ be the gap sequences at $Q_1$ and $Q_2$, respectively. For $i = 1, \dots, g$, let $\gamma(a_i) := \min\{b \in G(P_2) \mid (a_i, b) \in H(Q_1, Q_2)\}$; by [76, Lemma 2.6], $\{\gamma(a_i) \mid i = 1, \dots, g\} = G(Q_2)$. Therefore, there is a permutation $\sigma$ of the set $\{1, \dots, g\}$ such that $\gamma(a_i) = b_{\sigma(i)}$, and

$$\Gamma(Q_1, Q_2) := \{(a_i, b_{\sigma(i)}) \mid i = 1, \dots, g\}$$

is the graph of a bijective map $\gamma$ between $G(Q_1)$ and $G(Q_2)$. Define

$$r(Q_1, Q_2) := |\{(x, y) \in \Gamma(Q_1, Q_2) \mid x < y, \gamma(x) > \gamma(y)\}|.$$

**Theorem 1.1.42** ([70, Th. 1])**.** *Under the above notation, the number of gaps at $Q_1, Q_2$ is*

$$|G(Q_1, Q_2)| = \sum_{i=1}^{g} a_i + \sum_{i=1}^{g} b_i - r(Q_1, Q_2).$$

A characterization of $\Gamma(Q_1, Q_2)$ is the following.

**Lemma 1.1.43** ([70, Lemma 2])**.** *Let $\Gamma'$ be a subset of $(G(Q_1) \times G(Q_2)) \cap H(Q_1, Q_2)$. If there exists a permutation $\tau$ of $\{1, \dots, g\}$ such that $\Gamma' = \{(a_i, b_{\tau(i)}) \mid i = 1, \dots, g\}$, then $\Gamma' = \Gamma(Q_1, Q_2)$.*

The Weierstrass semigroup $H(Q_1, Q_2)$ can be recovered from $\Gamma(Q_1, Q_2)$ as follows. For $\mathbf{x} = (a_1, b_1), \mathbf{y} = (a_2, b_2) \in \mathbb{N}^2$, define the *least upper bound* of $\mathbf{x}$ and $\mathbf{y}$ as $\mathrm{lub}(\mathbf{x}, \mathbf{y}) := (\max\{a_1, a_2\}, \max\{b_1, b_2\})$. By [76, Lemma 2.2],

$$H(Q_1, Q_2) = \{\mathrm{lub}(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in \Gamma(Q_1, Q_2) \cup (H(Q_1) \times \{0\}) \cup (\{0\} \times H(Q_2))\}. \quad (1.2)$$

**Definition 1.1.44.** *An $s$-tuple $(n_1,\dots,n_s)\in\mathbb{N}^s$ is a* pure gap *at $Q_1,\dots,Q_s$ if*

$$\ell\Big(\sum_{i=1}^{s} n_iQ_i\Big)=\ell\Big(\big(\sum_{i=1}^{s} n_iQ_i\big)-Q_j\Big)\text{ for all } j=1,\dots,s.$$

*The set of pure gaps at $Q_1,\dots,Q_s$ is denoted by $G_0(Q_1,\dots,Q_s)$.*

Clearly, a pure gap is always a gap.

**Lemma 1.1.45** ([21, Lemma 2.5])**.** *An $s$-tuple $(n_1,\dots,n_s)$ is a pure gap at $Q_1,\dots,Q_s$ if and only if $\ell\big(\sum_{i=1}^{s} n_iQ_i\big)=\ell\big(\sum_{i=1}^{s}(n_i-1)Q_i\big)$.*

Finally, the following results shows how pure gaps can be used to improve the minimum distance of differential codes.

**Theorem 1.1.46** ([21, Theorem 3.4])**.** *Let $Q_1,\dots,Q_s,P_1,\dots,P_n$ be pairwise distinct $\mathbb{F}_q$-rational places of $F$ and $(a_1,\dots,a_s),(b_1,\dots,b_s)\in\mathbb{N}^s$ be two pure gaps at $Q_1,\dots,Q_s$. Consider the divisors $D=P_1+\dots+P_n$ and $G=\sum_{i=1}^{s}(a_i+b_i-1)Q_i$. Suppose that $a_i\le b_i$ for all $i=1,\dots,s$, and that each $s$-tuple $(c_1,\dots,c_s)\in\mathbb{N}^s$ with $a_i\le c_i\le b_i$ for $i=1,\dots,s$ is also a pure gap at $Q_1,\dots,Q_s$. Then the minimum distance $d$ of $C_\Omega(D,G)$ satisfies*

$$d\ge \deg(G)-(2g-2)+s+\sum_{i=1}^{s}(b_i-a_i).$$

Now we define the automorphism group of $C_{\mathcal{L}}(D,G)$; see [52, 74]. Here we make use of algebraic curves, namely, of a curve $\mathcal{X}$ defined over $\mathbb{F}_q$ whose function field $\mathbb{F}_q(\mathcal{X})$ is equal to $F$.

Let $\mathcal{M}_{n,q}\le \mathrm{GL}(n,q)$ be the subgroup of matrices having exactly one non-zero element in each row and column. For $\gamma\in\mathrm{Aut}(\mathbb{F}_q)$ and $M=(m_{i,j})_{i,j}\in\mathrm{GL}(n,q)$, let $M^\gamma$ be the matrix $(\gamma(m_{i,j}))_{i,j}$. Let $\mathcal{W}_{n,q}$ be the semidirect product $\mathcal{M}_{n,q}\rtimes\mathrm{Aut}(\mathbb{F}_q)$ with multiplication $M_1\gamma_1\cdot M_2\gamma_2:=M_1M_2^\gamma\cdot\gamma_1\gamma_2$, acting on $\mathbb{F}_q^n$ by $M\gamma(x_1,\dots,x_n):=((x_1,\dots,x_n)\cdot M)^\gamma$. The *automorphism group* $\mathrm{Aut}(C_{\mathcal{L}}(D,G))$ of $C_{\mathcal{L}}(D,G)$ is the subgroup of $\mathcal{W}_{n,q}$ preserving $C_{\mathcal{L}}(D,G)$. Let $\mathrm{Aut}_{\mathbb{F}_q}(\mathcal{X})$ be the $\mathbb{F}_q$-automorphism group of $\mathcal{X}$, and

$$\mathrm{Aut}_{\mathbb{F}_q,D,G}(\mathcal{X}):=\{\sigma\in\mathrm{Aut}_{\mathbb{F}_q}(\mathcal{X})\mid \sigma(D)=D,\,\sigma(G)\approx_D G\},$$

where $G'\approx_D G$ if and only if there exists $u\in\mathbb{F}_q(\mathcal{X})$ such that $G'-G=(u)$ and $u(P_i)=1$ for $i=1,\dots,n$, and let

$$\mathrm{Aut}^+_{\mathbb{F}_q,D,G}(\mathcal{X}):=\{\sigma\in\mathrm{Aut}_{\mathbb{F}_q}(\mathcal{X})\mid \sigma(D)=D,\,\sigma(|G|)=|G|\},$$

where $|G|=\{G+(f)\mid f\in\mathcal{L}(G)\}$ is the linear series associated with $G$. Note that $\mathrm{Aut}_{\mathbb{F}_q,D,G}(\mathcal{X})\subseteq\mathrm{Aut}^+_{\mathbb{F}_q,D,G}(\mathcal{X})$.

**Proposition 1.1.47.** *Let $N \in \mathbb{N}$ be such that any non-trivial element of $\mathrm{Aut}_{\mathbb{F}_q}(\mathcal{X})$ fixes at most $N$ $\mathbb{F}_q$-rational places of $\mathcal{X}$. If $n > N$, then $\mathrm{Aut}(C_{\mathcal{L}}(D,G))$ contains a subgroup isomorphic to*

$$(\mathrm{Aut}_{\mathbb{F}_q,D,G}(\mathcal{X}) \rtimes \mathrm{Aut}(\mathbb{F}_q)) \rtimes \mathbb{F}_q^*.$$

*Proof.* Arguing as in the proof of [107, Proposition 8.2.3 (b)], we obtain for $n > N$ a subgroup of $\mathrm{Aut}(C_{\mathcal{L}}(D,G))$ isomorphic to $\mathrm{Aut}_{\mathbb{F}_q,D,G}(\mathcal{X})$. As in [52], an automorphism group of $C_{\mathcal{L}}(D,G)$ isomorphic to $(\mathrm{Aut}_{\mathbb{F}_q,D,G}(\mathcal{X}) \rtimes \mathrm{Aut}(\mathbb{F}_q)) \rtimes \mathbb{F}_q^*$ is then constructed via semilinear and scalar matrices. □

**Remark 1.1.48.** *Suppose that* $\mathrm{supp}(D) \cup \mathrm{supp}(G) = \mathcal{X}(\mathbb{F}_q)$ *and each place in* $\mathrm{supp}(G)$ *has the same weight in $G$. Then*

$$\mathrm{Aut}_{\mathbb{F}_q,D,G}(\mathcal{X}) = \mathrm{Aut}^+_{\mathbb{F}_q,D,G}(\mathcal{X}) = \{\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(\mathcal{X}) \mid \sigma(\mathrm{supp}(G)) = \mathrm{supp}(G)\}.$$

**Theorem 1.1.49.** ([52, Th. 3.4]) *Suppose that the following conditions hold:*

- *$G$ is effective;*
- *$\ell(G-P) = \ell(G)-1$ and $\ell(G-P-Q) = \ell(G)-2$ for any $P, Q \in \mathcal{X}$;*
- *$\mathcal{X}$ has a plane model $\Pi(\mathcal{X})$ with coordinate functions $x, y \in \mathcal{L}(G)$;*
- *$\mathcal{X}$ is defined over $\mathbb{F}_p$;*
- $\mathrm{supp}(D)$ *is preserved by the Frobenius morphism $(x,y) \mapsto (x^p, y^p)$;*
- *$n > \deg(G) \cdot \deg(\Pi(\mathcal{X}))$.*

*Then*

$$\mathrm{Aut}(C_{\mathcal{L}}(D,G)) \cong (\mathrm{Aut}^+_{\mathbb{F}_q,D,G}(\mathcal{X}) \rtimes \mathrm{Aut}(\mathbb{F}_q)) \rtimes \mathbb{F}_q^*.$$

## 1.2 Maximal curves

In this section we present some important families of maximal curves, namely the Hermitian, Suzuki, Ree, GK, GGS, and GS curves. We refer to [39, 41, 42, 44, 115, 116] and [67, Chapt. 10] for surveys on maximal curves and their applications in Coding Theory.

We denote by $\mathbb{F}_q$ the finite field with $q$ element where $q$ is a power of a prime $p$, and by $\mathbb{K}$ the algebraic closure of $\mathbb{F}_q$. Also, $\mathrm{PG}(r,q)$ stands for the $r$-dimensional projective space $\mathrm{PG}(r, \mathbb{F}_q)$.

The most important result on the number of $\mathbb{F}_q$-rational points of a curve defined over a finite field is the Hasse-Weil bound.

**Hasse-Weil Bound.** *Let $\mathcal{X}$ be a non-singular curve of genus $g$ defined over $\mathbb{F}_q$. Then the number $\mathcal{X}(\mathbb{F}_q)$ of its $\mathbb{F}_q$-rational points satisfies*

$$||\mathcal{X}(\mathbb{F}_q)| - (q+1)| \leq 2g\sqrt{q}.$$

The Hasse-Weil bound is connected to the so-called zeta function of the curve $\mathcal{X}$. In particular, from the Hasse-Weil bound, the Riemann hypothesis for curves over finite fields is deduced; see [67, Chapt. 9.2].

**Definition 1.2.1.** *A non-singular curve $\mathcal{X}$ of genus $g$ defined over $\mathbb{F}_{q^2}$ is $\mathbb{F}_{q^2}$-*maximal *if it attains the Hasse-Weil upper bound, i.e.*

$$|\mathcal{X}(\mathbb{F}_{q^2})| = q^2 + 1 + 2gq.$$

A curve which is maximal over a certain finite field is also maximal over an infinite number of field extensions, as the following result shows.

**Proposition 1.2.2.** ([67, Eq. (10.1)]) *Let $\mathcal{X}$ be an $\mathbb{F}_{q^2}$-maximal curve and $n$ be a positive integer. If $n$ is odd, then $\mathcal{X}$ is $\mathbb{F}_{q^{2n}}$-maximal. If $n$ is even, then $\mathcal{X}$ is $\mathbb{F}_{q^{2n}}$-minimal (i.e. $|\mathcal{X}(\mathbb{F}_{q^{2n}})| = q^{2n} + 1 - 2gq^n$).*

The following results recall various algebraic and geometric characterizations of maximal curves.

**Theorem 1.2.3.** (see [67, Chapter 10]) *Let $\mathcal{X}$ an $\mathbb{F}_{q^2}$-rational curve of genus $g$. Then $\mathcal{X}$ is $\mathbb{F}_{q^2}$-maximal if and only if one of the following holds.*

- *The $L_{q^2}$-polynomial of $\mathcal{X}$ over $\mathbb{F}_{q^2}$ is equal to $L_{q^2}(t) = (t+q)^{2g}$.*
- *If $\tilde{\mathcal{X}} \subset \mathrm{PG}(r, \mathbb{K})$ is a non-singular model of $\mathcal{X}$ and $P_0$ is an $\mathbb{F}_{q^2}$-rational point of $\tilde{\mathcal{X}}$, then the divisors $qP + \Phi_{q^2}(P)$ and $(q+1)P_0$ are equivalent for any $P \in \tilde{\mathcal{X}}$, where $\Phi_{q^2}$ is the $\mathbb{F}_{q^2}$-Frobenius collineation of $\mathrm{PG}(r, \mathbb{K})$.*
- *$\mathcal{X}$ is $\mathbb{F}_{q^2}$-birationally equivalent to an irreducible curve $\bar{\mathcal{X}} \subset \mathrm{PG}(r, \mathbb{K})$ of degree $q+1$ lying on a non-degenerate Hermitian variety of $\mathrm{PG}(r, q^2)$.*

Starting from a maximal curve, other maximal curves can be obtained by the following result, commonly attributed to Serre.

**Theorem 1.2.4.** *(*[79, Prop. 6]) *Let $\mathcal{X}, \mathcal{Y}$ be two algebraic curves defined over $\mathbb{F}_{q^2}$ and suppose that there exists a non-constant rational map $\varphi : \mathcal{X} \to \mathcal{Y}$ defined over $\mathbb{F}_{q^2}$. If $\mathcal{X}$ is $\mathbb{F}_{q^2}$-maximal, then $\mathcal{Y}$ is also $\mathbb{F}_{q^2}$-maximal.*

*In particular, if $\mathcal{X}$ is $\mathbb{F}_{q^2}$-maximal and $G \leq \mathrm{Aut}(\mathcal{X})$ is $\mathbb{F}_{q^2}$-rational, then the quotient curve $\mathcal{X}/G$ is $\mathbb{F}_{q^2}$-maximal.*

The curves $\mathcal{X}$ that we present in Sections 1.2.1 and 1.2.2 are maximal over certain finite fields $\mathbb{F}_{q^2}$. When a singular model of $\mathcal{X}$ is provided, the $\mathbb{F}_{q^2}$-maximality is meant as the $\mathbb{F}_{q^2}$-maximality of a non-singular model of $\mathcal{X}$. Equivalently, the number of $\mathbb{F}_{q^2}$-rational places (rather than $\mathbb{F}_{q^2}$-rational points) attains the Hasse-Weil upper bound.

### 1.2.1 The Hermitian, Suzuki, and Ree curves

We introduce the Hermitian, Suzuki, and Ree curves. Altogether, they are known as *Deligne-Lusztig* curves and arise in algebraic geometry from the algebraic groups ${}^2A_2(q)$, ${}^2B_2(q)$, and ${}^2G_2(q)$, respectively. For an introduction, see [29].

The most important example of an $\mathbb{F}_{q^2}$-maximal curve is the Hermitian curve $\mathcal{H}_q$; see [67, Chapter 12.3] and the references therein for a detailed introduction and the proofs of the results of this section.

The curve $\mathcal{H}_q$ is defined as any $\mathbb{F}_{q^2}$-rational curve projectively equivalent to the plane curve with affine equation

$$X^{q+1} + Y^{q+1} + 1 = 0. \tag{1.3}$$

The model (1.3) is a so-called *Fermat* model of $\mathcal{H}_q$. This Fermat model is $\mathbb{F}_{q^2}$-isomorphic to the *Norm-Trace* model of $\mathcal{H}_q$, namely,

$$Y^{q+1} = X^q + X, \tag{1.4}$$

and $\mathbb{F}_{q^3}$-isomorphic to the *Singer* model of $\mathcal{H}_q$, namely,

$$X^qY + Y^q + X = 0. \tag{1.5}$$

Many of the $\mathbb{F}_{q^2}$-maximal curves known in the literature are constructed as $\mathbb{F}_{q^2}$-subcovers (often, Galois subcovers) of the Hermitian curve $\mathcal{H}_q$; see [28, 47, 49].

**Proposition 1.2.5.** ([101],[72],[67, Chapter 12.3]) *For the Hermitian curve the following properties hold:*

1. *$\mathcal{H}_q$ has genus $g(\mathcal{H}_q) = q(q-1)/2$, is non-singular and has $|\mathcal{H}_q(\mathbb{F}_{q^2})| = q^3+1$ $\mathbb{F}_{q^2}$-rational points.*

2. *If $\mathcal{X}$ is an $\mathbb{F}_{q^2}$-maximal curve, then $g(\mathcal{X}) \leq g(\mathcal{H}_q)$, and $g(\mathcal{X}) = g(\mathcal{H}_q)$ if and only if $\mathcal{X}$ is birationally equivalent to $\mathcal{H}_q$.*

3. *The full automorphism group* $\mathrm{Aut}(\mathcal{H}_q)$ *has order $(q^3+1)q^3$ and is defined over $\mathbb{F}_{q^2}$.*

4. $\mathrm{Aut}(\mathcal{H}_q)$ *acts* 2*-transitively on* $\mathcal{H}_q(\mathbb{F}_{q^2})$.

5. *A line of* $\mathrm{PG}(2,q^2)$ *has either* 1 *or* $q+1$ *common points with* $\mathcal{H}_q(\mathbb{F}_{q^2})$*, that is, it is either a* 1*-secant or a chord of* $\mathcal{H}_q(\mathbb{F}_{q^2})$.

6. *A unitary polarity* $\Pi$ *is associated with* $\mathcal{H}_q(\mathbb{F}_{q^2})$ *whose isotropic points are those of* $\mathcal{H}_q(\mathbb{F}_{q^2})$ *and isotropic lines are the* 1*-secants of* $\mathcal{H}_q(\mathbb{F}_{q^2})$*, that is, the tangents to* $\mathcal{H}_q$ *at the points of* $\mathcal{H}_q(\mathbb{F}_{q^2})$.

7. $\mathrm{Aut}(\mathcal{H}_q)$ *is isomorphic to the group* $\mathrm{PGU}(3,q) \leq \mathrm{PGL}(3,q^2)$ *of projectivities which commute with* $\Pi$*. The action of* $\mathrm{Aut}(\mathcal{H}_q)$ *on* $\mathcal{H}_q(\mathbb{F}_{q^2})$ *is equivalent to the action of* $\mathrm{PGU}(3,q)$ *in its natural* 2*-transitive permutation representation.*

The group $\mathrm{PGU}(3,q)$ contains a subgroup $\mathrm{PSU}(3,q)$ of index $\gcd(3,q+1)$, the *special* subgroup arising from elements of $\mathrm{PGL}(3,q^2)$ with determinant 1. We present the classification of maximal subgroups of $\mathrm{PSU}(3,q)$, going back to Mitchell [90] and Hartley [65].

**Theorem 1.2.6.** ([90, 65], see also [69],[67, Th. A.10]) *Let* $q = p^n$ *and* $d = \gcd(3,q+1)$*. Up to conjugacy, the following is a coomplete list of maximal subgroups of* $\mathrm{PSU}(3,q)$.

*(i) The stabilizer of an* $\mathbb{F}_{q^2}$*-rational point of* $\mathcal{H}_q$*, of order* $q^3(q^2-1)/d$.

*(ii) The stabilizer of an* $\mathbb{F}_{q^2}$*-rational point of* $\mathrm{PG}(2,q^2) \setminus \mathcal{H}_q$ *(equivalently the stabilizer of a chord of* $\mathcal{H}_q(\mathbb{F}_{q^2})$*), of order* $q(q-1)(q+1)^2/d$.

*(iii) The stabilizer of a self-polar triangle with respect to* $\Pi$*, of order* $6(q+1)^2/d$.

*(iv) The normalizer* $N$ *of a cyclic Singer subgroup* $S$*, of order* $|N| = 3(q^2-q+1)/d$*. The group* $N$ *preserves a triangle in* $\mathrm{PG}(2,q^6)\setminus\mathrm{PG}(2,q^2)$ *left invariant by the Frobenius collineation* $\Phi_{q^2} : (X,Y,T) \mapsto (X^{q^2}, Y^{q^2}, T^{q^2})$ *of* $\mathrm{PG}(2,\mathbb{K})$ *and fixed pointwise by* $S$.

Further, for $p > 2$:

*(v)* $\mathrm{PGL}(2,q)$ *preserving a conic.*

*(vi)* $\mathrm{PSU}(3,p^m)$ *with* $m \mid n$ *and* $n/m$ *odd.*

*(vii) Subgroups containing* $\mathrm{PSU}(3,p^m)$ *as a normal subgroup of index* 3*, when* $m \mid n$*,* $n/m$ *is odd, and* 3 *divides both* $n/m$ *and* $q+1$.

*(viii)* *The Hessian groups of order* $216$ *when* $9 \mid (q+1)$*, and of order* $72$ *and* $36$ *when* $3 \mid (q+1)$*.*

*(ix)* $\mathrm{PSL}(2,7)$ *when* $p=7$ *or* $-7$ *is not a square in* $\mathbb{F}_q$*.*

*(x)* *The alternating group* $A_6$ *on six letters, when either* $p=3$ *and* $n$ *is even, or* $5$ *is a square in* $\mathbb{F}_q$ *but* $\mathbb{F}_q$ *contains no cube root of unity.*

*(xi)* *The symmetric group* $S_6$ *on six letters, when* $p=5$ *and* $n$ *is odd.*

*(xii)* *The alternating group* $A_7$ *on seven letters, when* $p=5$ *and* $n$ *is odd.*

Further, for $p=2$:

*(xiii)* $\mathrm{PSU}(3,2^m)$ *with* $m \mid n$ *and* $n/m$ *an odd prime.*

*(xiv)* *Subgroups containing* $\mathrm{PSU}(3,2^m)$ *as a normal subgroup of index* $3$*, when* $n=3m$ *with* $m$ *odd.*

*(xv)* *A group of order* $36$ *when* $n=1$*.*

Case *(ii)* of Theorem 1.2.6 is related with the automorphism group of the projective line. Therefore, we present the classification of subgroups of $\mathrm{PGL}(2,q)$, which is due to Dickson [31].

**Theorem 1.2.7.** ([31, Chapter XII], see also [67, Th. A.8]) *Let* $q=p^n$*,* $d=\gcd(q-1,2)$*. Consider the group* $\mathrm{PGL}(2,q)$ *in its natural* $3$*-transitive action on a line* $\ell \subset \mathrm{PG}(2\mathbb{K})$*. The following is the complete list of subgroups of* $\mathrm{PGL}(2,q)$ *up to conjugacy:*

*(i)* *The cyclic group* $C_h$ *of order* $h$ *with* $h \mid (q \pm 1)$*. The group* $C_h$ *fixes two points* $P,Q \in \ell$ *and acts semiregularly on* $\ell \setminus \{P,Q\}$*. If* $h \mid (q-1)$*, then* $P,Q \in \mathrm{PG}(2,q)$*; if* $h \mid (q+1)$*, then* $P,Q \in \mathrm{PG}(2,q^2) \setminus \mathrm{PG}(2,q)$*.*

*(ii)* *The elementary abelian* $p$*-group* $E_{p^f}$ *of order* $p^f$ *with* $f \le k$*. The group* $E_{p^f}$ *fixes an* $\mathbb{F}_q$*-rational point* $P \in \ell$ *and acts semiregularly on* $\ell \setminus \{P\}$*.*

*(iii)* *The dihedral group* $D_h$ *of order* $2h$ *with* $h \mid (q \pm 1)$*, containing* $C_h$*.*

*(iv)* *The alternating group* $A_4$ *for* $p>2$*, or* $p=2$ *and* $k$ *even.*

*(v)* *The symmetric group* $S_4$ *for* $16 \mid (q^2-1)$*.*

*(vi)* *The alternating group* $A_5$ *for* $p=5$ *or* $5 \mid (q^2-1)$*.*

*(vii)* *The semidirect product* $E_{p^f} \rtimes C_h$ *with* $f \leq k$ *and* $h \mid (q-1)$*, of order* $p^f(h-1)$*, stabilizing the fixed point of* $E_{p^f}$*.*

*(viii)* $\mathrm{PSL}(2, p^f)$ *for* $f \mid k$*.*

*(ix)* $\mathrm{PGL}(2, p^f)$ *for* $f \mid k$*.*

Now we present a second class of Deligne-Lusztig curves, namely the Suzuki curves. For an exposition of results on the Suzuki curve and its quotients, we refer to [108, 109, 111, 112, 53] and [67, Chapter 12.2].

Let $s$ be a positive integer, $q_0 = 2^s$ and $q = 2q_0^2 = 2^{2s+1}$. The Suzuki curve $\mathcal{S}_q$ over $\mathbb{F}_q$ is defined by the affine equation

$$\mathcal{S}_q : \quad Y^q + Y = X^{q_0}(X^q + X). \tag{1.6}$$

**Proposition 1.2.8.** *For the Suzuki curve* $\mathcal{S}_q$ *the following properties hold:*

1. $\mathcal{S}_q$ *has genus* $g(\mathcal{S}_q) = q_0(q-1)$ *and is* $\mathbb{F}_{q^4}$*-maximal.*

2. $\mathcal{S}_q$ *has* $q^2 + 1$ $\mathbb{F}_q$*-rational points. The unique singular point of* $\mathcal{S}_q$ *is the point at infinity* $P_\infty$*. There is a unique place of* $\mathcal{S}_q$ *centered at* $P_\infty$*.*

3. *The full automorphism group* $S(q) := \mathrm{Aut}(\mathcal{S}_q)$ *has order* $(q^2+1)q^2(q-1)$ *and is defined over* $\mathbb{F}_q$*.*

4. $S(q)$ *has exactly* 2 *short orbits on* $\mathcal{S}_q$*. One is non-tame of size* $q^2+1$*, consisting of all* $\mathbb{F}_q$*-rational points. The other is tame of size* $q^2(q-1)(q+2q_0+1)$*, consisting of all* $\mathbb{F}_{q^4}$*-rational points which are not* $\mathbb{F}_q$*-rational.*

5. $S(q)$ *acts* 2*-transitively on* $\mathcal{S}_q(\mathbb{F}_q)$*.*

6. $S(q)$ *is isomorphic to the group* $Sz(q) \leq \mathrm{PGL}(4, q)$ *of projectivities preserving the Suzuki-Tits ovoid* $\mathcal{O}_S$ *in* $\mathrm{PG}(3, q)$*. The action of* $S(q)$ *on* $\mathcal{S}_q(\mathbb{F}_q)$ *is equivalent to the action of* $Sz(q)$ *on* $\mathcal{O}_S$ *in its natural* 2*-transitive permutation representation.*

7. $S(q)$ *is generated by the stabilizer*

$$S(q)_\infty = \{\psi_{a,b,c} : (x, y) \mapsto (ax + b, a^{q_0+1}y + b^{q_0}x + c) \mid a, b, c \in \mathbb{F}_q, a \neq 0\}$$

*of* $P_\infty$*, together with the involution* $\phi : (x, y) \mapsto (\alpha/\beta, y, \beta)$*, where* $\alpha := y^{2q_0} + x^{2q_0+1}$ *and* $\beta := xy^{2q_0} + \alpha^{2q_0}$*.*

The classification of maximal subgroups of $S(q)$ is known.

**Theorem 1.2.9.** (see [67, Th. A.12]) *Up to conjugacy, $S(q)$ has the following maximal subgroups:*

*(i) The stabilizer of an $\mathbb{F}_q$-rational point, of order $q^2(q-1)$.*

*(ii) The normalizer $N_+$ of a cyclic Singer subgroup $S_+$. The group $S_+$ has order $q+2q_0+1$ and fixes 4 $\mathbb{F}_{q^4}$-rational points of $\mathcal{S}_q$, the group $N_+$ has order $4(q+2q_0+1)$, and $N_+/S_+$ is a cyclic group permuting transitively the fixed points of $S_+$.*

*(iii) The normalizer $N_-$ of a cyclic Singer subgroup $S_-$. The group $S_-$ has order $q-2q_0+1$ and fixes 4 $\mathbb{F}_{q^4}$-rational points of $\mathcal{S}_q$, the group $N_-$ has order $4(q-2q_0+1)$, and $N_-/S_-$ is a cyclic group permuting transitively the fixed points of $S_-$.*

*(iv) The Suzuki subgroups $S(\tilde{q})$ where $q=\tilde{q}^m$ with $m$ prime.*

*Further, the subgroups listed below form a partition of $S(q)$:*

*(v) All subgroups of order $q^2$.*

*(vi) All cyclic subgroups of order $q-1$.*

*(vii) All cyclic Singer subgroups of order $q+2q_0+1$.*

*(viii) All cyclic Singer subgroups of order $q-2q_0+1$.*

Finally we present the third class of Deligne-Lusztig curves, namely the Ree curves. For an exposition of results on the Ree curve and its quotients, we refer to [112, 99, 35, 81, 18, 19] and [67, Chapter 12.4].

Let $s$ be a non-negative integer, $q_0=3^s$ and $q=3q_0^2=3^{2s+1}$. The Ree curve $\mathcal{R}_q$ over $\mathbb{F}_q$ is defined in $\mathrm{PG}(3,\mathbb{K})$ by the affine equations

$$\mathcal{R}_q: \quad Y^q-Y=X^{q_0}(X^q-X), \quad Z^q-Z=X^{2q_0}(X^q-X). \tag{1.7}$$

**Proposition 1.2.10.** *For the Ree curve $\mathcal{R}_q$ the following properties hold:*

1. *$\mathcal{R}_q$ has genus $g(\mathcal{R}_q)=\frac{3}{2}q_0(q-1)(q+q_0+1)$ and is $\mathbb{F}_{q^6}$-maximal.*
2. *$\mathcal{R}_q$ has $q^3+1$ $\mathbb{F}_q$-rational points. The unique singular point of $\mathcal{R}_q$ is the point at infinity $P_\infty$. There is a unique place of $\mathcal{R}_q$ centered at $P_\infty$.*

3. *The full automorphism group $R(q) := \mathrm{Aut}(\mathcal{R}_q)$ has order $(q^3+1)q^3(q-1)$ and is defined over $\mathbb{F}_q$.*

4. *$R(q)$ has exactly 2 short orbits on $\mathcal{R}_q$. One is non-tame of size $q^3+1$, consisting of all $\mathbb{F}_q$-rational points. The other is tame of size $q^2(q-1)(q+3q_0+1)$, consisting of all $\mathbb{F}_{q^6}$-rational points which are not $\mathbb{F}_q$-rational.*

5. *$R(q)$ acts 2-transitively on $\mathcal{S}_q(\mathbb{F}_q)$.*

6. *$R(q)$ is isomorphic to the group $Ree(q) \leq \mathrm{PGL}(7,q)$ of projectivities preserving the Ree-Tits ovoid $\mathcal{O}_R$ in $\mathrm{PG}(6,q)$. The action of $R(q)$ on $\mathcal{R}_q(\mathbb{F}_q)$ is equivalent to the action of $Ree(q)$ on $\mathcal{O}_R$ in its natural 2-transitive permutation representation.*

7. *$R(q)$ is generated by the stabilizer*

$$R(q)_\infty = \{\psi_{a,b,c,d} \mid a,b,c,d \in \mathbb{F}_q, a \neq 0\},$$

$$\psi_{a,b,c,d} : (x,y,z) \mapsto (ax+b, a^{q_0+1}y+ab^{q_0}x+c, a^{2q_0+1}z-a^{q_0+1}b^{q_0}y+ab^{2q_0}x+d),$$

*of $P_\infty$, together with the involution $\phi : (x,y,z) \mapsto (w_6/w_8, w_{10}/w_8, w^9/w_8)$, for certain polynomial functions $w_i \in \mathbb{F}_3[x,y,z]$.*

The classification of maximal subgroups of $R(q)$ is known.

**Theorem 1.2.11.** (see [67, Th. A.14]) *Up to conjugacy, $R(q)$ has the following maximal subgroups:*

*(i) The stabilizer of an $\mathbb{F}_q$-rational point, of order $q^3(q-1)$.*

*(ii) The centralizer of an involution $\iota \in R(q)$, isomorphic to $\iota \times \mathrm{PSL}(2,q)$, of order $q(q^2-1)$.*

*(iii) The normalizer $N_+$ of a cyclic Singer subgroup $S_+$. The group $S_+$ has order $q+3q_0+1$ and fixes 6 $\mathbb{F}_{q^6}$-rational points of $\mathcal{R}_q$, the group $N_+$ has order $6(q+3q_0+1)$, and $N_+/S_+$ is a cyclic group permuting transitively the fixed points of $S_+$.*

*(iv) The normalizer $N_-$ of a cyclic Singer subgroup $S_-$. The group $S_-$ has order $q-3q_0+1$ and fixes 6 $\mathbb{F}_{q^6}$-rational points of $\mathcal{R}_q$, the group $N_-$ has order $6(q-3q_0+1)$, and $N_-/S_-$ is a cyclic group permuting transitively the fixed points of $S_-$.*

(v) *A subgroup of order* $6(q+1)$*, which normalizes a cyclic subgroup of order* $q+1$.

(vi) *The Ree subgroups* $R(\tilde{q})$ *where* $q=\tilde{q}^m$ *with* $m$ *prime.*

### 1.2.2 The GK, GGS, and GS curves

In this section we present three classes of maximal curves recently constructed. The first curve is the so-called GK curve, named after Giulietti and Korchmáros who constructed it in [50], which we refer to for an exposition of the results below. The GK curve was the first $\mathbb{F}_{q^2}$-maximal curve shown not to be covered by the Hermitian curve $\mathcal{H}_q$. This result motivated a new interest towards maximal curves, subcover (or Galois subcovers) of the Hermitian curve, and subcovers of other maximal curves. Examples of subcovers of the GK curve can be found in [38, 110].

Let $n$ be a power of a prime $p$, and $q=n^3$. The GK curve $\mathcal{GK}_n$ is defined in $\mathrm{PG}(3,\mathbb{K})$ by the affine equations

$$\mathcal{GK}_n : \begin{cases} Z^{n^2-n+1} = Y\frac{X^{n^2}-X}{X^n+X} \\ Y^{n+1} = X^n+X \end{cases}. \tag{1.8}$$

By direct checking, equivalent equations for $\mathcal{GK}_n$ are

$$Z^{n^2-n+1}=Y^{n^2}-Y, \quad Y^{n+1}=X^n+X.$$

Note that $\mathcal{GK}_n$ has a unique infinite point $P_\infty$.

**Proposition 1.2.12.** ([50]) *For the GK curve* $\mathcal{GK}_n$ *the following properties hold:*

1. $\mathcal{GK}_n$ *is non-singular.*

2. $\mathcal{GK}_n$ *has genus* $g(\mathcal{GK}_n)=\frac{(n^3+1)(n^2-2)}{2}+1$ *and has* $|\mathcal{GK}_n(\mathbb{F}_{n^6})|=n^8-n^6+n^5+1$ $\mathbb{F}_{n^6}$*-rational points. Hence,* $GK_n$ *is* $\mathbb{F}_{n^6}$*-maximal.*

3. *For* $n>2$*,* $\mathcal{GK}_n$ *is not covered by the Hermitian curve* $\mathcal{H}_{n^3}$.

4. *The full automorphism group* $\mathrm{Aut}(\mathcal{GK}_n)$ *has order* $n^3(n^3+1)(n^2-1)(n^2-n+1)$ *and is defined over* $\mathbb{F}_{n^6}$.

5. $\mathrm{Aut}(\mathcal{GK}_n)$ *has exactly* 2 *short orbits on* $\mathcal{GK}_n$*. One is non-tame of size* $n^3+1$*, consists of all* $\mathbb{F}_{n^2}$*-rational points of* $\mathcal{GK}_n$*, and is given by the intersection of* $\mathcal{GK}_n$ *with the plane* $Z=0$*. The other is tame of size* $n^3(n^3+1)(n^2-1)$*, consisting of all* $\mathbb{F}_{n^6}$*-rational points of* $\mathcal{GK}_n$ *which are not* $\mathbb{F}_{n^2}$*-rational.*

6. *$\mathrm{Aut}(\mathcal{GK}_n)$ has a normal subgroup of index $d = \gcd(3, n+1)$ isomorphic to $\mathrm{SU}(3,n) \times C_{(n^2-n+1)/d}$, where $\mathrm{SU}(3,n)$ is the special unitary group which preserves $\mathcal{GK}_n(\mathbb{F}_{n^2})$ and $C_{(n^2-n+1)/d}$ is cyclic of order $(n^2-n+1)/d$. The subgroup isomorphic to $\mathrm{SU}(3,n)$ is normal in $\mathrm{Aut}(\mathcal{GK}_n)$.*

7. *The stabilizer $\mathrm{Aut}(\mathcal{GK}_n)_{P_\infty}$ of $P_\infty$ has order $n^3(n^2-1)(n^2-n+1)$ and constains a subgroup $(Q_{n^3} \rtimes H_{q^2-1}) \times C_{(n^2-n+1)/d}$, where $Q_{n^3}$ is a Sylow $p$-subgroup of $\mathrm{Aut}(\mathcal{GK}_n)$ and $H_{n^2-1}$ is cyclic of order $n^2-1$.*

8. *The action of $\mathrm{SU}(3,n)$ on $\mathcal{GK}_n(\mathbb{F}_{n^2})$ is equivalent to the action of $\mathrm{PGU}(3,n)$ in its natural 2-transitive permutation representation. The group $\mathrm{SU}(3,n)$ is normal in $\mathrm{Aut}(\mathcal{GK}_n)$, and $\mathrm{Aut}(\mathcal{GK}_n)/\mathrm{SU}(3,n)$ acts trivially on $\mathcal{GK}_n(\mathbb{F}_{n^2})$.*

9. *The principal divisors of the coordinate functions $x, y, z$ are*

   - $(x) = (n^3+1)P_{(0,0,0)} - (n^3+1)P_\infty$,
   - $(y) = (n^2-n+1)\left(\sum_{a:a^n+a=0} P_{(a,0,0)}\right) - (n^3-n^2+n)P_\infty$,
   - $(z) = \left(\sum_{a,b\in\mathbb{F}_{n^2}:a^n+a=b^{n+1}} P_{(a,b,0)}\right) - n^3 P_\infty$,

   *where $P_{(a,b,c)}$ is the place centered at the affine point $(a,b,c) \in \mathcal{GK}_n$.*

The GK curve was generalized to a broader class of maximal curves $\mathcal{GGS}_{n,m}$ by Garcia, Güneri, and Stichtenoth in [43], where the authors show the $\mathbb{F}_{n^{2m}}$-maximality of $\mathcal{GGS}_{n,m}$. The automorphism group of $\mathcal{GGS}_{n,m}$ was determined in [60] and [61], and the quotient curves of $\mathcal{GGS}_{n,m}$ are investigated in [3]. In [34] it was shown that $\mathcal{GGS}_{n,m}$ is not Galois covered by $\mathcal{H}_{n^m}$ whenever $n \geq 3$.

Let $n$ be a power of a prime $p$ and $m \geq 5$ be an odd integer. The GGS curve $\mathcal{GGS}_{n,m}$ is defined in $\mathrm{PG}(3,\mathbb{K})$ be the affine equations

$$\mathcal{GGS}_{n,m} : \begin{cases} Z^{\frac{n^m+1}{n+1}} = Y^{n^2} - Y \\ Y^{n+1} = X^n + X \end{cases} .$$

Note that $\mathcal{GGS}_{n,m}$ coincides with $\mathcal{GK}_n$ when $m = 3$.

**Proposition 1.2.13.** *For the GGS curve $\mathcal{GGS}_{n,m}$ the following properties hold:*

1. *$\mathcal{GGS}_{n,m}$ has a unique point at infinity $P_\infty$, which is $\mathbb{F}_{n^{2m}}$-rational and is the center of a unique place of $\mathcal{GGS}_{n,m}$.*

2. *$\mathcal{GGS}_{n,m}$ has genus $g(\mathcal{GGS}_{n,m}) = (n-1)(n^{m+1}+n^m-n^2)/2$ and has $n^{2m+2} - n^{m+3} + n^{m+2} + 1$ $\mathbb{F}_{n^{2m}}$-rational places. Therefore, $\mathcal{GGS}_{n,m}$ is $\mathbb{F}_{n^{2m}}$-maximal.*

3. *For $n \geq 3$, $\mathcal{GGS}_{n,m}$ is not Galois covered by the Hermitian curve $\mathcal{H}_{n^m}$.*

4. *The full automorphism group* $\mathrm{Aut}(\mathcal{GGS}_{n,m})$ *has order* $n^3(n-1)(n^m+1)$ *and is defined over* $\mathbb{F}_{n^{2m}}$*.*

5. $\mathrm{Aut}(\mathcal{GGS}_{n,m})$ *fixes* $P_\infty$*, and* $P_\infty$ *is the unique fixed place of* $\mathrm{Aut}(\mathcal{GGS}_{n,m})$*.*

6. *If $n$ is a power of $2$, then the number of $\mathbb{F}_{n^{2m}}$-rational places of $\mathcal{GGS}_{n,m}$ is a multiple of $3$.*

Finally we introduce the Garcia-Stichtenoth curves. Garcia and Stichtenoth constructed in [45] the following curve in characteristic 3:

$$\mathcal{GS}_3: \quad Y^7 = X^9 - X.$$

The authors proved that $\mathcal{GS}_3$ is not Galois covered by the Hermitian curve $\mathcal{H}_{27}$; this was the first example of maximal curve shown not to be Galois covered by the Hermitian curve. This curve was generalized in [1] to the curve

$$Y^{\frac{n^m+1}{n+1}} = X^{n^2} - X, \tag{1.9}$$

which was shown to be maximal over $\mathbb{F}_{n^{2m}}$; this also follows from the $\mathbb{F}_{n^{2m}}$-maximality of the GGS curve $\mathcal{GGS}_{n,m}$, since the curve (1.9) is $\mathbb{F}_{n^{2m}}$-covered by $\mathcal{GGS}_{n,m}$.

We restrict to the case $m = 3$, and consider the Garcia-Stichtenoth curve

$$\mathcal{GS}_n: \quad Y^{n^2-n+1} = X^{n^2} - X.$$

Note that $\mathcal{GS}_n$ is an $\mathbb{F}_{n^6}$-subcover of the GK curve $\mathcal{GK}_n$, and hence $\mathcal{GS}_n$ is $\mathbb{F}_{n^6}$-maximal.

**Proposition 1.2.14.** (see [67, Chapter 12.1]) *For the GS curve $\mathcal{GS}_n$ the following properties hold:*

1. *$\mathcal{GS}_n$ has genus $(n^2-n)(n^2-1)/2$ and has $n^7-n^5+n^4+1$ $\mathbb{F}_{n^6}$-rational places; hence, $\mathcal{GS}_n$ is $\mathbb{F}_{n^6}$-maximal.*

2. *$\mathcal{GS}_n$ has a unique singular point, namely the point at infinity $P_\infty$. There is a unique place of $\mathcal{GS}_n$ centered at $P_\infty$.*

3. *$P_\infty$ is the unique fixed point of* $\mathrm{Aut}(\mathcal{GS}_n)$*.*

4. *$\mathcal{GS}_2$ is Galois covered by the Hermitian curve $\mathcal{H}_8$.*

5. *$\mathcal{GS}_3$ is not Galois covered by the Hermitian curve $\mathcal{H}_{27}$.*

# Chapter 2

# Results on maximal curves

## 2.1 Maximal curves from subcovers of the GK curve

In this section we construct and investigate families of Galois subcovers of the GK curve $\mathcal{GK}_n$. In particular, we compute explicit equations and the genera for a number of Galois subcovers of $\mathcal{GK}_n$. Also, we provide new examples of $\mathbb{F}_{n^6}$-maximal curve that are not covered, or Galois covered, by the Hermitian curve $\mathcal{H}_{n^3}$. In several cases, such curves give new values in the spectrum of genera of $\mathbb{F}_{n^6}$-maximal curves. The results obtained in this section are the object of [56].

Throughout this section, $n$ is a power of a prime $p$, $q = n^3$, and $\mathbb{K}$ is the algebraic closure of $\mathbb{F}_p$.

### 2.1.1 A new model of the GK curve

Let $\mathcal{GK}_n$ be given by the equations (1.8). Let $\rho \in \mathbb{F}_{n^2}$ with $\rho+\rho^n = 1$. Consider the $\mathbb{F}_{n^2}$-projectivity $\varphi$ associated to the matrix $A$, where

$$A = \begin{pmatrix} 1 & 0 & 0 & 1-\rho \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & -\rho \end{pmatrix}.$$

Then $\mathcal{X} := \varphi(\mathcal{GK}_n)$ has equations

$$\mathcal{X} : \begin{cases} Z^{n^2-n+1} = Y\frac{X^{n^2}-X}{X^{n+1}-1} \\ Y^{n+1} = X^{n+1}-1 \end{cases} .$$

We will consider subgroups of the following tame $\mathbb{F}_{q^2}$-automorphism group $G$ of $\mathcal{X}$ of size $(n+1)^2(n^2-n+1)$:

$$G = \left\{ g_{a,b,\lambda} : (X,Y,Z,T) \mapsto (aX, bY, \lambda Z, T) \mid a^{n+1} = b^{n+1} = 1, \lambda^{n^2-n+1} = ab \right\}. \tag{2.1}$$

By conjugation, an $\mathbb{F}_{q^2}$-automorphism group $G^A = A^{-1}GA$ of $\mathcal{X}$ is obtained:

$$G^A = \left\{ g^A_{a,b,\lambda} \mid a^{n+1} = b^{n+1} = 1, \lambda^{n^2-n+1} = ab \right\}, \quad \text{where}$$

$$g^A_{a,b,\lambda} = \begin{pmatrix} a\rho + \rho^n & 0 & 0 & a\rho - a\rho^2 - \rho^{n+1} \\ 0 & b & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ a-1 & 0 & 0 & a - a\rho + \rho \end{pmatrix}.$$

According to the notation of [38], we compute the projection $\bar{G^A}$ of $G^A$ over $\mathrm{PGU}(3,n)$ and the intersection $G^A_\Lambda$ of $G^A$ with

$$\Lambda = \left\{ \alpha_\lambda : (X,Y,Z,T) \mapsto (X, Y, \lambda Z, T) \mid \lambda^{n^2-n+1} = 1 \right\} : \tag{2.2}$$

$$G^A_\Lambda = \Lambda, \quad \bar{G^A} = \left\{ \bar{g}_{a,b} \mid a^{n+1} = b^{n+1} = 1 \right\}, \quad \text{where}$$

$$\bar{g}_{a,b} = \begin{pmatrix} a\rho + \rho^n & 0 & a\rho - a\rho^2 - \rho^{n+1} \\ 0 & b & 0 \\ a-1 & 0 & a - a\rho + \rho \end{pmatrix}.$$

Note that $\bar{G^A} = \overline{A^{-1}GA} = \bar{A}^{-1}\bar{G}\bar{A}$, where $\bar{A}$ (resp. $\bar{G}$) is obtained by deleting the third row and column in $A$ (resp. in the matrices of $G$). Let $\pi$ be the plane $Z=0$. Then $\mathrm{Aut}(\mathcal{X})$ has a non-tame short orbit

$$\mathcal{O} := \mathcal{X}(\mathbb{F}_{n^2}) = \mathcal{X} \cap \pi,$$

which is the image under $\varphi$ of the non-tame short orbit of $\mathrm{Aut}(\mathcal{GK}_n)$ described in Proposition 1.2.12. Hence, $\bar{G^A}$ acts naturally on $\bar{\mathcal{O}} = \mathcal{H}_n(\mathbb{F}_{n^2})$, where the Hermitian curve $\mathcal{H}_q$ has the Fermat equation $Y^{n+1} = X^{n+1} - 1$.

### 2.1.2 A family of Galois subcovers of $\mathcal{X}$

In this section we find out equations and genera for a family of curves covered by the curve $\mathcal{X}$, depending on three parameters.

Let $d_1, d_2, d_3$ be divisors of $n+1$, and consider the $\mathbb{F}_p$-rational morphism

$$u = x^{\frac{n+1}{d_1}}, \; v = y^{\frac{n+1}{d_2}}, \; w = z^{\frac{n+1}{d_3}}$$

over the function field $\mathbb{K}(x,y,z)$ of $\mathcal{X}$. Then for the subfield $\mathbb{K}(u,v,w)$ we have the relations

$$w^{d_3(n^2-n+1)} = u^{d_1}(u^{d_1}-1)\left(\frac{u^{d_1(n-1)}-1}{u^{d_1}-1}\right)^{n+1}, \qquad v^{d_2}=u^{d_1}-1. \tag{2.3}$$

Let $G \le \mathrm{Aut}(\mathcal{X})$ as in (2.1) and $L \le G$ be the following subgroup of $G$:

$$L = \left\{(X,Y,Z,T)\mapsto(\lambda^3 b^n X, bY, \lambda Z, T) \mid b^{n+1}=\lambda^{n+1}=1\right\}.$$

Clearly, $L$ has order $(n+1)^2$, and the fixed field $Fix(L)$ contains $x^{n+1}$, $y^{n+1}$, and $z^{n+1}$. Actually, $Fix(L)$ coincides with $\mathbb{K}(x^{n+1},y^{n+1},z^{n+1})$, since $\mathbb{K}(x^{n+1},y^{n+1},z^{n+1})$ coincides with $\mathbb{K}(x^{n+1},z^{n+1})$ and the degree of the extension $\mathbb{K}(x,y,z)|\mathbb{K}(x^{n+1},z^{n+1})$ is at most $(n+1)^2$. Then $Fix(L)\subseteq\mathbb{K}(u,v,w)$ and we consider the double extension of function fields

$$Fix(L)\subseteq\mathbb{K}(u,v,w)\subseteq\mathbb{K}(x,y,z).$$

Since $\mathbb{K}(x,y,z)|Fix(L)$ is a Galois extension, $\mathbb{K}(x,y,z)|\mathbb{K}(u,v,w)$ is Galois as well, that is, $\mathbb{K}(u,v,w)$ is the function field of the quotient curve of $\mathcal{X}$ over some automorphism subgroup $H\le L$.

In order to provide irreducible equations for $\mathcal{X}/H$, consider the rational function $\alpha\in\mathbb{K}(u,v)$ defined as

$$\alpha = u^{d_1}(u^{d_1}-1)\left(\frac{u^{d_1(n-1)}-1}{u^{d_1}-1}\right)^{n+1}.$$

By direct computation the principal divisor of $\alpha$ in $\mathbb{K}(u,v)$ is obtained:

$$\begin{array}{rl} div(\alpha)= & d_1\sum_{i=1}^{d_2}Q_{0,i}+d_2\sum_{i=1}^{d_1}Q_{\alpha_i} \\ & +(n+1)\sum_{i=1}^{d_1(n-2)}\sum_{j=1}^{d_2}Q_{\beta_i,j}-\frac{d_1d_2n(n-1)}{(d_2,2d_1)}\sum_{i=1}^{(d_2,2d_1)}Q_{\infty,i} \end{array}, \tag{2.4}$$

where $Q_{0,i}$ lies over the zero $P_0$ of $u$, $Q_{\alpha_i}$ lies over the zero $P_{\alpha_i}$ of $u^{d_1}-1$, $Q_{\beta_i,j}$ lies over the zero $P_{\beta_i}$ of $(u^{d_1(n-1)}-1)/(u^{d_1}-1)$, and $Q_{\infty,i}$ lies over the pole $P_\infty$ of $u$. Let

$$D=\gcd\left(d_1,d_2,n+1,\frac{d_1d_2n(n-1)}{(d_2,2d_1)}\right),$$

$$M=\gcd\left(D,d_3(n^2-n+1)\right)=\gcd\left(d_1,d_2,d_3(n^2-n+1)\right).$$

If $M=1$, then $\mathbb{K}(u,v,w)|\mathbb{K}(u,v)$ is a Kummer extension of degree $d_3(n^2-n+1)$ from equations (2.3), and the quotient curve has irreducible equations

$$\mathcal{X}/H:\left\{\begin{array}{l} W^{d_3(n^2-n+1)}=U^{d_1}V^{d_2}\left(\frac{U^{d_1(n-1)}-1}{U^{d_1}-1}\right)^{n+1} \\ V^{d_2}=U^{d_1}-1 \end{array}\right..$$

More generally, for $M \geq 1$, both sides of the firs equation in (2.3) are a power of $M$, and we can factor the equation to obtain an irreducible curve

$$\mathcal{X}/H : \begin{cases} w^{\frac{d_3}{M}(n^2-n+1)} = u^{\frac{d_1}{M}} v^{\frac{d_2}{M}} \left(\frac{u^{d_1(n-1)}-1}{u^{d_1}-1}\right)^{\frac{n+1}{M}} \\ v^{d_2} = u^{d_1} - 1 \end{cases} . \tag{2.5}$$

**Remark 2.1.1.** *We compute the order of the group $H$, that is, the degree of the extension $[\mathbb{K}(x,y,z) : \mathbb{K}(u,v,w)]$. By the Fundamental Equality after Definition* 1.1.15*, the zero divisor of $x$ in $\mathbb{K}(x,y,z)$ has degree $[\mathbb{K}(x,y,z) : \mathbb{K}(x)] = n^3+1$, and*

$$[\mathbb{K}(x,y,z) : \mathbb{K}(u)] = \deg(x^{\frac{n+1}{d_1}})_0 = \frac{(n+1)^2(n^2-n+1)}{d_1}, \quad [\mathbb{K}(u,v) : \mathbb{K}(u)] = d_2.$$

*Hence,*

$$[\mathbb{K}(x,y,z) : \mathbb{K}(u,v)] = \frac{(n+1)^2(n^2-n+1)}{d_1, d_2}, \; [\mathbb{K}(u,v,w) : \mathbb{K}(u,v)] = \frac{d_3(n^2-n+1)}{M}.$$

*Therefore*

$$|H| = [\mathbb{K}(x,y,z) : \mathbb{K}(u,v,w)] = \frac{M(n+1)^2}{d_1 d_2 d_3}.$$

The general equations (2.5) of $\mathcal{X}/H$ have been obtained by working on $d_1$, $d_2$, $d_3(n^2-n+1)/M$. If we start from $d_1/M, d_2, d_3$, or from $d_1, d_2/M, d_3$, then we get irreducible equations for other quotient curves, respectively:

$$\begin{cases} W^{d_3(n^2-n+1)} = U^{\frac{d_1}{M}} \left(U^{\frac{d_1}{M}(n-1)} - 1\right) \left(\frac{U^{\frac{d_1}{M}(n-1)}-1}{U^{\frac{d_1}{M}}-1}\right)^n \\ V^{d_2} = U^{\frac{d_1}{M}} - 1 \end{cases} ,$$

$$\begin{cases} W^{d_3(n^2-n+1)} = U^{d_1} \left(U^{d_1(n-1)} - 1\right) \left(\frac{U^{d_1(n-1)}-1}{U^{d_1}-1}\right)^n \\ V^{\frac{d_2}{M}} = U^{d_1} - 1 \end{cases} .$$

Over the function fields of these curves we can also consider the morphism

$$(u : v : w^{\frac{n^2-n+1}{e}} : 1),$$

for any divisor $e$ of $n^2-n+1$. Then, for $s = w^{\frac{n^2-n+1}{e}}$, $\mathbb{K}(u,v,s)$ is the function field of new subcovers of $\mathcal{X}$. The degree $[\mathbb{K}(x,y,z) : \mathbb{K}(u,v,s)]$ of these coverings is easily computed arguing as in Remark 2.1.1. To sum up, the following result is obtained.

**Theorem 2.1.2.** *Let $d_1$, $d_2$, and $d_3$ be divisors of $n+1$, $e$ be a divisor of $n^2-n+1$, and $M = \gcd(d_1, d_2, d_3(n^2-n+1))$. The following equations define $\mathbb{F}_{n^6}$-maximal curves which are Galois subcovers of $\mathcal{X}$:*

$$\mathcal{C}_1 : \begin{cases} S^{\frac{d_3}{M}e} = U^{\frac{d_1}{M}} V^{\frac{d_2}{M}} \left(\frac{U^{d_1(n-1)}-1}{U^{d_1}-1}\right)^{\frac{n+1}{M}} \\ V^{d_2} = U^{d_1} - 1 \end{cases}, \tag{2.6}$$

$$\mathcal{C}_2 : \begin{cases} S^{d_3 e} = U^{\frac{d_1}{M}} \left(U^{\frac{d_1}{M}(n-1)} - 1\right) \left(\frac{U^{\frac{d_1}{M}(n-1)}-1}{U^{\frac{d_1}{M}}-1}\right)^{n} \\ V^{d_2} = U^{\frac{d_1}{M}} - 1 \end{cases}, \tag{2.7}$$

$$\mathcal{C}_3 : \begin{cases} S^{d_3 e} = U^{d_1} \left(U^{d_1(n-1)} - 1\right) \left(\frac{U^{d_1(n-1)}-1}{U^{d_1}-1}\right)^{n} \\ V^{\frac{d_2}{M}} = U^{d_1} - 1 \end{cases}. \tag{2.8}$$

*The degree of the covering is $\frac{(n^2-n+1)M(n+1)^2}{ed_1d_2d_3}$ for $\mathcal{C}_1$ and $\mathcal{C}_3$, and $\frac{(n^2-n+1)(n+1)^2}{ed_1d_2d_3}$ for $\mathcal{C}_2$.*

Note that, when $\frac{(n^2-n+1)M(n+1)^2}{ed_1d_2d_3} = 1$ or $\frac{(n^2-n+1)(n+1)^2}{ed_1d_2d_3} = 1$, Theorem 2.1.2 provides models for the GK curve; in some cases they are plane models.

Now we compute the genera of the curves described in Theorem 2.1.2 for $e = n^2-n+1$, i.e. for $s = w$. This is done via Kummer theory.

**Theorem 2.1.3.** *Let $e = n^2-n+1$. Then the genera of the curves $\mathcal{C}_1$, $\mathcal{C}_2$, and $\mathcal{C}_3$ described in Theorem 2.1.2 are the following:*

$$\begin{aligned} g(\mathcal{C}_1) = \;& 1 + \tfrac{1}{2}\Big[d_1 d_2 \tfrac{d_3(n^2-n+1)}{M}(n-1) - d_2(\tfrac{d_1}{M}, \tfrac{d_3(n^2-n+1)}{M}) \\ & -d_1(\tfrac{d_2}{M}, \tfrac{d_3(n^2-n+1)}{M}) + -d_1d_2(n-2)(\tfrac{d_3(n^2-n+1)}{M}, \tfrac{n+1}{M}) \\ & - \Big((d_1,d_2)\tfrac{d_3(n^2-n+1)}{M}, \tfrac{2d_1d_2}{M}\Big)\Big] \end{aligned} \tag{2.9}$$

*and, for $i = 2, 3$,*

$$g(\mathcal{C}_i) = 1 + \frac{1}{2}\left[hkr(n-1) - k(h,r) - h(k,r) - hk(n-2)(r, n+1) - ((h,k)r, 2hk)\right], \tag{2.10}$$

*where*

$$r = d_3(n^2-n+1), \quad h = \begin{cases} d_1/M & \text{for } \mathcal{C}_2 \\ d_1 & \text{for } \mathcal{C}_3 \end{cases}, \quad k = \begin{cases} d_2 & \text{for } \mathcal{C}_2 \\ d_2/M & \text{for } \mathcal{C}_3 \end{cases}.$$

*Proof.* We start with $\mathcal{C}_1$, and use the notation of (2.4) for

$$\alpha = u^{\frac{d_1}{M}} v^{\frac{d_2}{M}} \left(\frac{u^{d_1(n-1)}-1}{u^{d_1}-1}\right)^{\frac{n+1}{M}} \in \mathbb{K}(u,v).$$

Since $\mathbb{K}(u,v)|\mathbb{K}(u)$ is a Kummer extension of degree $d_2$, we have

$$e(Q_{\alpha_i}|P_{\alpha_i}) = d_2, e(Q_{0,i}|P_0) = 1, e(Q_{\beta_i,j}|P_{\beta_i}) = 1, e(Q_{\infty,i}|P_\infty) = \frac{d_2}{\gcd(d_1,d_2)},$$

and $\mathbb{K}(u,v)$ has genus

$$g(\mathbb{K}(u,v)) = 1 + \frac{1}{2}(d_1d_2 - d_1 - d_2 - \gcd(d_1,d_2)).$$

Let $\bar{P}_0$ be the zero and $\bar{P}_\infty$ the pole of $v$ in $\mathbb{K}(v)$. Then the places lying over $\bar{P}_0$ in $\mathbb{K}(u,v)|\mathbb{K}(v)$ are $Q_{\alpha_1},\dots,Q_{\alpha_{d_1}}$, with ramification index 1. The places over $\bar{P}_\infty$ are $Q_{\infty,1},\dots,Q_{\infty,(d_1,d_2)}$, with ramification index $d_1/\gcd(d_1,d_2)$.

In the Kummer extension $\mathbb{K}(u,v,s)|\mathbb{K}(u,v)$ of degree $\frac{d_3}{M}(n^2-n+1)$,

$$v_{Q_{\alpha_i}}(\alpha) = e(Q_{\alpha_i}|P_{\alpha_i}) \cdot v_{P_{\alpha_i}}\left(u^{\frac{d_1}{M}}\left(\frac{u^{d_1(n-1)}-1}{u^{d_1}-1}\right)^{\frac{n+1}{M}}\right) + e(Q_{\alpha_i}|\bar{P}_0)\cdot v_{\bar{P}_0}\left(v^{\frac{d_2}{M}}\right) = \frac{d_2}{M},$$

and hence

$$e(R_{\alpha_i,j}|Q_{\alpha_i}) = \frac{\frac{d_3}{M}(n^2-n+1)}{\gcd\left(\frac{d_3}{M}(n^2-n+1), \frac{d_2}{M}\right)},$$

where $R_{\alpha_i,j}$ is a place of $\mathbb{K}(u,v,s)$ lying over $Q_{\alpha_i}$. The theory of Kummer extensions also gives the ramification indices

$$\frac{\frac{d_3}{M}(n^2-n+1)}{\gcd\left(\frac{d_3}{M}(n^2-n+1), v_Q(\alpha)\right)}$$

of the places of $\mathbb{K}(u,v,s)$ lying over $Q$, for all places $Q$ of $\mathbb{K}(u,v)$. Then the different divisor of $\mathbb{K}(u,v,s)|\mathbb{K}(u,v)$ has degree $\Delta$ equal to

$$\Delta = d_1\left(m - \left(m, \frac{d_2}{M}\right)\right) + d_2\left(m - \left(m, \frac{d_1}{M}\right)\right) +$$

$$+d_1(n-2)d_2\left(m - \left(m, \frac{n+1}{M}\right)\right) + (d_1,d_2)\left(m - \left(m, \frac{d_1d_2(n^2-n)}{M(d_1,d_2)}\right)\right) =$$

$$= d_1\left(m - \left(m, \frac{d_2}{M}\right)\right) + d_2\left(m - \left(m, \frac{d_1}{M}\right)\right) +$$

$$+d_1(n-2)d_2\left(m-\left(m,\frac{n+1}{M}\right)\right)+(d_1,d_2)\left(m-\left(m,\frac{2d_1d_2}{M(d_1,d_2)}\right)\right),$$

where $m=d_3(n^2-n+1)/M$. Finally, the Riemann-Hurwitz formula applied to the Galois extension $\mathbb{K}(u,v,s)|\mathbb{K}(u,v)$ provides the genus of $\mathcal{C}_1$.

The curves $\mathcal{C}_2$ and $\mathcal{C}_3$ are both defined by equations of the form

$$\mathcal{C}_i:\begin{cases} S^r=U^a\left(U^{a(n-1)}-1\right)\left(\frac{U^{a(n-1)}-1}{U^a-1}\right)^n \\ V^b=U^a-1\end{cases}.$$

The genus of $\mathbb{K}(u,v)$ is obtained as above:

$$g(\mathbb{K}(u,v))=1+\frac{1}{2}(ab-a-b-\gcd(a,b)).$$

Similar computations yield the degree $\Delta$ of the different divisor of the Kummer extension $\mathbb{K}(u,v,s)|\mathbb{K}(u,v)$:

$$\Delta=a\left(r-\gcd(r,b)\right)+b\left(r-\gcd(r,a)\right)+$$
$$+a(n-2)b\left(r-\gcd(r,n+1)\right)+\gcd(a,b)\left(r-\gcd\left(r,\frac{2ab}{\gcd(a,b)}\right)\right),$$

and the Riemann-Hurwitz formula applied to $\mathbb{K}(u,v,s)|\mathbb{K}(u,v)$ provides the genus of $\mathcal{C}_i$, for $i=2,3$. □

**Remark 2.1.4.** *The previous results provide new equations of $\mathbb{F}_{q^2}$-maximal curves for many genera. Consider for instance the case $n=5$. Then Theorem* 2.1.2 *provides new equations for the following genera:*

$$37,74,109,121,148,220,242,361,442,484,724,1450,$$
$$160,233,469,478,496,737,1477,1486.$$

*Up to our knowledge, the integers in the second row are new values in the spectrum of genera of $\mathbb{F}_{5^6}$-maximal curves.*

### 2.1.3 The Galois groups of some Galois extensions

In this section we assume that

$$\gcd\left(d_1,d_2,d_3(n^2-n+1)\right)=1.$$

In some cases we are able to give an explicit description of the automorphism groups $H$ of order $\frac{(n+1)^2}{d_1d_2d_3}$ such that $Fix(H)=\mathbb{K}(u,v,w)$.

We also provide an alternative computation of the genus of $\mathcal{X}/H$, by means of the Riemann-Hurwitz genus formula and [38, Prop. 3.2]. We use [38, Prop. 3.2] in a slightly different form: in the original paper [38], the authors consider a model $\tilde{\mathcal{X}}$ of the GK curve lying on the cone $\tilde{\mathcal{K}}$ over the Hermitian curve with equation $Y^n + Y = X^{n+1}$. It is not difficult to see that the same computations hold for the curve $\mathcal{X}$.

This relies on the fact that $\tilde{\mathcal{X}}$ and $\mathcal{X}$ are projectively equivalent, with a projectivity defined over $\mathbb{F}_{n^6}$ which maps the Hermitian cone $\tilde{\mathcal{K}}$ to the Hermitian cone over $Y^n + Y = X^{n+1}$.

**Proposition 2.1.5.** [38, Prop. 3.2] *Let $L$ be a tame subgroup of $\mathrm{Aut}(\mathcal{X})$, $\bar{L}$ the projection of $L$ to $\mathrm{PGU}(3,n)$ and $L_\Lambda = L \cap \Lambda$, where $\Lambda$ is defined in equation (2.2). Assume that no non-trivial element in $\bar{L}$ fixes a point in $\mathcal{H}_n \setminus \mathcal{H}_n(\mathbb{F}_{n^6})$, where $\mathcal{H}_n$ is the Hermitian curve $Y^{n+1} = X^{n+1} - 1$. Then:*

$$g_L = g_{\bar{L}} + \frac{(n^3+1)(n^2 - |L_\Lambda| - 1) - |L_\Lambda|(n^2 - n - 2)}{2|L|},$$

*where $g_L$ is the genus of the quotient curve $\mathcal{H}_n/\bar{L}$.*

**Case 2.1.6.** *Suppose that $d_1$ divides $3d_3$ and $\gcd(d_1, d_2) = 1$. Then $\mathbb{K}(u,v,w)$ is the function field of the quotient curve of $\mathcal{X}$ with respect to the group*

$$H = \left\{ (X,Y,Z,T) \mapsto (\lambda^3 b^n X, bY, \lambda Z, T) \mid b^{\frac{n+1}{d_1 d_2}} = \lambda^{\frac{n+1}{d_3}} = 1 \right\}.$$

*In fact, by Remark 2.1.1, the size $(n+1)^2/(d_1 d_2 d_3)$ of $H$ coincides with the degree $[\mathbb{K}(x,y,z) : \mathbb{K}(u,v,w)]$. Also, $u$, $v$, and $w$ are all fixed by $H$ since*

$$\lambda^{(n+1)/d_3} = 1, \qquad b^{(n+1)/d_2} = (b^{(n+1)/d_2 d_1})^{d_1} = 1,$$

*and*

$$(\lambda^3 b^n)^{(n+1)/d_1} = (\lambda^{(n+1)/d_3})^{3d_3/d_1} b^{-((n+1)/d_1)} = (b^{-((n+1)/d_1 d_2)})^{d_2} = 1.$$

*The projection $\bar{H}$ of $H$ on $\mathrm{PGU}(3,n)$ is*

$$\bar{H} = \left\{ [\lambda^3 b^n, b, 1] \mid b^{\frac{n+1}{d_2 d_1}} = \lambda^{\frac{n+1}{d_3}} = 1 \right\} \quad \text{with} \quad |\bar{H}| = \frac{(n+1)^2}{d_1 d_2 d_3 \gcd\left(3, \frac{n+1}{d_3}\right)},$$

*where $[\lambda^3 b^n, b, 1]$ denotes the automorphism $(X,Y,T) \mapsto (\lambda^3 b^n X, bY, T)$. No non-trivial element in $\bar{H}$ fixes a point in $\mathcal{H}_n \setminus \mathcal{H}_n(\mathbb{F}_{n^6})$, and*

$$H_\Lambda = \left\{ [1,1,\lambda,1] \mid \lambda^{n^2-n+1} = \lambda^{\frac{n+1}{d_3}} = 1 \right\}$$

*has size* $\gcd\left(\frac{n+1}{d_3}, 3\right)$. *Then by Proposition* 2.1.5 *the genus of* $\mathcal{X}/H$ *is*

$$g_H = g_{\bar{H}} + \frac{d_1d_2d_3[(n^3+1)(n^2-\gcd(3,\frac{n+1}{d_3})-1)-\gcd(3,\frac{n+1}{d_3})(n^2-n-2)]}{2(n+1)^2},$$

*where* $g_{\bar{H}}$ *is the genus of* $\mathcal{H}_n/\bar{H}$. *The only points of* $\mathcal{H}_n$ *that can be fixed by a non-trivial element in* $\bar{H}$ *are the fundamental points. It is easily seen that*

*(i)* $[\lambda^3 b^n, b, 1]$ *fixes* $P_i = (0, \alpha_i, 1)$, $i = 1, \ldots, n+1$, *if and only if* $b = 1$;

*(ii)* $[\lambda^3 b^n, b, 1]$ *fixes* $Q_j = (\beta_j, 0, 1)$, $j = 1, \ldots, n+1$, *if and only if* $\lambda^3 = b$;

*(iii)* $[\lambda^3 b^n, b, 1]$ *fixes* $R_k = (\beta_k, 1, 0)$, $k = 1, \ldots, n+1$, *if and only if* $\lambda^3 = b^2$.

*Let* $\bar{H}_P$ *denote the stabilizer of* $P$ *in* $\bar{H}$. *We distinguish two cases.*

*(**A**)* 3 *does not divide* $(n+1)/d_3$. *Then* $\lambda \mapsto \lambda^3$ *is an automorphism of the multiplicative group of the* $((n+1)/d_3)$*-th roots of unity.*

*(i) We have* $\bar{H}_{P_i} = \left\{[\lambda^3, 1, 1] \mid \lambda^{\frac{n+1}{d_3}} = 1\right\}$, *and hence* $|\bar{H}_{P_i}| = \frac{n+1}{d_3}$.

*(ii) We have*

$$\bar{H}_{Q_j} = \left\{[1, b, 1] \mid b^{\frac{n+1}{d_2d_1}} = 1, b = \lambda^3 \textit{ for some } \lambda \textit{ with } \lambda^{\frac{n+1}{d_3}} = 1\right\},$$

*hence*

$$|\bar{H}_{Q_j}| = \gcd\left(\frac{n+1}{d_3}, \frac{n+1}{d_1d_2}\right).$$

*(iii) We distinguish two subcases.*

- $\frac{n+1}{d_1d_2}$ *is even. Then*

$$\bar{H}_{R_k} = \left\{[b, b, 1] \mid (b^2)^{\frac{n+1}{d_3}} = 1, (b^2)^{\frac{n+1}{2d_1d_2}} = 1\right\} \quad \textit{and} \quad b \neq -b,$$

*hence*

$$|\bar{H}_{R_k}| = 2\gcd\left(\frac{n+1}{d_3}, \frac{n+1}{2d_1d_2}\right) = \gcd\left(\frac{2(n+1)}{d_3}, \frac{n+1}{d_1d_2}\right).$$

- $\frac{n+1}{d_1d_2}$ *is odd. Then* $b \mapsto b^2$ *is an automorphism of the multiplicative group of the* $((n+1)/d_1d_2)$*-th roots of unity, and*

$$\bar{H}_{R_k} = \left\{[b, b, 1] \mid \lambda^{\frac{n+1}{d_3}} = b^{\frac{n+1}{d_1d_2}} = 1, \lambda^3 = b^2\right\};$$

*hence,*

$$|\bar{H}_{R_k}| = \gcd\left(\frac{n+1}{d_3}, \frac{n+1}{d_1d_2}\right) = \gcd\left(\frac{2(n+1)}{d_3}, \frac{n+1}{d_1d_2}\right).$$

*Therefore, if* $3 \nmid (n+1)/d_3$ *then the Hurwitz formula applied to the covering* $\mathcal{H} \to \mathcal{H}/\bar{H}$ *provides the genus of* $\mathcal{H}/\bar{H}$*:*

$$\begin{aligned} g_{\bar{H}} = \;& 1 + \frac{1}{2\frac{(n+1)^2}{d_1d_2d_3}}\Big[n^2 - n - 2 - (n+1) \\ & \Big(\tfrac{n+1}{d_3} + \gcd(\tfrac{n+1}{d_1d_2}, \tfrac{n+1}{d_3}) + \gcd(\tfrac{n+1}{d_1d_2}, \tfrac{2(n+1)}{d_3}) - 3\Big)\Big], \end{aligned}$$

*that is,*

$$g_{\bar{H}} = 1 + \frac{d_1d_2d_3}{2(n+1)}\Big[n - 2 - \frac{n+1}{d_3} - \Big(\frac{n+1}{d_1d_2}, \frac{n+1}{d_3}\Big) - \Big(\frac{n+1}{d_1d_2}, \frac{2(n+1)}{d_3}\Big) + 3\Big],$$

*hence*

$$\begin{aligned} g_H = 1 + \frac{d_1d_2d_3}{2(n+1)}\left(n + 1 - \frac{n+1}{d_3} - \Big(\frac{n+1}{d_1d_2}, \frac{n+1}{d_3}\Big) - \Big(\frac{n+1}{d_1d_2}, \frac{2(n+1)}{d_3}\Big)\right) + \\ + \frac{d_1d_2d_3\left(n^3 - 2n^2 + n\right)}{2}. \end{aligned} \tag{2.11}$$

(**B**) $3$ *divides* $(n+1)/d_3$*. Let* $\lambda' = \lambda^3$*, then*

$$\bar{H} = \left\{[\lambda' b^n, b, 1] \mid (\lambda')^{\frac{n+1}{3d_3}} = b^{\frac{n+1}{d_1d_2}} = 1\right\}.$$

*The same arguments yield*

$$\begin{aligned} g_H = 1 + \frac{3d_1d_2d_3}{2(n+1)}\left(n + 1 - \frac{n+1}{3d_3} - \Big(\frac{n+1}{d_1d_2}, \frac{n+1}{3d_3}\Big) - \Big(\frac{n+1}{d_1d_2}, \frac{2(n+1)}{3d_3}\Big)\right) + \\ + \frac{d_1d_2d_3\left(n^3 - 2n^2 - n + 2\right)}{2}. \end{aligned}$$

**Case 2.1.7.** *Suppose that* $d_1$ *divides* $d_2$*, and* $(d_1, d_3(n^2 - n + 1)) = 1$*. Then* $\mathbb{K}(u, v, w)$ *is the function field quotient curve of* $\mathcal{X}$ *with respect to the group*

$$H = \left\{(X, Y, Z, T) \mapsto (\lambda^3 b^n X, bY, \lambda Z, T) \mid b^{\frac{n+1}{d_2}} = \lambda^{\frac{n+1}{d_1d_3}} = 1\right\}.$$

*This follows from*

$$\lambda^{(n+1)/d_3} = (\lambda^{(n+1)/d_1d_3})^{d_1} = 1, \qquad b^{(n+1)/d_2} = 1,$$

*and*

$$(\lambda^3 b^n)^{(n+1)/d_1} = (\lambda^{\frac{n+1}{d_1d_3}})^{3d_3} b^{-((n+1)/d_1)} = (b^{-((n+1)/d_2)})^{d_2/d_1} = 1.$$

*Similar computations provide the genus of* $\mathcal{X}/H$*:*

$$\begin{aligned} g_H = 1 + \frac{d_1d_2d_3m}{2(n+1)}\left(n + 1 - \frac{n+1}{d_1d_3m} - \Big(\frac{n+1}{d_2}, \frac{n+1}{d_1d_3m}\Big) - \Big(\frac{n+1}{d_2}, \frac{2(n+1)}{d_1d_3m}\Big)\right) + \\ + \frac{d_1d_2d_3\left[n^3 - 2n^2 + (2-m)n + m - 1\right]}{2}, \end{aligned}$$

*where* $m = \gcd(3, (n+1)/(d_1d_3))$*.*

### 2.1.4 Another family of Galois subcovers of $\mathcal{X}$

In this section we consider another subgroup of the group $G$ given in (2.1). Let $c \mid (n+1)$, $d \mid (n^2-n+1)$, and consider the following automorphism group $K$ of $\mathcal{X}$ of size $(n^3+1)/(cd)$:

$$K = \left\{ (X,Y,Z,T) \mapsto (b^{-1}X, bY, \lambda Z, T) \mid b^{\frac{n+1}{c}} = 1, \lambda^{\frac{n^2-n+1}{d}} = 1 \right\}.$$

By applying the $\mathbb{F}_p$-rational morphism

$$u = x^{\frac{n+1}{c}}, \quad v = xy, \quad w = z^{\frac{n^2-n+1}{d}}$$

over the function field $\mathbb{K}(x,y,z)$ of $\mathcal{X}$, we have the following relations:

$$w^d = v\left(1 + u^c + u^{2c} + \ldots + u^{(n-2)c}\right), \quad v^{n+1} = u^{2c} - u^c. \tag{2.12}$$

In the double field extension $\mathbb{K}(u,v,w) \subseteq Fix(K) \subseteq \mathbb{K}(x,y,z)$ we have

$$[\mathbb{K}(x,y,z) : \mathbb{K}(u,v,w)] \leq \frac{n^3+1}{cd} = [\mathbb{K}(x,y,z) : Fix(K)],$$

which implies $Fix(K) = \mathbb{K}(u,v,w)$.

The equations (2.12) are irreducible. To show this, let $P = (0,a)$ be an affine point of the Hermitian curve $\mathcal{H}_n : Y^{n+1} = X^{n+1} - 1$, and let $\bar{P}$ be a place of the curve $\mathcal{W} : V^{n+1} = U^{2c} - U^c$ centered at the image $\varphi(P)$ of $P$ under the $\mathbb{F}_p$-rational map

$$\varphi : \mathcal{H}_n \to \mathcal{W}, \quad \varphi(X,Y,T) = (X^{\frac{n+1}{c}}, XY, T).$$

The rational function $\beta := xy(1 + x^{n+1} + x^{2(n+1)} \ldots + x^{(n-2)(n+1)}) \in \mathbb{K}(x,y)$ has valuation $v_P(\beta) = 1$ at $P$, hence the pull-back $\alpha = v(1 + u^c + \ldots + u^{(n-2)c}) \in \mathbb{K}(u,v)$ of $\beta$ has valuation $v_{\bar{P}}(\alpha) = 1$ at $\bar{P}$, since $v_P(\beta) = e(P|\bar{P}) \cdot v_{\bar{P}}(\alpha)$. Hence the equations (2.12) are irreducible, i.e. the quotient curve $\mathcal{X}/K$ has irreducible equations:

$$\mathcal{X}/K : \left\{ \begin{array}{l} W^d = V\left(1 + U^c + U^{2c} + \ldots + U^{(n-2)c}\right) \\ V^{n+1} = U^{2c} - U^c \end{array} \right. . \tag{2.13}$$

From the Hurwitz formula applied to the tame covering $\mathcal{X} \to \mathcal{X}/K$, we compute the genus of $\mathcal{X}/K$:

$$g(\mathcal{X}/K) = \frac{c}{2}\left[(d-1)n^2 + n - d - \gcd\left(2, \frac{n+1}{c}\right)\right] + 1. \tag{2.14}$$

### 2.1.5 New examples of maximal curves not (Galois) covered by the Hermitian curve

Let a curve $\mathcal{Y}$ be a subcover of the Hermitian curve $\mathcal{H}_q$ by an $\mathbb{F}_{q^2}$-rational map

$$\varphi : \mathcal{H} \to \mathcal{Y}.$$

Then for the degree $\deg(\varphi)$ of the covering we have the following bounds:

$$\frac{\mathcal{H}(\mathbb{F}_{q^2})}{\mathcal{Y}(\mathbb{F}_{q^2})} \leq \deg(\varphi) \leq \frac{2g(\mathcal{H})-2}{2g(\mathcal{Y})-2}.$$

In particular, the lower bound $L_{\mathcal{H},\mathcal{Y}} = \mathcal{H}(\mathbb{F}_{q^2})/\mathcal{Y}(\mathbb{F}_{q^2})$ and the upper bound $U_{\mathcal{H},\mathcal{Y}} = (2g(\mathcal{H})-2)/(2g(\mathcal{Y})-2)$ satisfy $\lceil L_{\mathcal{H},\mathcal{Y}} \rceil \leq \lfloor U_{\mathcal{H},\mathcal{Y}} \rfloor$.

Therefore, a curve $\mathcal{Y}$ having $\lceil L_{\mathcal{H},\mathcal{Y}} \rceil > \lfloor U_{\mathcal{H},\mathcal{Y}} \rfloor$ cannot be a subcover of the Hermitian curve. By applying this argument to the curves given in Theorems 2.1.2 and 2.1.3, we get many new examples of curves which are not covered by the Hermitian curve.

To exemplify this, we list in Table 2.1 below some genera of curves not covered by the Hermitian curve. We remark that for such curves we have both the genus and explicit equations.

**Remark 2.1.8.** *Let $\mathcal{Y}$ be an $\mathbb{F}_{q^2}$-maximal curve of genus $g$ which is $\mathbb{F}_{q^2}$-covered by the Hermitian curve $\mathcal{H}_q$. If $g > f(q)$, where*

$$f(q) = \frac{\sqrt{q^5+2q^4+q^3+q^2+2q+1}-q^2-1}{2q},$$

*then the degree $d$ of the covering $\mathcal{H}_q \to \mathcal{Y}$ is uniquely determined by*

$$L_{\mathcal{H},\mathcal{Y}} \leq d \leq U_{\mathcal{H},\mathcal{Y}}.$$

*Proof.* By direct computation, $g > f(q)$ is equivalent to $U_{\mathcal{H},\mathcal{Y}} - L_{\mathcal{H},\mathcal{Y}} < 1$, which implies $\lceil L_{\mathcal{H},\mathcal{Y}} \rceil = \lfloor U_{\mathcal{H},\mathcal{Y}} \rfloor$. □

**Theorem 2.1.9.** *Let $n \geq 7$ be a power of a prime $p$ and $k \mid (n+1)$ with $k < \sqrt{n+1}+1$. Define $d_1 = (n+1)/k$, $d_2 = 1$, and $d_3 = n+1$. Then the curve $\mathcal{C}_1$ in Theorem 2.1.2 is not Galois covered by the Hermitian curve $\mathcal{H}_{n^3}$.*

Table 2.1: New maximal curves not covered by the Hermitian curve

| $g$ | $n$ | $(d_1, d_2, d_3)$ | Reference |
|---|---|---|---|
| 233416 | 17 | (1,18,6), (2,9,6), (2,18,3), (2,18,6), (3,18,6), (6,9,6), (6,18,3), (6,18,6), (9,2,6), (9,6,6), (9,18,2), (9,18,6), (18,1,6), (18,2,3), (18,2,6), (18,3,6), (18,6,3), (18,6,6), (18,9,2), (18,9,6) | Th. 2.1.3 (2.9),(2.10) |
| 233398 | 17 | (9,18,2) | Th. 2.1.3 (2.10) |
| 1064701 | 23 | (1,24,8), (8,3,8), (24,8,1), (24,1,8), (2,24,8), (3,8,8), (3,24,8), (4,24,8), (6,8,8), (6,24,8), (8,3,8), (8,6,8), (8,12,8), (8,24,1), (8,24,2) | Th. 2.1.3 (2.9),(2.10) |
| 1064689 | 23 | (2,24,8), (4,24,8), (6,8,8), (6,24,8), (8,6,8), (8,12,8) | Th. 2.1.3 (2.10) |
| 3206257 | 23 | (2,24,24), (4,24,24), (6,24,24), (8,6,24), (8,12,24) | Th. 2.1.3 (2.10) |
| 3402406 | 29 | (30,10,1), (10,30,1), (10,15,2), (30,2,5), (10,6,5), (10,3,10) | Th. 2.1.3 (2.9) |
| 5570731 | 32 | (33,11,1), (11,33,1), (11,3,11) | Th. 2.1.3 (2.9) |

*Proof.* Let $\mathcal{H}_{n^3}$ be given in the Norm-Trace form (1.4) and let $P_\infty$ be the point at infinity of $\mathcal{H}_{n^3}$. Suppose that $\mathcal{C}_1$ is Galois covered by $\mathcal{H}_{n^3}$, so that $\mathcal{C}_1 \cong \mathcal{H}_{n^3}/N$ for some subgroup $N$ of $\mathrm{PGU}(3, n^3)$.

The genus of $\mathcal{C}_1$ can be computed from (2.11), whence $L_{\mathcal{H}_{n^3},\mathcal{C}_1} > kn - 1$ if and only if

$$n^8 - k(k-2)n^7 - 2n^6 + n^5 - (k-1)[2k+1-(k,2)]n^4 + [2k-1-(k,2)]n^3 - k^2n + 2k > 0,$$

while $U_{\mathcal{H}_{n^3},\mathcal{C}_1} < kn + 1$ if and only if

$$n^5 - 2kn^4 + 2(k-1)n^3 - [k(k,2) - k - 1]n^2 - [(k,2)(k+1) + k - 1]n + 2k - (k,2) - 1 > 0.$$

For $n \geq 7$, both conditions are implied by the hypothesis $k < \sqrt{n+1} + 1$. Then $|N| = kn$.

Let $S$ be a Sylow $p$-subgroup of $N$. The group $S$ fixes an $\mathbb{F}_{n^6}$-rational point $P \in \mathcal{H}_{n^3}$ by [67, Lemma 11.129]. Since all Sylow $p$-subgroups are conjugate, we assume that $S$ fixes $P_\infty$. Moreover, the action of $S$ on $\mathcal{H}(\mathbb{F}_{n^6})\setminus\{P_\infty\}$ is semiregular, i.e. each element of $S$ has no fixed point but $P_\infty$. Hence the orbit $\mathcal{O}$ of $P_\infty$ under $N$ satisfies $|\mathcal{O}| \equiv 1 \pmod{n}$.

Suppose $P_\infty$ is not fixed by $N$, then $|\mathcal{O}| \geq n+1$. Hence, by the orbit-stabilizer theorem, $n$ divides the size of the stabilizer $N_Q$ of $Q$ in $N$, for all $Q \in \mathcal{O}$. Then a Sylow $p$-subgroup $M_Q$ of $N_Q$ has size $n$. Since $S$ is semiregular on $\mathcal{H}_{n^3} \setminus \{P_\infty\}$, $M_Q$ and $M_R$ have trivial intersection for $Q \neq R$ in $\mathcal{O}$. Therefore $N$ has at least $1 + (n+1)(n-1) = n^2$ elements, thus $k \geq n$, a contradiction.

Therefore the whole $N$ fixes $P_\infty$. If $k = 1$, then $\mathcal{C}_1$ is isomorphic to the GK curve $\mathcal{X}$ and the thesis holds. Otherwise, the genus of $\mathcal{H}/N$ can be computed by [47, Th. 4.4]:

$$g(\mathcal{H}/N) = \frac{n^3 - p^w}{2kn}\left(n^3 - (k-1)p^v\right) = \frac{p^{5u} - p^{3u-v} - (k-1)p^{3u-w} + k - 1}{2k},$$

where $n = p^u$ and $v, w$ are non-negative integers satisfying $u = v + w$.

On the other side, the genus of $\mathcal{C}_1$ as computed in (2.11) is

$$g(\mathcal{C}_1) = \frac{n^5 - 2n^3 + n^2 + 2k - 1 - h}{2k}, \quad \text{where} \quad h = \begin{cases} n+2 & \text{if } k \text{ is even} \\ 1 & \text{if } k \text{ is odd} \end{cases}.$$

Hence the equality $g(\mathcal{H}/N) = g(\mathcal{C}_1)$ reads

$$k = \frac{2p^{3u} + p^{3u-w} - p^{3u-v} - p^{2u} + h}{p^{3u-w} + 1}.$$

We have the following possibilities for $v$ and $w$: either $v = 0$ and $w = u$, or $v \leq u/2$ and $w \geq u/2$, or $v > u/2$ and $w < u/2$. By considering separately each case, it is shown after some computation that

$$\left(p^{3u-w}+1\right) \nmid \left(2p^{3u}+p^{3u-w}-p^{3u-v}-p^{2u}+h\right),$$

which is impossible since $k$ is integer. □

**Theorem 2.1.10.** *Let $n > 3$ be a power of a prime $p$, $k$ a divisor of $n+1$ such that $3 \nmid (n+1)/k$ and $k < \sqrt{n+1}+1$; if $3 \mid (n+1)$, assume also $n \geq 23$. Define $d_1 = (n+1)/k$, $d_2 = n+1$, and $d_3 = 1$. Then the curve $\mathcal{C}_1$ in Theorem* 2.1.2 *is not Galois covered by the Hermitian curve $\mathcal{H}_{n^3}$.*

*Proof.* The genus of the curve $\mathcal{C}_1$ can be computed as in Case 2.1.7. Separating the cases $3 \mid (n+1)$ and $3 \nmid (n+1)$ and arguing as in the proof of Theorem 2.1.9, it is proved that a putative Galois covering has degree $kn$.

Suppose that such a covering exists and $\mathcal{C}_1 \cong \mathcal{H}/N$ with $N \leq \mathrm{PGU}(3,n^3)$. The same argument used in the proof of Theorem 2.1.9 allows to apply [47, Th. 4.4] and yields the following expression for $k$:

$$k = \frac{(1+\gcd(3,k))\,p^{3u}+p^{3u-w}-p^{3u-v}-p^{2u}-\gcd(3,k)p^{u}}{p^{3u-w}-p^{u}-2}, \tag{2.15}$$

where $n = p^u$ and $v, w$ are non-negative integers satisfying $u = v + w$. A case-analysis now shows that the fraction in (2.15) cannot be integer. □

**Theorem 2.1.11.** *Let $n$ be a power of a prime $p$, $\gamma$ a divisor of $n+1$, $\delta$ a divisor of $n^2-n+1$, $c = (n+1)/\gamma$, and $d = (n^2-n+1)/\delta$. Suppose that one of the following holds:*

- *$n = 5$, $\gamma = 2$, and $\delta = 1$;*
- *$n \geq 7$, $\gamma \leq 2$, and $\delta \leq (\sqrt{2\gamma n+1}-1)/2$;*
- *$n \geq 7$, $\gamma > 2$, and $\gamma\delta(\gamma\delta-\delta-1) < n$.*

*Then the curve $\mathcal{X}/K$ with equations* (2.13) *is not Galois covered by the Hermitian curve $\mathcal{H}_{n^3}$.*

*Proof.* By arguing as in the proof of Theorem 2.1.9, it is proved that a putative Galois covering has degree $\gamma\delta n$. Suppose that such a covering exists and $\mathcal{X}/K \cong$

$\mathcal{H}/N$ with $N \leq \mathrm{PGU}(3, n^3)$. The same argument used in the proof of Theorem 2.1.9 allows to apply [47, Th. 4.4] and yields the following identity:

$$\delta \left[p^{3u} - \gamma p^{3u-w} + (\gcd(2,\gamma) - 1)\, p^u - \gamma + \gcd(2,\gamma)\right] = -p^{3u} + p^{3u-v} - p^{3u-w} + p^{2u}, \tag{2.16}$$

where $n = p^u$ and $v, w$ are non-negative integers with $u = v + w$. By a case-analysis, it can be shown that (2.16) contradicts the hypothesis on the integers $\gamma$ and $\delta$. □

## 2.2 Maximal curves that are not quotients of the Hermitian curve

In this section we prove the following result

**Theorem 2.2.1.** *For any odd number $m \geq 5$, the GGS curve $\mathcal{GGS}_{2,m}$ is not Galois covered by the Hermitian curve $\mathcal{H}_{2^m}$.*

Together with a result by Duursma and Mak [34, Theorem 1.1], this shows that the GGS curve $\mathcal{GGS}_{n,m}$ is not Galois covered by $\mathcal{H}_{n^m}$ for any prime power $n$ and any odd $m \geq 5$.

We also prove an analogous result for the GS curve.

**Theorem 2.2.2.** *For any prime power $q > 3$, the GS curve $\mathcal{GS}_q$ is not Galois covered by the Hermitian curve $\mathcal{H}_{q^3}$.*

By Proposition 1.2.14, this shows that $\mathcal{GS}_n$ is not Galois covered by $\mathcal{H}_{n^3}$ for any prime power $n \geq 3$, while $\mathcal{GS}_2$ is Galois covered by $\mathcal{H}_8$.

In this section, we exploit the properties of the automorphism group $\mathrm{PGU}(3, q)$ of the Hermitian curve $\mathcal{H}_q$. Essentialy, we study the putative subgroups $G \leq \mathrm{PGU}(3, q)$ realizing the isomorphism between the GGS curve (or the GS curve) and the quotient curve $\mathcal{H}_q/G$, and prove that the automorphism groups of the two curves cannot be equivalent.

The results obtained in this section are the object of [54].

### 2.2.1 $\mathcal{GGS}_{2,m}$ is not Galois covered by $\mathcal{H}_{2^m}$, for any $m \geq 5$

Through Section 2.2.1, $m \geq 5$ is an odd integer and $q = 2^m$. We rely on a result by Duursma and Mak [34, Theorem 1.2].

**Lemma 2.2.3.** *Let $m \geq 5$ be odd. If $\mathcal{GGS}_{2,m} \cong \mathcal{H}_{2^m}/G$ for some $G \leq \mathrm{Aut}(\mathcal{H}_{2^m})$, then $G$ has order $(2^m+1)/3$ and acts semiregularly on $\mathcal{H}_{2^m}$.*

*Proof.* The order of $G$ is equal to the degree of the covering $\varphi : \mathcal{H}_{2^m} \to \mathcal{GGS}_{2,m}$. Hence, by [34, Theorem 1.2], $G$ has order $(2^m+1)/3$. Also, by [34, Theorem 1.2], $\varphi$ is unramified. Since $\mathcal{H}_{2^m}$ is non-singular, this means that there are exactly $|G|$ points of $\mathcal{H}_{2^m}$ lying over each point of $\mathcal{H}_{2^m}/G$, that is, every orbit of $G$ is long. □

By Lemma 2.2.3 only subgroups $G \leq \mathrm{Aut}(\mathcal{H}_q)$ of order $(q+1)/3$ acting semiregularly on $\mathcal{H}_q$ need to be considered. We will also use the fact that $\mathrm{Aut}(\mathcal{GGS}_{2.m})$ has a unique fixed place $P_\infty \in \mathcal{GGS}_{2.m}$, see Proposition 1.2.13.

**Proposition 2.2.4.** *Let $G \leq \mathrm{Aut}(\mathcal{H}_q)$. If there exists $\bar{G} \leq \mathrm{Aut}(\mathcal{H}_q)$ such that $G$ is a proper normal subgroup of $\bar{G}$ and $\bar{G}$ acts semiregularly on $\mathcal{H}_q$, then $\mathcal{GGS}_{2,m} \not\cong \mathcal{H}_q/G$.*

*Proof.* The claim follows from Proposition 1.2.13 *5.*, taking into account that $\bar{G}/G \leq \mathrm{Aut}(\mathcal{H}_q/G)$ acts semiregularly on $\mathcal{H}_q/G$. □

The following well-known result about finite groups will be used (see [85, Ex. 16 Page 232]).

**Lemma 2.2.5.** *Let $H$ be a finite group and $K$ a subgroup of $H$ such that the index $[H : K]$ is the smallest prime number dividing the order of $H$. Then $K$ is normal in $H$.*

**Proposition 2.2.6.** *Let $G \leq \mathrm{PSU}(3,q)$. If a maximal subgroup of $\mathrm{PSU}(3,q)$ containing $G$ is of type $(ii)$ in Theorem 1.2.6, then $\mathcal{GGS}_{2,m} \not\cong \mathcal{H}_q/G$.*

*Proof.* Let $\ell$ be the $(q+1)$-secant to $\mathcal{H}_q$ stabilized by $G$; we show that $G$ is isomorphic to a cyclic subgroup of $\mathrm{PSL}(2,q^2)$. We can assume that $\ell$ is the line at infinity $T=0$; in fact, the group $\mathrm{PGU}(3,q)$ is transitive on the points of $\mathrm{PG}(2,q^2) \setminus \mathcal{H}_q$, and hence also on the $(q+1)$-secant lines. The action of an element $g \in G$ on $\ell$ is given by $(X,Y,0) \mapsto A_g \cdot (X,Y,0)$, where the matrix $A_g = (a_{ij})_{i=1,2,3}^{j=1,2,3}$ satisfies $a_{31}=a_{32}=0$; we set $a_{33}=1$. By direct computation, the map

$$\varphi : G \to \mathrm{PGL}(2,q^2), \qquad \varphi(g) : \begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} X \\ Y \end{pmatrix},$$

is a well-defined group homomorphism. Moreover, $\varphi$ is injective, since no non-trivial element of $G$ can fix the points of $\mathcal{H}_q \cap \ell$, by the semiregularity of $G$. Hence

$G$ is isomorphic to a subgroup of $\mathrm{PGL}(2,q^2)$. Since $|G|$ is odd, Theorem 1.2.7 implies that $G$ is cyclic.

Let $g \in G$ be an element of prime order $d > 3$; such a $d$ exists, since it is easy to check that $2^m + 1$ is a power of 3 only when $m = 1$ or $m = 3$. If we denote by $d^h$ the highest power of $d$ dividing $(q+1)/3$, then $d^{2h}$ is the highest power of $d$ dividing

$$|\mathrm{PGU}(3,q)| = q^3(q^3+1)(q^2-1) = q^3(q+1)^2(q-1)(q^2-q+1).$$

Let $\mathcal{H}_q$ be given in the Fermat form (1.3); then

$$D = \Big\{(X:Y:T) \mapsto (\lambda X : \mu Y : T) \mid \lambda^{d^h} = \mu^{d^h} = 1\Big\}$$

is a Sylow $d$-subgroup of $\mathrm{PGU}(3,q)$. By Sylow theorems we can assume, up to conjugation, that $g \in D$; therefore, the fixed points of the subgroup $\langle g \rangle$ generated by $g$ are the fundamental points $P_1 = (1:0:0)$, $P_2 = (0:1:0)$, and $P_3 = (0:0:1)$. Since $G$ is abelian, $\langle g \rangle$ is normal in $G$; hence, $G$ acts on $\mathcal{T} = \{P_1, P_2, P_3\}$. As $|G|$ is odd, we have by the orbit-stabilizer theorem that the orbits of any $h \in G$ on $\mathcal{T}$ have length 1 or 3. If $h$ has a single orbit on $\mathcal{T}$, then $h$ is either

$$\begin{pmatrix} 0 & 0 & \lambda \\ \mu & 0 & 0 \\ 0 & \rho & 0 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & \lambda & 0 \\ 0 & 0 & \mu \\ \rho & 0 & 0 \end{pmatrix}; \quad \text{in both cases} \quad h^3 = \begin{pmatrix} \lambda\mu\rho & 0 & 0 \\ 0 & \lambda\mu\rho & 0 \\ 0 & 0 & \lambda\mu\rho \end{pmatrix},$$

that is, $h^3$ is the identity element of $G$ and clearly $G$ cannot be generated by $h$. Therefore, a generator $\alpha$ of $G$ has the form

$$\alpha : (X:Y:T) \mapsto (\theta X : \eta Y : T),$$

with $\theta^{\frac{q+1}{3}} = \eta^{\frac{q+1}{3}} = 1$. If $\theta$ had order $m < (q+1)/3$, then $\alpha^m$ would fix the points of $\mathcal{H}_q \cap (Y=0)$, against the semiregularity of $G$. Then $\theta$ is a primitive $(q+1)/3$-th root of unity, and the same holds for $\eta$; hence

$$\alpha = \alpha_\theta : (X:Y:T) \mapsto (\theta X : \theta^i Y : T),$$

with $\theta$ a primitive $(q+1)/3$-th root of unity, and $i$ coprime with $(q+1)/3$. Let $\zeta \in \mathbb{F}_{q^6}$ with $\zeta^3 = \theta$, and let $\bar{G}$ be the group generated by $\alpha_\zeta : (X:Y:T) \mapsto (\zeta X : \zeta^i Y : T)$. Any element of $\bar{G}$ fixes only the fundamental points, hence $\bar{G}$ is semiregular on $\mathcal{H}_q$; moreover, $G$ is normal in $\bar{G}$ of index 3. Then the thesis follows from Proposition 2.2.4. □

**Proposition 2.2.7.** *Let $G \leq \mathrm{PSU}(3,q)$. If a maximal subgroup of $\mathrm{PSU}(3,q)$ containing $G$ is of type (iii) in Theorem 1.2.6, then $\mathcal{GGS}_{2,m} \not\cong \mathcal{H}_q/G$.*

*Proof.* Let $\mathcal{H}_q$ be given by the Fermat equation (1.3). Up to conjugation, the self-polar triangle stabilized by $G$ is the fundamental triangle $\mathcal{T} = \{P_1, P_2, P_3\}$, whose vertices are not points of $\mathcal{H}_q$. The elements of $G$ stabilizing $\mathcal{T}$ pointwise form a normal subgroup $N$ of $G$, and $G/N$ acts faithfully on $\mathcal{T}$; hence, either $G = N$ or $[G : N] = 3$.

If $G = N$, then $G$ fixes a fundamental point, say $P_1$, and its polar line $P_2P_3$; therefore, the thesis follows from Proposition 2.2.6.

If $[G : N] = 3$, then $N$ is cyclic, by the same argument used in the proof of Proposition 2.2.6; say $N = \langle \alpha_\xi \rangle$, where $\xi$ is a primitive $(q+1)/9$-th root of unity, $\alpha_\xi : (X, Y, T) \mapsto (\xi X, \xi^i Y, T)$, and $i$ is coprime with $(q+1)/9$. Let $h \in G \setminus N$. By arguing as in the proof of Proposition 2.2.6, $h$ has order 3. Moreover, $G$ is the semidirect product $N \rtimes \langle h \rangle$; in fact, $N$ is normal in $G$, $N$ and $\langle h \rangle$ have trivial intersection, and $|G| = |N| \cdot |\langle h \rangle|$. Let $\bar{N}$ be the cyclic group generated by $\alpha_\theta : (X, Y, T) \mapsto (\theta X, \theta^i Y, T)$, where $\theta \in \mathbb{F}_{q^6}$ satisfies $\theta^3 = \xi$. Let $\bar{G}$ be the group generated by $\bar{N}$ and $h$. Then $\bar{G}$ is the semidirect product $\bar{N} \rtimes \langle h \rangle$. We want to double count the size of the set

$$I = \left\{ (\bar{g}, P) \mid \bar{g} \in \bar{G} \setminus \{id\}, \ P \in \mathcal{H}_q, \ \bar{g}(P) = P \right\}.$$

Since $G$ and $\bar{N}$ are semiregular on $\mathcal{H}_q$, we consider only elements of the form $\bar{n}h$ or $\bar{n}h^2$, with $\bar{n} \in \bar{N} \setminus N$. Up to reordering of the fundamental points, we have

$$\bar{n} = \begin{pmatrix} \rho & 0 & 0 \\ 0 & \rho^i & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad h = \begin{pmatrix} 0 & \lambda & 0 \\ 0 & 0 & \mu \\ 1 & 0 & 0 \end{pmatrix}, \tag{2.17}$$

where $\lambda^{q+1} = \mu^{q+1} = 1$, $\gcd(i, (q+1)/3) = 1$, and $\rho = \theta^{3j+u}$ with $0 < j < (q+1)/3$ and $u \in \{1, 2\}$. Hence

$$\bar{n}h = \begin{pmatrix} \rho & 0 & 0 \\ 0 & \rho^i & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & \lambda & 0 \\ 0 & 0 & \mu \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & A & 0 \\ 0 & 0 & B \\ 1 & 0 & 0 \end{pmatrix}, \tag{2.18}$$

where $A^{q+1} = B^{q+1} = 1$, and $\det(\bar{n}h) = AB$ is not a cube in $\mathbb{F}_{q^6}$, since $\bar{n}h \notin \mathrm{PSU}(3,q)$. Then $\bar{n}h$ has three distinct eigenvalues in a cubic extension of $\mathbb{F}_{q^6}$, namely $z$, $zx$, and $z(x+1)$, where $x^2 + x + 1 = 0$ and $z^3 = AB$. Therefore, $\bar{n}h$ has exactly three fixed points, namely

$$Q_1 = \left( z, \frac{z^2}{A}, 1 \right), \quad Q_2 = \left( zx, \frac{z^2x^2}{A}, 1 \right), \quad \text{and} \quad Q_3 = \left( z(x+1), \frac{z^2(x+1)^2}{A}, 1 \right);$$

it is easy to check that $Q_1$, $Q_2$, and $Q_3$ are points of $\mathcal{H}_q$. The same holds for $\bar{n}h^2$.

Therefore, any element $\bar{n}h$ or $\bar{n}h^2$ with $\bar{n} \in \bar{N} \setminus N$ has exactly three fixed points on $\mathcal{H}_q$; then

$$|I| = 2 \cdot \left(|\bar{N}| - |N|\right) \cdot 3 = 2 \cdot \left( \frac{q+1}{3} - \frac{q+1}{9} \right) \cdot 3 = 4 \cdot \frac{q+1}{3}. \tag{2.19}$$

The orbit $\mathcal{O}$ of a point $P \in \mathcal{H}_q$ under $\bar{G}$ has size $|\mathcal{O}| \geq |G| = (q+1)/3$. Then the stabilizer $\mathcal{S}$ of $P$ under $\bar{G}$ has size $|\mathcal{S}| \leq 3$; in particular, $|\mathcal{S}| \in \{1,3\}$ since $|\bar{G}|$ is odd. Hence, the number $|\mathcal{S}|-1$ of pairs in $I$ having $P$ in the second coordinate is either zero or 2.

Therefore $|I| = 2m$, where $m$ is the number of points of $\mathcal{H}_q$ fixed by some non-trivial element of $\bar{G}$. By (2.19), we get

$$m = 2 \cdot \frac{q+1}{3} = 2 \cdot |G|.$$

Hence, $\bar{G}/G$ has two fixed points $R_1, R_2 \in \mathcal{H}_q/G$ and acts semiregularly on $(\mathcal{H}_q/G) \setminus \{R_1, R_2\}$. By Proposition 1.2.13, either $R_1$ or $R_2$ is $\mathbb{F}_{q^6}$-rational. Then the number $|\mathcal{H}_q/G(\mathbb{F}_{q^2})|$ of $\mathbb{F}_{q^2}$-rational points of $\mathcal{H}_q/G$ satisfies

$$|\mathcal{H}_q/G(\mathbb{F}_{q^2})| \equiv |\{P \in \{R_1, R_2\} \mid P \text{ is } \mathbb{F}_{q^2}\text{-rational}\}| \pmod{|\bar{G}/G|},$$

that is, $|\mathcal{H}_q/G(\mathbb{F}_{q^2})|$ is congruent to 1 or 2 modulo 3.

On the other side, the number $|\mathcal{GGS}_{2,m}(\mathbb{F}_{q^2})|$ of $\mathbb{F}_{q^2}$-rational points of $\mathcal{GGS}_{2,m}$ is a multiple of 3, by Proposition 1.2.13. Therefore, $\mathcal{H}_q/G \not\cong \mathcal{GGS}_{2,m}$. □

**Proposition 2.2.8.** *Let* $G \leq \mathrm{PGU}(3,q)$, $G \not\subseteq \mathrm{PSU}(3,q)$. *If a maximal subgroup of* $\mathrm{PSU}(3,q)$ *containing* $G \cap \mathrm{PSU}(3,q)$ *is of type (ii) in Theorem* 1.2.6, *then* $\mathcal{GGS}_{2,m} \not\cong \mathcal{H}_q/G$.

*Proof.* Let $G' = G \cap \mathrm{PSU}(3,q)$. Since $\mathrm{PSU}(3,q)$ has index 3 in $\mathrm{PGU}(3,q)$, we have $\mathrm{PGU}(3,q) = G \cdot \mathrm{PSU}(3,q)$ and $[G : G'] = 3$; hence, $G'$ is normal in $G$ by Lemma 2.2.5. Arguing as in the proof of Proposition 2.2.6, $G'$ is cyclic; moreover, $G'$ is generated by $\alpha_\xi : (X:Y:T) \mapsto (\xi X : \xi^i Y : T)$, where $\xi$ is a primitive $(q+1)/9$-th root of unity and $i$ is coprime with $(q+1)/9$. Then $G$ stabilizes the fundamental triangle $\mathcal{T}$.

If there exists $h \in G \setminus G'$ of order 3, then $G = G' \rtimes \langle h \rangle$ by arguing as in the proof of Proposition 2.2.7. Let $\theta \in \mathbb{F}_{q^6}$ with $\theta^3 = \xi$, and define $\alpha_\theta : (X : Y : T) \mapsto (\theta X : \theta^i Y : T)$. Let $\bar{G'}$ be the cyclic group generated by $\alpha_\theta$, and let $\bar{G}$ be the group generated by $\bar{G'}$ and $h$; then $\bar{G} = \bar{G'} \rtimes \langle h \rangle$. Moreover, $[\bar{G} : G] = [\bar{G'} : G'] = 3$; hence, by Lemma 2.2.5, $G'$ is normal in $\bar{G'}$ and $G$ is normal in $\bar{G}$. We can repeat the same argument used in the proof of Proposition 2.2.7, after replacing $N$ with $G'$ and $\bar{N}$ with $\bar{G'}$; then $|\mathcal{H}_q/G(\mathbb{F}_{q^2})| \equiv 1, 2 \pmod 3$, while $|\mathcal{GGS}_{2,m}| \equiv 0 \pmod 3$. This yields the thesis.

If there is no $h \in G \setminus G'$ of order 3, then $G$ is made of diagonal matrices, since $G$ acts on $\mathcal{T}$. By Theorem 1.2.7, $G$ is cyclic; a generator of $G$ has the form $\alpha_\theta : (X : Y : T) \mapsto (\theta X : \theta^j Y : T)$, with $\theta$ a primitive $(q+1)/3$-th root of unity and $j$ coprime with $(q+1)/3$. Let $\bar{G}$ be the group generated by $\alpha_\zeta : (X : Y : T) \mapsto (\zeta X : \zeta^i Y : T)$, where $\zeta \in \mathbb{F}_{q^6}$ satisfies $\zeta^3 = \theta$. Then $G$ is a normal subgroup of $\bar{G}$ of index 3, and $\bar{G}$ acts semiregularly on $\mathcal{H}_q$. Proposition 2.2.4 yields the thesis. □

**Proposition 2.2.9.** *Let* $G \leq \mathrm{PGU}(3,q)$, $G \not\leq \mathrm{PSU}(3,q)$. *If a maximal subgroup of* $\mathrm{PSU}(3,q)$ *containing* $G \cap \mathrm{PSU}(3,q)$ *is of type (iii) in Theorem* 1.2.6, *then* $\mathcal{GGS}_{2,m} \not\cong \mathcal{H}_q/G$.

*Proof.* As in the proof of Proposition 2.2.8, $G' = G \cap \mathrm{PSU}(3,q)$ is normal in $G$ of index 3. Arguing as in the proof of Proposition 2.2.7, it can be shown that there are two possible cases for $G'$: (A) $G'$ is cyclic and generated by $\alpha_\xi : (X : Y : T) \mapsto (\xi X : \xi^i Y : T)$, with $\xi$ a primitive $(q+1)/9$-th root of unity and $i$ coprime with $(q+1)/9$; (B) $G' = \langle \alpha_\eta \rangle \rtimes \langle h \rangle$, where $\alpha_\eta : (X : Y : T) \mapsto (\eta X : \eta^i Y : T)$ with $\eta$ a primitive $(q+1)/27$-th root of unity and $i$ coprime with $(q+1)/27$, and $h$ is an element of order 3 acting with a single orbit on the fundamental triangle $\mathcal{T}$, hence having the form (2.17).

(A) Since $G'$ is normal in $G$, we have that $G$ acts on $\mathcal{T}$. If $G$ fixes $\mathcal{T}$ pointwise, then the elements of $G$ are diagonal matrices whose diagonal coefficients are $(q+1)/3$-th roots of unity, hence cubes in $\mathbb{F}_{q^2}$; therefore $G \leq \mathrm{PSU}(3,q)$, against the hypothesis. Then $G = G' \rtimes \langle h \rangle$, where $h \in G \setminus G'$ has order 3. Let $\theta \in \mathbb{F}_{q^2}$ with $\theta^3 = \xi$, and let $\bar{G}$ be the group generated by $\alpha_\theta : (X : Y : T) \mapsto (\theta X : \theta^i Y : T)$ and $h$; then $\bar{G} = \langle \alpha_\theta \rangle \rtimes \langle h \rangle$. By arguing as in the proof of Proposition 2.2.7, we have that $|\mathcal{H}_q/G(\mathbb{F}_{q^2})| \equiv 1, 2 \pmod 3$, while $|\mathcal{GGS}_{2,m}| \equiv 0 \pmod 3$. This yields the thesis.

(B) Any element of $G' \setminus \langle \alpha_\eta \rangle$ has order 3; in fact, a matrix $h$ of the form (2.17) has the form (2.18), which has order 3. Therefore, $\langle \alpha_\eta \rangle$ is the only cyclic subgroup of order $(q+1)/27$ in $G'$; note that $(q+1)/27 \neq 3$ since $q$ is a prime power. Thus, $\langle \alpha_\eta \rangle$ is characteristic in $G'$, and hence normal in $G$. Therefore, $G$ acts on the set of points which are fixed by $\langle \alpha_\eta \rangle$, i.e. the fundamental points. Let $G''$ be the subgroup of $G$ fixing $\mathcal{T}$ pointwise. The group $G''$ is abelian, as it is made of diagonal matrices; moreover, $G''$ is normal in $G$ of index 3, and $G = G'' \rtimes \langle h \rangle$. By the primary decomposition of abelian groups, either $G'' = \langle \alpha_\xi \rangle$ with $\xi^3 = \eta$ and $\alpha_\xi : (X : Y : T) \mapsto (\xi X : \xi^i Y : T)$, or $G'' = \langle \alpha_\eta \rangle \times \langle k \rangle$, where $k$ has order 3. In the latter case $\det(k)^3 = 1$, as $k^3$ is the identity element; hence, $\det(k)$ is a cube in $\mathbb{F}_{q^2}$, and $k \in G \cap \mathrm{PSU}(3,q) = G'$. Therefore $G' = G''$, contradicting $h \in G' \setminus G''$. Then $G'' = \langle \alpha_\xi \rangle$ and $G = \langle \alpha_\xi \rangle \rtimes \langle h \rangle$. Let $\bar{G} = \langle \alpha_\theta \rangle \rtimes \langle h \rangle$, with $\theta^3 = \xi$ and $\alpha_\theta : (X : Y : T) \mapsto (\theta X : \theta^i Y : T)$. We can argue as in the proof of Proposition 2.2.7, after replacing $N$ with $\langle \alpha_\xi \rangle$ and $\bar{N}$ with $\langle \alpha_\theta \rangle$; we get that $|\mathcal{H}_q/G(\mathbb{F}_{q^2})| \equiv 1, 2 \pmod 3$, while $|\mathcal{GGS}_{2,m}(\mathbb{F}_{q^2})| \equiv 0 \pmod 3$. This yields the thesis.

□

**Lemma 2.2.10.** *Let $G \leq \mathrm{PSU}(3,q)$. If a maximal subgroup $M$ of $\mathrm{PSU}(3,q)$ containing $G$ is neither of type (ii) nor of type (iii) in Theorem* 1.2.6*, then $M$ is of type (xiv); that is, $G \not\subseteq \mathrm{PSU}(3, 2^{m/3})$ and $M$ contains $\mathrm{PSU}(3, 2^{m/3})$ as a normal subgroup of index* 3.

*Proof.* With the notations of Theorem 1.2.6, we can exclude cases *(ii)* and *(iii)* by hypothesis, case *(i)* by the semiregularity of $G$, and cases *(iv)* and *(xv)* since $|G|$ does not divide neither $3(q^2 - q + 1)$ nor 36. The thesis will follow if we exclude case *(xiii)*. Assume by contradiction that $M$ is of type *(xiii)*; we apply Theorem 1.2.6 to $M = \mathrm{PSU}(3, 2^s)$, where $m = p's$ with $p'$ an odd prime. Note that, since $m \geq 5$ is odd, either $p' \geq 5$, or $p' = 3$ and $s \geq 3$.

Case *(i)*. $G$ fixes an $\mathbb{F}_{2^{2s}}$-rational point $P \in \mathcal{H}_{2^s}$. Since $P \notin \mathcal{H}_q$ by the semiregularity of $G$, $M$ is of type *(ii)* in the list of maximal subgroups of $\mathrm{PSU}(3,q)$, against the hypothesis.

Case *(ii)*. The order $(2^{p's} + 1)/3$ of $G$ divides $2^s(2^s - 1)(2^s + 1)^2/3$, which is impossible.

Case *(iii)*. The order of $G$ divides $2(2^s + 1)^2$, which is impossible.

Case *(iv)*. The order of $G$ divides $2^{2s} - 2^s + 1$, which is impossible.

Case *(xiii)*. $G$ is contained in $\mathrm{PSU}(3,2^r)$, where $s/r$ is an odd prime; hence $m/r \geq 9$. This is impossible, since the order of $G$ is greater than the order of any maximal subgroup of $\mathrm{PSU}(3,2^r)$.

Case *(xiv)*. $G$ is contained in a group $K$ containing $\mathrm{PSU}(3,2^r)$ as a normal subgroup of index 3, where $r = s/3$. If $H$ is a maximal subgroup of $K$ and $H \neq \mathrm{PSU}(3,2^r)$, then $H \cap \mathrm{PSU}(3,2^r)$ has index 3 in $H$; therefore, $|H|/3$ divides the order of a maximal subgroup of $\mathrm{PSU}(3,2^r)$. This yields a contradiction, since, by direct computation, the order of $G$ does not divide three times the order of any maximal subgroup of $\mathrm{PSU}(3,2^r)$.

Case *(xv)*. The order of $G$ divides 36, which is impossible. □

**Proposition 2.2.11.** *Let $G \leq \mathrm{PSU}(3,q)$. If a maximal subgroup $M$ of* $\mathrm{PSU}(3,q)$ *containing $G$ is of type (xiv) in Theorem* 1.2.6*, then $\mathcal{GGS}_{2,m} \ncong \mathcal{H}_q/G$.*

*Proof.* The subgroup $M$ contains $\mathrm{PSU}(3,2^s)$ as a normal subgroup of order 3, where $s = m/3 \geq 3$. As in the proof of Lemma 2.2.10, $|G|$ divides three times the order of a maximal subgroup of $\mathrm{PSU}(3,2^s)$. We apply Theorem 1.2.6 to $\mathrm{PSU}(3,2^s)$.

Case *(i)*. The order $(2^{3s}+1)/3$ of $G$ divides $2^{3s}(2^{2s}-1)$, which is impossible.

Case *(ii)*. The order of $G$ divides $2^s(2^s+1)^2(2^s-1)$, which is impossible.

Case *(iii)*. The order of $G$ divides $6(2^s+1)^2$, which is impossible.

Case *(iv)*. The order of $G$ divides $3(2^{2s}-2^s+1)$; this happens if and only if $s=3$.

Cases *(xiii)* and *(xiv)*. The order of $G$ divides either $3 \cdot |PSU(3,2^r)|$ or $3 \cdot |PGU(3,2^r)|$, where $s/r$ is an odd prime. This is impossible, since $|G|$ exceeds three times the order of any subgroup of $\mathrm{PGU}(3,2^r)$.

Case *(xv)*. The order of $G$ divides 36, which is impossible.

Therefore, we have to consider only case *(iv)*, with $s=3$. In this case, $G$ has order 171 and $G'' = G \cap \mathrm{PSU}(3,2^s)$ has order $|G|/3 = 57$; moreover, $G''$ coincides with the normalizer in $\mathrm{PSU}(3,2^s)$ of a cyclic Singer group $S$. The fixed points of $S$ are three non-collinear points $P_1, P_2, P_3$ whose coordinate are in a cubic extension of $\mathbb{F}_{2^{2s}}$, hence in $\mathbb{F}_{2^{2m}}$. Since $G$ is semiregular, we have that $P_i \notin \mathcal{H}_q$; therefore, $\mathcal{T} = \{P_1, P_2, P_3\}$ is a self-polar triangle with respect to $\mathcal{H}_q$. Since $G$ acts on $\mathcal{T}$, the thesis follows as in the proof of Proposition 2.2.9, after replacing $q$ with $2^s$ and $G'$ with $G''$. □

**Theorem 2.2.12.** *$\mathcal{GGS}_{2,m}$ is not a Galois subcover of the Hermitian curve $\mathcal{H}_q$.*

*Proof.* Suppose $\mathcal{GGS}_{2,m} \cong \mathcal{H}_q/G$. Then $G \nsubseteq \mathrm{PSU}(3,q)$, by Propositions 2.2.6, 2.2.7, 2.2.11 and Lemma 2.2.10. Hence, $G' = G \cap \mathrm{PSU}(3,q)$ has index 3 in $G$. After replacing $G$ with $G'$, we can repeat the proofs of Propositions 2.2.8 and 2.2.9, the proof of Lemma 2.2.10, and the first part of the proof of Proposition 2.2.11. Then $m = 9$, and any maximal subgroup $M$ of $\mathrm{PSU}(3, 2^9)$ containing $G'$ contains also $\mathrm{PSU}(3, 2^3)$ as a normal subgroup of index 3. Moreover, $G'' = G' \cap \mathrm{PSU}(3, 2^3)$ is contained in the normalizer $N'$ of a cyclic Singer group with $|N'| = 57$.

If $G' \leq \mathrm{PSU}(3, 2^3)$, then we argue as in the proof of Proposition 2.2.11, after replacing $G$ with $G'$. In this way we get a contradiction.

If $G' \not\subseteq \mathrm{PSU}(3, 2^3)$, then $G'' = G' \cap \mathrm{PSU}(3, 2^3)$ has order $|G'|/3 = 19$. By Sylow theorems, $G''$ is the only Sylow 19-subgroup of $G'$; hence, $G''$ is a cyclic Singer group. Therefore $G''$ fixes a triangle $\mathcal{T}$ with coordinates in the cubic extension $\mathbb{F}_{2^{18}}$ of $\mathbb{F}_{2^6}$, and $\mathcal{T}$ is self-polar with respect to $\mathcal{H}_{2^9}$. Since $G'$ acts on $\mathcal{T}$, the thesis follows from Proposition 2.2.9. □

Now Theorem 2.2.1 follows.

### 2.2.2 $\mathcal{GS}_q$ is not Galois covered by $\mathcal{H}_{q^3}$, for any $q > 3$

Throughout this section $q > 3$ is a power of a prime $p$. We rely on the following bound by Duursma and Mak.

**Proposition 2.2.13.** ([34, Theorem 1.3]) *If there exists a Galois covering $\mathcal{H}_{q^3} \to \mathcal{GS}_q$ of degree $d$, then*

$$q^2 + q \leq d \leq q^2 + q + 2.$$

Therefore, we have to exclude three possible values of $d$.

**Proposition 2.2.14.** *There is no Galois covering $\varphi : \mathcal{H}_{q^3} \to \mathcal{GS}_q$ of degree $q^2 + q + 2$.*

*Proof.* If such $\varphi$ existed, then $q^2 + q + 2$ would divide the order $q^9(q^9 + 1)(q^6 - 1)$ of $\mathrm{PGU}(3, q^3)$, hence $q^2 + q + 2$ would divide $2128q - 1568$. But this is impossible for any prime power greater than 3. □

Now we consider the case $d = q^2 + q + 1$.

**Lemma 2.2.15.** *Let $G \leq \mathrm{PGU}(3, q^3)$ with $|G| = q^2+q+1$. Then $G \leq \mathrm{PSU}(3, q^3)$.*

*Proof.* If $\mathrm{PSU}(3, q^3) \neq \mathrm{PGU}(3, q^3)$, then $\mathrm{PSU}(3, q^3)$ has index 3 in $\mathrm{PGU}(3, q^3)$ and 3 divides $q^3 + 1$; hence, 3 does not divide $|G|$. Suppose $G \not\subseteq \mathrm{PSU}(3, q^3)$; then $\mathrm{PGU}(3, q^3) = G \cdot \mathrm{PSU}(3, q^3)$, and $G$ has a subgroup $G \cap \mathrm{PSU}(3, q^3)$ of index 3, which is impossible. □

**Proposition 2.2.16.** *There is no Galois covering $\varphi : \mathcal{H}_{q^3} \to \mathcal{GS}_q$ of degree $q^2 + q + 1$.*

*Proof.* Suppose by contradiction that such $\varphi$ exists. Then $\mathcal{GS}_q \cong \mathcal{H}_{q^3}/G$ with $G \leq \mathrm{PSU}(3, q^3)$ by Lemma 2.2.15, and Theorem 1.2.6 can be applied.

Case *(i)*. Let $\mathcal{H}_{q^3}$ be given by the Norm-Trace equation (1.4). Up to conjugation, $G$ fixes the ideal point $P_\infty$ of $\mathcal{H}_{q^3}$. By [47, Section 4], the stabilizer $S$ of $P_\infty$ in $\mathrm{PGU}(3, q^3)$ has order $q^9(q^6 - 1)$. The group $S$ is the semidirect product $Q \rtimes H$, where $Q$ is the unique Sylow $p$-subgroup of $S$, and $H$ is a cyclic group generated by $\alpha_a : (X : Y : T) \mapsto (a^{q^3+1}X : aY : T)$, where $a$ is a primitive $(q^6 - 1)$-th root of unity; moreover, $H$ fixes two $\mathbb{F}_{q^3}$-rational points $P_\infty, O \in \mathcal{H}_{q^3}$ and is semiregular on $\mathcal{H}_{q^3} \setminus \{P_\infty, O\}$. We have $G \subset H$, because $Q$ is normal in $S$, $|Q|$ and $|H|$ are coprime, and $|G|$ divides $|H|$. In particular, $G$ is generated by $\alpha_b : (X : Y : T) \mapsto (b^{q^3+1}X : bY : T)$, with $b = a^{(q^3+1)(q-1)}$. Let $\bar{G}$ be the group generated by $\alpha_c : (X : Y : T) \mapsto (c^{q^3+1}X : cY : T)$, with $c = a^{q-1}$; then $G$ is normal in $\bar{G}$ of index $q^3 + 1$. The group $\bar{G}/G$ fixes two $\mathbb{F}_{q^6}$-rational points of $\mathcal{H}_{q^3}/G$ and acts semiregularly on the other points of $\mathcal{H}_{q^3}/G$. Therefore, the number of $\mathbb{F}_{q^6}$-rational points of $\mathcal{H}_{q^3}/G$ is congruent to 2 modulo $q^3 + 1$. On the other hand, the number of $\mathbb{F}_{q^6}$-rational points of $\mathcal{X}_q$ is $q^7 - q^5 + q^4 + 1$, which is congruent to $q^2 + 1$ modulo $q^3 + 1$.

Case *(ii)*. Let $\mathcal{H}_{q^3}$ be given by the Fermat equation (1.3). Up to conjugation, $G$ fixes the affine point $(0, 0)$ and the line at infinity $\ell : T = 0$. The action of $G$ on $\ell$ is faithful. In fact, if $g \in G$ fixes $\ell$ pointwise, then $g$ is a homology of the form $g : (X : Y : T) \mapsto (X : Y : \lambda T)$, whose order divides $q^3 + 1$; since $|G|$ and $q^3 + 1$ are coprime, $g$ is the identity element. Therefore, as in the proof of Proposition 2.2.6, $G$ is isomorphic to a subgroup of $\mathrm{PGL}(2, q^6)$; by Theorem 1.2.7, $G$ is cyclic. Moreover, since $|G|$ divides $q^6 - 1$, $G$ has two fixed points $P_1, P_2 \in \ell$ and acts semiregularly on $\ell \setminus \{P_1, P_2\}$; see Theorem 1.2.7. As $|\ell \cap \mathcal{H}_{q^3}|$ is congruent to 2 modulo $|G|$, we have that $P_1, P_2 \in \mathcal{H}_{q^3}$. Now the same argument used in case *(i)* yields a contradiction.

Cases *(iii)* and *(iv)*. The order of $G$ does not divide the order of these maximal subgroups.

Case *(v)*. The group $G$ acts on the $q^6+1$ $\mathbb{F}_{q^6}$-rational points of a conic $\mathcal{C}$ defined over $\mathbb{F}_{q^6}$. As in case *(ii)*, $G$ is isomorphic to a cyclic subgroup $\Gamma$ of $\mathrm{PGL}(2, q^6)$ acting on a line $\ell$ with no short orbits apart from two fixed $\mathbb{F}_{q^6}$-rational points. The action of $G$ on $\mathcal{C}$ is equivalent to the action of $\Gamma$ on $\ell$, see [118, Chapt. VIII, Thm. 15]; hence $G$ has no short orbits on $\mathcal{C}$ apart from two fixed $\mathbb{F}_{q^6}$-rational points $P_1, P_2$. If $G$ has a fixed $\mathbb{F}_{q^6}$-point on $\mathcal{H}_{q^3}$, then we get a contradiction by arguing as in case *(i)*. Otherwise, $P_1, P_2 \notin \mathcal{H}_{q^3}$; by [90, Par. 2] and [65, Page 141], $G$ fixes a third $\mathbb{F}_{q^6}$-rational point $P_3 \in \mathcal{H}_{q^3}$, and $\mathcal{T} = \{P_1, P_2, P_3\}$ is a self-polar triangle. Let now $\mathcal{H}_{q^3}$ be given by the Fermat equation (1.3); up to conjugation, $\mathcal{T}$ is the fundamental triangle and a generator of $G$ has the form $g : (X : Y : T) \mapsto (\lambda X : \mu Y : T)$. Then the order $|G|$ of $g$ divides $q^3 + 1$, which is impossible.

Cases *(viii)* to *(xii)*, and case *(xv)*. The order of $G$ does not divide the order of these maximal subgroups.

Cases *(vi)*, *(vii)*, *(viii)*, and *(xiv)*. If $K$ is a group containing $\mathrm{PSU}(3, 2^m)$ as a normal subgroup of index 3, then the order of any maximal subgroup of $K$ divides three times the order of a maximal subgroup of $\mathrm{PSU}(3, 2^m)$. Hence, applying Theorem 1.2.6 to $\mathrm{PSU}(3, p^m)$, it can be checked that $|G|$ does not divide neither the order of any maximal subgroup of $\mathrm{PSU}(3, p^m)$, nor the order of any maximal subgroup of $K$. □

**Lemma 2.2.17.** *Let $G \leq \mathrm{PGU}(3, q^3)$ with $|G| = q(q + 1)$. Then the number of Sylow $p$-subgroups of $G$ is either 1 or $q + 1$.*

*Proof.* Let $Q_1, \ldots, Q_n$ be the Sylow $p$-subgroups of $G$. By [67, Theorem 12.25 (i),(ii)], for each $i = 1, \ldots, n$ there is a unique point $P_i \in \mathcal{H}_{q^3}$ fixed by $Q_i$. Moreover, $P_i$ is $\mathbb{F}_{q^6}$-rational, and $P_i \neq P_j$ for $i \neq j$. If $n > 1$, then $G$ has no fixed points; hence, the length of the orbit $\mathcal{O}_{P_1}$ of $P_1$ under $G$ is at least $q + 1$, since $Q_1$ is semiregular on $\mathcal{H}_{q^3} \setminus \{P_1\}$. On the other hand, the stabilizer of $P_1$ in $G$ has length at least $q$, as it contains $Q_1$. Therefore $|\mathcal{O}_{P_1}| = q + 1$ by the orbit-stabilizer theorem. If $P \in \mathcal{O}_{P_1}$, then the stabilizer of $P$ in $G$ has order $q$, hence $P = P_i$ for some $i \in \{2, \ldots, n\}$. Then $n = q + 1$. □

**Proposition 2.2.18.** *Let $G \leq \mathrm{PGU}(3, q^3)$ with $|G| = q(q + 1)$. If $G$ has a unique Sylow $p$-subgroup $Q$, then $\mathcal{GS}_q$ is not birationally equivalent to $\mathcal{H}_{q^3}/G$.*

*Proof.* Let $\mathcal{H}_{q^3}$ be given by the Norm-Trace equation (1.4). Since $Q$ is normal in $G$, we have that $G$ fixes the unique fixed point of $Q$ on $\mathcal{H}_{q^3}$, which can be assumed to be the ideal point $P_\infty$. The stabilizer of $P_\infty$ in $\mathrm{PGU}(3, q^3)$ is solvable; hence, by Hall's theorem [64, Theorems 2.1-2.4], we have that, up to conjugation, $G = Q \rtimes \langle \alpha_\lambda \rangle$, where $\alpha_\lambda : (X : Y : T) \mapsto (X : \lambda Y : T)$ and $\lambda$ is a primitive $(q+1)$-th root of unity. The genus $g$ of $\mathcal{H}_{q^3}/G$ is computed in [47, Theorem 4.4]. In the terminology of [47, Theorem 4.4], $g = g(\mathcal{GS}_q)$ implies $q = p^w$, that is, the elements of $Q$ are involutions of the form $\beta_\mu : (X : Y : T) \mapsto (X + \mu T : Y : T)$, with $\mu^{q^3} + \mu = 0$. Then there exists a $p$-linearized polynomial $L \in \mathbb{F}_{q^6}[X]$ of degree $q$

dividing $X^{q^3}+X$, such that the set of roots of $L$ coincides with $\{\mu \in \mathbb{F}_{q^6} \mid \beta_\mu \in Q\}$. By [82, Theorem 3.62], there is also a $p$-linearized polynomial $F \in \mathbb{F}_{q^6}[X]$ of degree $q^2$ dividing $X^{q^3}+X$, such that $F(L(X)) = X^{q^3}+X$. Then it is easy to see that the quotient curve $\mathcal{H}_{q^3}/G$ is $\mathbb{F}_{q^6}$-birationally equivalent to the plane curve $\mathcal{C}$ with equation $V^{q^2-q+1} = F(U)$.

Assume that there exists an $\mathbb{F}_{q^6}$-isomorphism $\psi : \mathcal{C} \to \mathcal{GS}_q$. We will show that in this case $F(U)$ cannot be a divisor of $U^{q^3}+U$, which is a contradiction.

By [67, Theorem 12.11], the ideal points $R_\infty \in \mathcal{GS}_q$ and $S_\infty \in \mathcal{C}$ are the unique fixed points of the automorphism groups $\mathrm{Aut}(\mathcal{X}_q)$ and $\mathrm{Aut}(\mathcal{C})$, respectively. Hence, $\psi(S_\infty) = R_\infty$. Also, the coordinate functions have pole divisors

$$div(x)_\infty = (q^2-q+1)R_\infty,\ div(y)_\infty = q^2R_\infty,\ div(u)_\infty = (q^2-q+1)S_\infty,\ div(v)_\infty = q^2S_\infty,$$

and the Weierstrass semigroups at the ideal points are $H(R_\infty) = H(S_\infty) = \langle q^2-q+1, q^2\rangle$ (see [67, Lemmas 12.1, 12.2]). Then $\{1,u\}$ is a basis of the Riemann-Roch space $\mathcal{L}((q^2-q+1)R_\infty)$ and $\{1,u,v\}$ is a basis of $\mathcal{L}(q^2R_\infty)$. Therefore, there exist constants $a,b,c,d,e \in \mathbb{F}_{q^6}$, $a,d \neq 0$, such that $\psi^*(x) = au+b$ and $\psi^*(y) = cu+dv+e$, where $\psi^* : \mathbb{F}_{q^6}(\mathcal{GS}_q) \to \mathbb{F}_{q^6}(\mathcal{C})$ is the pull-back of $\psi$; equivalently, $\psi : (U,V,T) \mapsto (aU+b, cU+dV+e, T)$.

Then the polynomial identity

$$(aU+b)^{q^2} - (aU+b) - (cU+dV+e)^{q^2-q+1} = k\big(F(U) - V^{q^2-q+1}\big)$$

holds for some non-zero $k \in \mathbb{K}$. By comparing the coefficients we get $c = e = 0$, $b \in \mathbb{F}_{q^2}$, and $k = d^{q^2-q+1}$; this implies

$$F(U) = k^{-1}a^{q^2}U^{q^2} - k^{-1}aU.$$

It is easily checked that the conventional $p$-associate of the $p$-linearized polynomial $F(X)$ is not a divisor of the conventional $p$-associate of $U^{q^3}+U$, hence $F(U)$ is not a divisor of $U^{q^3}+U$ by [82, Theorem 3.62]. □

**Lemma 2.2.19.** *Let $G \leq \mathrm{PGU}(3,q^3)$ with $|G| = q(q+1)$. If $G$ has $q+1$ distinct Sylow $p$-subgroup $Q_1,\ldots,Q_{q+1}$, then $G \cong (\mathbb{Z}_{p'})^s \rtimes Q_1$, where $p'$ is a prime and $(p')^s = q+1$.*

*Proof.* By the proof of Lemma 2.2.17, the points $P_1,\ldots,P_{q+1}$, fixed by $Q_1,\ldots,Q_{q+1}$, respectively, form a single orbit $\mathcal{O}$ under the action of $G$. By Burnside's Lemma [17, Chapter VIII, Par. 118], $G$ is sharply 2-transitive on $\mathcal{O}$. Then, by [63, Theorem 20.7.1], $G$ is isomorphic to the group of affine transformations of a near-field

$F$; also, $G$ has a regular normal subgroup $N$, and hence $G = N \rtimes Q_1$. The order $f$ of $F$ satisfies $q(q+1) = (f-1)f$, hence $f = q+1$. This implies that $F$ cannot be one of the seven exceptional near-fields listed in [122] and then $F$ is a Dickson near-field; see [63, Theorem 20.7.2]. In particular, $N$ is isomorphic to the additive group $(\mathbb{Z}_{p'})^s$ of a finite field. □

**Proposition 2.2.20.** *Let $G \leq \mathrm{PGU}(3,q^3)$ with $|G| = q(q+1)$. If $G$ has $q+1$ distinct Sylow $p$-subgroups, then $\mathcal{GS}_q$ is not birationally equivalent to $\mathcal{H}_{q^3}/G$.*

*Proof.* Suppose that $q$ is odd. Then all involutions of $\mathrm{PGU}(3,q^3)$ are conjugate, and they are homologies of $\mathrm{PG}(2,q^6)$; see [75, Lemma 2.2]. The maximum number of pairwise commuting involutions is 3; in fact, two homologies commute if and only if the center of one homology lies on the axis of the other (see [30, Theorem. 3.1.12]). Then $q+1=4$ by Lemma 2.2.19, a contradiction to $q>3$.

Suppose that $q$ is even, and $\mathcal{GS}_q \cong \mathcal{H}_{q^3}/G$. Let $Q_1,\ldots,Q_{q+1}$ be the Sylow $p$ subgroups of $G$. The group $Q_1$ is isomorphic to the multiplicative group of $F$, hence $Q_1$ is metacyclic; see e.g. [20, Ex. 1.19]. Also, $Q_1$ has exponent 2 or 4 by [75, Lemma 2.1]. Therefore, $q \in \{2,4,8,16\}$. The case $q=2$ is excluded. If $q=16$, then $F$ has prime order 17 and $F$ is a field; hence $Q_1$ has exponent 16, a contradiction.

For $q \in \{4,8\}$ we apply the Riemann-Hurwitz genus formula to the covering $\mathcal{H}_{q^3} \to \mathcal{GS}_q$, in order to get a contradiction on the degree

$$\Delta = (2g(\mathcal{H}_{q^3})-2) - |G|\,(2g(\mathcal{X}_q)-2)$$

of the different divisor. By [107, Theorem 3.8.7],

$$\Delta = \sum_{\sigma \in G \setminus \{id\}} i(\sigma),$$

where $i(\sigma) \geq 0$ satisfies the following conditions.

- If $\sigma$ has order 2, then $i(\sigma) = q^3+2$; if $\sigma$ has order 4, then $i(\sigma)=2$ (see [107, Eq. (2.12)]).
- If $\sigma$ has odd order, then $i(\sigma)$ equals the number of fixed points of $\sigma$ on $\mathcal{H}_{q^3}$, see [107, Cor. 3.5.5]. Also, by [65, pp. 141-142], either $\sigma$ has exactly 3 fixed points or $\sigma$ is a homology. In the former case $i(\sigma) \leq 3$, in the latter $i(\sigma) = q^3+1$.

If $q = 4$, then $\Delta = 470$ and $G = \mathbb{Z}_5 \rtimes Q_1$. If $Q_1 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, then $G$ has 15 involutions, whose contributions to $\Delta$ sum up to $990 > \Delta$. Then $Q_1 \cong \mathbb{Z}_4$, and the contributions of the $Q_i$'s to $\Delta$ sum up to $5 \cdot 66 + 10 \cdot 2 = 350$. The remaining four non-trivial elements of $G$ are generators of $\mathbb{Z}_5$; then either all of them are homologies, or all of them fix 3 points. In both cases, their contribution cannot be equal to $120 = \Delta - 350$.

Let $q = 8$, hence $\Delta = 7758$ and $G = (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes Q_1$. If $Q_1$ has more than one involution, then the involutions of $G$ contribute to $\Delta$ for at least $18 \cdot 514 > \Delta$. Hence, $Q_1$ is the quaternion group, and the sum of $Q_i$'s contributions to $\Delta$ is $9 \cdot 514 + 54 \cdot 2 = 4734$. The contribution to $\Delta$ of the elements of $\mathbb{Z}_3 \times \mathbb{Z}_3$ is either 513 or less than 4; hence, it cannot sum up to $3024 = \Delta - 4734$. □

The following result follows rom Lemma 2.2.17 and Propositions 2.2.18 and 2.2.20.

**Proposition 2.2.21.** *There is no Galois covering $\mathcal{H}_{q^3} \to \mathcal{GS}_q$ of degree $q^2 + q$.*

From Propositions 2.2.13, 2.2.14, 2.2.16, and 2.2.21, Theorem 2.2.2 follows.

## 2.3 Some Ree and Suzuki curves are not quotients of the Hermitian curve

The results of this section are the object of [92]. We prove that the Suzuki and Ree curves over $\mathbb{F}_q$ for the smallest values of $q$, are not quotients of the corresponding maximal Hermitian curves. We use the notation and results of Section 1.2.

**Theorem 2.3.1.** *The Suzuki curve $\mathcal{S}_8$ is not a quotient curve of $\mathcal{H}_{64}$.*

**Theorem 2.3.2.** *The Ree curve $\mathcal{R}_3$ is not a quotient curve of $\mathcal{H}_{27}$.*

We note that Theorem 2.3.2 is an unpublished result due to Rains and Zieve.

In analogy with the Suzuki curves, we can define the plane curve

$$\mathcal{S}_2 : \quad Y^2 + Y = X(X^2 + X)$$

over $\mathbb{F}_2$. We prove the following proposition.

**Proposition 2.3.3.** *The curve $\mathcal{S}_2$ is a quotient curve of $\mathcal{H}_4$.*

We classify the elements of $\mathrm{PGU}(3,q)$ in terms of their order and their action on $\mathrm{PG}(2,\mathbb{K})$ and $\mathcal{H}_q$. In this way, we get the contribution of any element $\sigma \in \mathrm{PGU}(3,q)$ to the degree of the different exponent of a Galois covering $\mathcal{H}_q \to \mathcal{H}_q/G$, where $G \leq \mathrm{PGU}(3,q)$ contains $\sigma$; see Theorem 2.3.9. This is a result of independent interest, which extends [34, Lemma 4.1].

In Section 2.3.1 we present some preliminary results on quotient curves of the Hermitian curve and the proof of Proposition 2.3.3. Sections 2.3.2 and 2.3.3 contain the proofs of Theorems 2.3.1 and 2.3.2, respectively. Section 2.3.4 provides the spectrum of genera of quotient curves of $\mathcal{H}_{27}$ and three examples of quotient curves of $\mathcal{R}_3$ which are not quotient curves of $\mathcal{H}_{27}$.

### 2.3.1 Preliminary results

In our investigation it is useful to know how an element of $\mathrm{PGU}(3,q)$ of a given order acts on $\mathrm{PG}(2,\mathbb{K})$, and in particular on $\mathcal{H}_q(\mathbb{F}_{q^2})$. This can be obtained as a corollary of Theorem 1.2.6, and is stated in Lemma 2.2 with the usual terminology of collineations of projective planes; see [72]. In particular, a linear collineation $\sigma$ of $\mathrm{PG}(2,\bar{\mathbb{F}}_q)$ is a $(P,\ell)$-*perspectivity*, if $\sigma$ preserves each line through the point $P$ (the *center* of $\sigma$), and fixes each point on the line $\ell$ (the *axis* of $\sigma$). A $(P,\ell)$-perspectivity is either an *elation* or a *homology* according as $P \in \ell$ or $P \notin \ell$. A $(P,\ell)$-perspectivity is in $\mathrm{PGL}(3,q^2)$ if and only if its center and its axis are in $\mathrm{PG}(2,\mathbb{F}_{q^2})$.

**Lemma 2.3.4.** *For a nontrivial element $\sigma \in \mathrm{PGU}(3,q)$, one of the following cases holds.*

*(A)* $\mathrm{ord}(\sigma) \mid (q+1)$. *Moreover, $\sigma$ is a homology whose center $P$ is a point off $\mathcal{H}_q$ and whose axis $\ell$ is a chord of $\mathcal{H}_q(\mathbb{F}_{q^2})$ such that $(P,\ell)$ is a pole-polar pair with respect to the unitary polarity associated to $\mathcal{H}_q(\mathbb{F}_{q^2})$.*

*(B)* $\mathrm{ord}(\sigma)$ *is coprime to $p$. Moreover, $\sigma$ fixes the vertices $P_1,P_2,P_3$ of a non-degenerate triangle $T$.*

*(B1) The points $P_1,P_2,P_3$ are $\mathbb{F}_{q^2}$-rational, $P_1,P_2,P_3 \notin \mathcal{H}_q$ and the triangle $T$ is self-polar with respect to the unitary polarity associated to $\mathcal{H}_q(\mathbb{F}_{q^2})$. Also,* $\mathrm{ord}(\sigma) \mid (q+1)$.

*(B2) The points $P_1,P_2,P_3$ are $\mathbb{F}_{q^2}$-rational, $P_1 \notin \mathcal{H}_q$, $P_2,P_3 \in \mathcal{H}_q$. Also,* $\mathrm{ord}(\sigma) \mid (q^2-1)$ *and* $\mathrm{ord}(\sigma) \nmid (q+1)$.

*(B3) The points $P_1,P_2,P_3$ have coordinates in $\mathbb{F}_{q^6} \setminus \mathbb{F}_{q^2}$, and $P_1,P_2,P_3 \in \mathcal{H}_q$. Also,* $\mathrm{ord}(\sigma) \mid (q^2-q+1)$.

*(C)* $\mathrm{ord}(\sigma) = p$. *Moreover, $\sigma$ is an elation whose center $P$ is a point of $\mathcal{H}_q$ and whose axis $\ell$ is a tangent of $\mathcal{H}_q(\mathbb{F}_{q^2})$ such that $(P, \ell)$ is a pole-polar pair with respect to the unitary polarity associated to $\mathcal{H}_q(\mathbb{F}_{q^2})$.*

*(D)* $\mathrm{ord}(\sigma) = p$ *with* $p \neq 2$, *or* $\mathrm{ord}(\sigma) = 4$ *and* $p = 2$. *Moreover, $\sigma$ fixes an $\mathbb{F}_{q^2}$-rational point $P \in \mathcal{H}_q$, and a line $\ell$ which is a tangent of $\mathcal{H}_q(\mathbb{F}_{q^2})$, such that $(P, \ell)$ is a pole-polar pair with respect to the unitary polarity associated to $\mathcal{H}_q(\mathbb{F}_{q^2})$.*

*(E)* $p \mid \mathrm{ord}(\sigma)$, $p^2 \nmid \mathrm{ord}(\sigma)$, *and* $\mathrm{ord}(\sigma) \neq p$. *Moreover, $\sigma$ fixes two $\mathbb{F}_{q^2}$-rational points $P, Q$, with $P \in \mathcal{H}_q$, $Q \notin \mathcal{H}_q$.*

*Proof.* Let $p \mid \mathrm{ord}(\sigma)$, $\mathrm{ord}(\sigma) \neq p$, and $(p, \mathrm{ord}(\sigma)) \neq (2, 4)$. By [90, §2 p. 212] and [65, pp. 141-142], the fixed elements of $\sigma$ are two points $P, Q$, the line $PQ$, and another line $\ell$ through $P$. Also, $p^2 \nmid \mathrm{ord}(\sigma)$. The Frobenius collineation $\Phi_{q^2} : (X : Y : T) \mapsto (X^{q^2} : Y^{q^2} : T^{q^2})$ commutes with $\sigma$. Hence $\Phi_{q^2}$ acts on $\{P, Q\}$, and $P, Q$ are $\mathbb{F}_{q^4}$-rational. If $R \in \{P, Q\}$ is the pole of $PQ$, then $R \in \mathcal{H}_q$. Since $\mathcal{H}_q$ has no points with coordinates in $\mathbb{F}_{q^4} \setminus \mathbb{F}_{q^2}$, $R$ is $\mathbb{F}_{q^2}$-rational. Thus the line $PQ$ is a tangent of $\mathcal{H}_q(\mathbb{F}_{q^2})$ at $R$. Hence the pole of $\ell$ is $\mathbb{F}_{q^2}$-rational and off $\ell$. Therefore $R = P$ and the assertions of Case (E) follow.

Let $\mathrm{ord}(\sigma) = p$, and let $\mathcal{H}_q$ have Norm-Trace equation (1.4). Up to conjugation, $\sigma$ is contained in the Sylow $p$-subgroup $S$ of $\mathrm{PGU}(3, q)$ defined by $S = \{\tau_{1,b,c} \mid b, c \in \mathbb{F}_{q^6},\ b^{q+1} = c^q + c\}$, where

$$\tau_{1,b,c} = \begin{pmatrix} 1 & b^q & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}. \tag{2.20}$$

Hence $\sigma$ fixes the $\mathbb{F}_{q^2}$-rational point $P_\infty = (1 : 0 : 0) \in \mathcal{H}_q$ and its polar line $\ell_\infty : T = 0$, which satisfies $\ell_\infty \cap \mathcal{H}_q = \{P_\infty\}$. If $p = 2$, then $\sigma$ is of type $\tau_{1,0,c}$, and $\sigma$ is an elation with center $P_\infty$ and axis $\ell_\infty$, which is Case (C). If $p \neq 2$, then by [90, §2 p. 212] $\sigma = \tau_{1,b,c}$ satisfies either Case (C) or Case (D). By direct computation, Cases (C) and (D) correspond to $b = 0$ and $b \neq 0$, respectively.

Let $p \nmid \mathrm{ord}(\sigma)$. By [90, §2 p. 212] and [65, pp. 141-142], either $\sigma$ fixes a point $P$ and a line $\ell$ pointwise, or $\sigma$ fixes exactly three non-collinear points.

Assume that the former case holds. Then $P$ and $\ell$ are fixed by $\Phi_{q^2}$. Hence, they are defined over $\mathbb{F}_{q^2}$. We have $P \notin \mathcal{H}_q$. In fact, if $P \in \mathcal{H}_q$, then the tangent to $\mathcal{H}_q$ at $P$ intersect $\ell$ at an $\mathbb{F}_{q^2}$-rational point $Q \notin \mathcal{H}_q$, and the $\mathbb{F}_{q^2}$-rational pole $R$ of $\ell$ lies on $\ell$, hence also on $\mathcal{H}_q$. For any $\mathbb{F}_{q^2}$-rational point $\bar{P}$ of $\ell \setminus \{R\}$, we have that $\bar{P} \notin \mathcal{H}_q$ and the polar line of $\bar{P}$ intersects $\ell$ at another $\mathbb{F}_{q^2}$-rational point of $\ell$. Since the line $PQ$ is the polar line of $P$, this is a contradiction. Therefore, $\ell$ is the polar line of $P$, and $\ell$ is a chord of $\mathcal{H}_q(\mathbb{F}_{q^2})$. Now we show that $\mathrm{ord}(\sigma) \mid (q+1)$. Let $\mathcal{H}_q$ have Fermat equation (1.3). Up to conjugation, $P = (0:0:1)$ and $\ell : T = 0$. Hence $\sigma$ is a diagonal matrix of the form $\mathrm{diag}(\lambda, 1, 1)$, which implies $\mathrm{ord}(\sigma) = \mathrm{ord}(\lambda)$ with $\mathrm{ord}(\lambda) \mid (q+1)$. This shows that $\sigma$ satisfies Case (A).

Now assume that $\sigma$ fixes exactly the vertices $P_1, P_2, P_3$ of a triangle $T$.

- Suppose that $P_1$, $P_2$, and $P_3$ are $\mathbb{F}_{q^2}$-rational. If $P_1, P_2, P_3 \notin \mathcal{H}_q$, then $P_jP_k$ is the polar line of $P_i$, for $\{i,j,k\} = \{1,2,3\}$. Let $\mathcal{H}_q$ have Fermat equation (1.3). Up to conjugation $P_1$, $P_2$, and $P_3$ are the fundamental points. Thus $\sigma$ is a diagonal matrix and $\mathrm{ord}(\sigma) \mid (q+1)$, which is Case (B1). Assume $P_2 \in \mathcal{H}_q$. Then the polar line $\ell_2$ of $P_2$ is either $P_1P_2$ or $P_2P_3$, say $P_1P_2$. The polar line $\ell_3$ of $P_3$ is either $P_1P_3$ or $P_2P_3$, whence $P_3 \in \ell_3$ and $P_3 \in \mathcal{H}_q$. Then $\ell_3 \cap \mathcal{H}_q = \{P_3\}$, and hence $\ell_3$ is $P_1P_3$. This implies that $P_2P_3$ is the polar line of $P_1$ and $P_1 \notin \mathcal{H}_q$. Let $\mathcal{H}_q$ have Norm-Trace equation (1.4). Up to conjugation, $P_2 = (1:0:0)$ and $P_3 = (0:0:1)$. Thus $P_1 = (0:1:0)$ and $\sigma$ is the diagonal matrix $\mathrm{diag}(\mu^{q+1}, \mu, 1)$ for some $\mu \in \mathbb{F}_{q^2}^*$. Since $\sigma$ is not a homology, $\mathrm{ord}(\sigma) = \mathrm{ord}(\mu)$ does not divide $q+1$. This is Case (B2).

- Suppose that $P_1$ has coordinates in $\mathbb{F}_{q^6} \setminus \mathbb{F}_{q^2}$. The orbit of $P_1$ under $\Phi_{q^2}$ is $\{P_1, P_2, P_3\}$. Hence, $P_2$ and $P_3$ have coordinates in $\mathbb{F}_{q^6} \setminus \mathbb{F}_{q^2}$ as well. Assume $P_1 \in \mathcal{H}_q$. Then the polar line $\ell_1$ of $P_1$ is tangent to $\mathcal{H}_q$ at $P_1$ and $\ell_1$ has exactly another point $P$ in common with $\mathcal{H}_q$, which is then fixed by $\sigma$. Up to reordering, $P = P_2$. In the same way, $P_3 \in \mathcal{H}_q$ and the polar line of $P_1, P_2, P_3$ are $P_1P_2$, $P_2P_3$, $P_3P_1$, respectively. Let $H \leq \mathrm{PGU}(3,q)$ be the Singer group consisting of the elements of $\mathrm{PGU}(3,q)$ fixing the triangle $T$. Then $H$ has order $q^2-q+1$ by Theorem 1.2.6. Since $\sigma \in H$, $\mathrm{ord}(\sigma) \mid (q^2-q+1)$ and $\sigma$ satisfies Case (B3).

  Elements satisfying Case (B3) do exist; see for instance [27, Lemma 4.4]. The number $k$ of triangles $T$ whose vertices $Q_1, Q_2, Q_3$ are such that $Q_i \in \mathrm{PG}(2,q^6) \setminus \mathrm{PG}(2,q^2)$ and there exists some $\sigma \in \mathrm{PGU}(3,q)$ stabilizing $T$, is equal to the index in $\mathrm{PGU}(3,q)$ of the normalizer $N$ of $H$. By Case (iv) in Theorem 1.2.6, $|N| = 3(q^2-q+1)$. Hence $k = q^3(q+1)^2(q-1)/3$. By direct computation, $k$ is equal to the number of triangles $T'$ whose vertices $Q_1', Q_2', Q_3'$ are such that $Q_i' \in \mathrm{PG}(2,q^6) \setminus \mathrm{PG}(2,q^2)$ and $Q_i' \in \mathcal{H}_q$, $i = 1,2,3$. Therefore, it is not possible that $P_1, P_2, P_3$ have coordinates in $\mathbb{F}_{q^6} \setminus \mathbb{F}_{q^2}$ and $P_1 \notin \mathcal{H}_q$.

- The case that $P_1$ has coordinates in $\mathbb{F}_{q^4} \setminus \mathbb{F}_{q^2}$ cannot occur. In fact, since $\Phi_{q^2}$ acts on $\{P_1, P_2, P_3\}$, if $P_1 \in \mathrm{PG}(2, \mathbb{F}_{q^4}) \setminus \mathrm{PG}(2, \mathbb{F}_{q^2})$, then up to reordering $P_2 \in \mathrm{PG}(2, \mathbb{F}_{q^4}) \setminus \mathrm{PG}(2, \mathbb{F}_{q^2})$ and $P_3 \in \mathrm{PG}(2, q^2)$. Let $i, j \in \{1, 2, 3\}$, $i \neq j$. By [90, §2 p. 212] and [65, pp. 141-142], any power of $\sigma$ either fixes the line $P_iP_j$ pointwise or has no fixed points on $P_iP_j \setminus \{P_i, P_j\}$. Thus $\sigma$ has long orbits on $P_iP_j \setminus \{P_i, P_j\}$. In particular, $\mathrm{ord}(\sigma)$ divides the number of $\mathbb{F}_{q^2}$-rational points of both $P_1P_2$ and $P_1P_3 \setminus \{P_3\}$, a contradiction.

□

Throughout the paper, a nontrivial element of $\mathrm{PGU}(3, q)$ is said to be of type (A), (B), (B1), (B2), (B3), (C), (D), or (E), as given in Lemma 2.3.4. Moreover, $G$ always stands for a subgroup of $\mathrm{PGU}(3, q)$.

**Lemma 2.3.5.** *Let $H$ be a normal subgroup of $G$. Let $A$ be the set of points of $\mathrm{PG}(2, \mathbb{K})$ fixed by every element of $H$, and $B = A \cap \mathcal{H}_q$. Then $G$ acts on $B$ and on $A \setminus B$.*

**Lemma 2.3.6.** *Let $H$ be a $m$-subgroup of $\mathrm{PGU}(3, q)$, where $m \notin \{2, 3\}$ is a prime divisor of $q + 1$. Then $H$ is abelian. Also, the nontrivial elements of $H$ are either of types (A) or (B1), and in the latter case the fixed triangle $T$ is the same for every element of $H$. In addiction, if $H$ is a Sylow $m$-subgroup of $\mathrm{PGU}(3, q)$, then the unique fixed points of $H$ are the vertices of $T$ and $H$ is the direct product of two cyclic groups whose nontrivial elements are of type (A).*

*Proof.* Since $p \notin \{2, 3\}$, the maximum power of $m$ dividing $|\mathrm{PGU}(3, q)|$ is a square, say $m^{2s}$. Let $\mathcal{H}_q$ have Fermat equation (1.3), and define

$$K = \{\mathrm{diag}(\lambda, \mu, 1) \mid \lambda^s = \mu^s = 1\} \cong \{\mathrm{diag}(\lambda, 1, 1) \mid \lambda^s = 1\} \times \{\mathrm{diag}(1, \mu, 1) \mid \mu^s = 1\}. \tag{2.21}$$

Then $K$ is an abelian Sylow $m$-subgroup of $\mathrm{PGU}(3, q)$, whose fixed points are the fundamental points. Also, the nontrivial elements of $K$ are either of type (A) or (B1). Up to conjugation, $H$ is contained in $K$ and the claim follows. □

**Lemma 2.3.7.** *Let $H$ be a $m$-subgroup of $\mathrm{PGU}(3, q)$, where $m$ is an odd prime divisor of $q - 1$. Then $H$ is abelian and the unique fixed points of $H$ are the vertices of a triangle $T$.*

*Proof.* Let $\mathcal{H}_q$ have Norm-Trace equation (1.4), and define

$$K = \{\mathrm{diag}(a^{q+1}, a, 1) \mid a \in \mathbb{F}_{q^2}^*\}. \tag{2.22}$$

Then $K$ is an abelian Sylow $m$-subgroup of $\mathrm{PGU}(3,q)$, and the nontrivial elements of $K$ fix exactly the fundamental points. Up to conjugation, $H$ is contained in $K$ and the claim follows. □

**Lemma 2.3.8.** *Let $p \in \{2,3\}$. If $G$ has a nontrivial normal subgroup $H$ of prime order other than p, then $p^2 \nmid |G|$.*

*Proof.* Assume by contradiction that $p^2 \mid |G|$ and let $\sigma \in H$. By Lemma 2.3.4, the type of $\sigma$ is either (A) or (B). Suppose that $\sigma$ is of type (A). Then, since $H = \langle\sigma\rangle$, all nontrivial elements of $H$ are of type (A) and they have the same center $P$ and axis $\ell$. On the other hand, by Lemma 2.3.5, any $p$-element of $G$ fixes $P$ and acts on $\ell$; a contradiction to Lemma 2.3.4. Suppose that $\sigma$ is of type (B). Then, since $H = \langle\sigma\rangle$, all nontrivial elements of $H$ are of type (B) and they fix the same triangle $T$. By Lemma 2.3.5, $G$ preserves $T$. Hence, by the orbit-stabilizer theorem, the elements of $G$ fixing $T$ pointwise form a subgroup $M$ of index 1, 2, or 3. In all cases, $M$ contains a $p$-element of type (A) or type (B), a contradiction to Lemma 2.3.4. □

Let $G$ be a subgroup of $\mathrm{PGU}(3,q)$ and $\Delta$ be the degree of the Different divisor of the covering $\mathcal{H}_q \to \mathcal{H}_q/G$, that is, $\Delta = (2g(\mathcal{H}_q)-2) - |G|(2g(\mathcal{H}_q/G)-2)$. The Hilbert's Different formula can be written as

$$\Delta = \sum_{\sigma \in G\setminus\{id\}} i(\sigma),$$

where

$$i(\sigma) = \textstyle\sum_{P\in\mathcal{H}_q(\bar{\mathbb{F}}_q)} v_P(\sigma(t)-t), \tag{2.23}$$

with $t$ a local parameter at $P$.

By analyzing the geometric properties of the elements $\sigma \in \mathrm{PGU}(3,q)$, it turns out that there are only a few possibilities for $i(\sigma)$. This is obtained as a corollary of Lemma 2.3.4 and stated in the following proposition.

**Theorem 2.3.9.** *For any nontrivial element $\sigma \in \mathrm{PGU}(3,q)$ the following holds.*

1. *If $\mathrm{ord}(\sigma) = 2$ and $2 \mid (q+1)$, then $\sigma$ is of type (A) and $i(\sigma) = q+1$.*

2. *If $\mathrm{ord}(\sigma) = 3$, $3 \mid (q+1)$ and $\sigma$ is of type (B3), then $i(\sigma) = 3$.*

3. *If $\mathrm{ord}(\sigma) \neq 2$, $\mathrm{ord}(\sigma) \mid (q+1)$ and $\sigma$ is of type (A), then $i(\sigma) = q+1$.*

4. *If $\mathrm{ord}(\sigma) \neq 2$, $\mathrm{ord}(\sigma) \mid (q+1)$ and $\sigma$ is of type (B1), then $i(\sigma) = 0$.*

5. *If* $\mathrm{ord}(\sigma) \mid (q^2-1)$ *and* $\mathrm{ord}(\sigma) \nmid (q+1)$*, then* $\sigma$ *is of type* (B2) *and* $i(\sigma)=2$.

6. *If* $\mathrm{ord}(\sigma) \neq 3$ *and* $\mathrm{ord}(\sigma) \mid (q^2-q+1)$*, then* $\sigma$ *is of type* (B3) *and* $i(\sigma)=3$.

7. *If* $p=2$ *and* $\mathrm{ord}(\sigma)=4$*, then* $\sigma$ *is of type* (D) *and* $i(\sigma)=2$.

8. *If* $\mathrm{ord}(\sigma)=p$*,* $p\neq 2$ *and* $\sigma$ *is of type* (D)*, then* $i(\sigma)=2$.

9. *If* $\mathrm{ord}(\sigma)=p$ *and* $\sigma$ *is of type* (C)*, then* $i(\sigma)=q+2$.

10. *If* $\mathrm{ord}(\sigma)\neq p$*,* $p \mid \mathrm{ord}(\sigma)$ *and* $\mathrm{ord}(\sigma)\neq 4$*, then* $\sigma$ *is of type* (E) *and* $i(\sigma)=1$.

*Proof.* Suppose $p \nmid \mathrm{ord}(\sigma)$. Then by [67, Theorem 11.74] $i(\sigma)$ equals the number of points of $\mathcal{H}_q$ fixed by $\sigma$. Also, for $q$ odd all involutions are conjugated and are of type (A), by [75, Lemma 2.2 (ii)]. Therefore Cases (1) - (6) follow from Lemma 2.3.4.

Suppose $\mathrm{ord}(\sigma)=p$, or $p=2$ and $\mathrm{ord}(\sigma)=4$. As in the proof of Lemma 2.3.4, we can assume that $\sigma$ has the form $\tau_{1,b,c}$ defined in (2.20). By direct computation, $\sigma$ is of type (C) or (D) if and only if $b=0$ or $b\neq 0$, respectively. By [47, Eq. (2.12)], $b=0$ or $b\neq 0$ if and only if $i(\sigma)=q+2$ or $i(\sigma)=2$, respectively. From this, Cases (8) and (9) follow. Since $(p,\mathrm{ord}(\tau_{1,b,c}))=(2,4)$ implies $b\neq 0$, Case (7) follows as well.

Suppose $p \mid \mathrm{ord}(\sigma)$, $\mathrm{ord}(\sigma)\neq p$, and $\mathrm{ord}(\sigma)\neq 4$. By [90, §2 p. 212] and [65, pp. 141-142], $\sigma$ is of type (E). Let $P\in\mathcal{H}_q$ be the unique fixed point of $\sigma$ on $\mathcal{H}_q$. By [67, Theorem 11.74], $\sigma$ is in the stabilizer of $P$ but is not a $p$-element. Hence $i(\sigma)=1$. Since Cases (A) - (E) in Lemma 2.3.4 cover all nontrivial elements of $\mathrm{PGU}(3,q)$, Cases (1) - (10) give a complete classification. □

Theorem 2.3.9 extends [34, Lemma 4.1], where the result is for $\sigma$ fixing an $\mathbb{F}_{q^2}$-rational point of $\mathcal{H}_q$. Groups fixing an $\mathbb{F}_{q^2}$-rational point of $\mathcal{H}_q$ are investigated in [47].

**Theorem 2.3.10.** [47, Theorem 3.3 and Eq. (2.12)] *Let* $p=2$*. For a positive integer* $g$*, the following assertions are equivalent.*

1. *There exists a* 2*-subgroup* $G\leq \mathrm{PGU}(3,q)$ *such that* $g=g(\mathcal{H}_q/G)$.

2. $g=2^{n-v-1}(2^{n-w}-1)$ *with* $0\leq v\leq n-1$ *and* $0\leq w\leq n-1$*, and there exist additive subgroups* $V\subseteq\mathbb{F}_{q^2}$ *and* $W\subseteq\mathbb{F}_q$ *of order* $\mathrm{ord}(V)=2^v$ *and* $\mathrm{ord}(W)=2^w$*, such that* $V^{q+1}=\{b^{q+1}\mid b\in V\}$ *is contained in* $W$.

Assume that assertions (1) and (2) hold, and let $\mathcal{H}_q$ have Norm-Trace equation (1.4). Up to conjugation the unique point of $\mathcal{H}_q$ fixed by every element of $G$ is $P_\infty = (1:0:0)$, and the elements of $G$ have the form (2.20). Then $|G| = 2^{v+w}$ and the additive subgroups $\{b \in \mathbb{F}_{q^2} \mid \tau_{1,b,c} \in G\} \leq \mathbb{F}_{q^2}$ and $\{c \in \mathbb{F}_{q^2} \mid \tau_{1,0,c} \in G\} \leq \mathbb{F}_q$ have order $2^v$ and $2^w$, respectively. In particular, the number of involutions of $G$ equals $2^w - 1$.

**Theorem 2.3.11.** [47, Theorem 4.4 and Eq. (2.12)] *Let $G$ fix an $\mathbb{F}_{q^2}$-rational point $P \in \mathcal{H}_q$, and let $|G| = m \cdot p^u$ with $m > 1$, $m$ coprime with $p$. Then $\mathcal{H}_q/G$ has genus*

$$g(\mathcal{H}_q/G) = \frac{(q-p^w)\,(q-(\gcd(m,q+1)-1)p^v)}{2mp^u},$$

*where $v, w$ are non-negative integers such that $v + w = u$.*

Assume that $G$ satisfies the hypotheses of Theorem 2.3.11 and let $\mathcal{H}_q$ have Norm-Trace equation (1.4). Up to conjugation $P = (1:0:0)$ and the elements of $G$ have the form

$$\tau_{a,b,c} = \begin{pmatrix} a^{q+1} & b^q & c \\ 0 & a & b \\ 0 & 0 & 1 \end{pmatrix},$$

with $a, b, c \in \mathbb{F}_{q^2}$, $a \neq 0$, $b^{q+1} = c^q + c$. Then the additive subgroups $\{b \in \mathbb{F}_{q^2} \mid \tau_{1,b,c} \in G\}$ and $\{c \in \mathbb{F}_{q^2} \mid \tau_{1,0,c} \in G\}$ of $\mathbb{F}_{q^2}$ have order $p^v$ and $p^w$, respectively. In particular, the number of nontrivial elements $\sigma \in G$ with $i(\sigma) = q + 2$ equals $p^w - 1$.

As a consequence of Theorem 2.3.9, the following result is obtained.

**Proposition 2.3.12.** *$\mathcal{S}_2 : Y^2 + Y = X(X^2 + X)$ is Galois covered by $\mathcal{H}_4$.*

*Proof.* The curve $\mathcal{S}_2$ has genus 1 and is $\mathbb{F}_{16}$-maximal. Let $G \leq \mathrm{PGU}(3,4)$ be a cyclic group of order 4. By Theorem 2.3.9, the $\mathbb{F}_{16}$-maximal quotient curve $\mathcal{H}_4/G$ is elliptic. By [73, Theorem 77], there is only one $\mathbb{F}_{16}$-isomorphism class of $\mathbb{F}_{16}$-maximal elliptic curves. Then $\mathcal{S}_2$ is $\mathbb{F}_{16}$-isomorphic to $\mathcal{H}_4/G$. □

Throughout the rest of the paper, $C_r$ stands for a cyclic group of order $r$, $S_m$ is a Sylow $m$-subgroup of $G$, and $n_m$ is the number of Sylow $m$-subgroups of $G$.

### 2.3.2 Proof of Theorem 2.3.1

By contradiction, let $G \leq \mathrm{PGU}(3,64)$ be such that $\mathcal{S}_8 \cong \mathcal{H}_{64}/G$. The order of $\mathrm{PGU}(3,64)$ is equal to $2^{18} \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 13^2 \cdot 37 \cdot 109$. From the Riemann-Hurwitz formula,

$$44 < \frac{|\mathcal{H}_{64}(\mathbb{F}_{8^4})|}{|\mathcal{S}_8(\mathbb{F}_{8^4})|} \leq |G| \leq \frac{2g(\mathcal{H}_{64})-2}{2g(\mathcal{S}_8)-2} \leq 155.$$

Since $|G|$ divides $|\mathrm{PGU}(3,64)|$,

$$|G| \in \{45,48,50,52,56,60,63,64,65,70,72,74,75,78,80,84,90,91,96,$$

$$100,104,105,109,111,112,117,120,126,128,130,140,144,148,150\}.$$

The different divisor has degree

$$\Delta = (2g(\mathcal{H}_{64})-2) - |G|(2g(\mathcal{S}_8)-2) = 4030 - 26\cdot|G|. \tag{2.24}$$

**Case $|G|=45$.** By Sylow's Third Theorem [100, Theorem 6.10] and Schur-Zassenhaus Theorem [100, Theorem 9.19], $G$ is the direct product $G = S_3 \times C_5$. Then $G$ has 4 elements of order 5 and 40 elements of odd order multiple of 3. By Theorem 2.3.9, $\Delta \leq 4\cdot 65 + 40\cdot 2$, a contradiction (2.24).

**Case $|G|=48$.** Any group of order 48 has a normal subgroup of order 8 or 16 (see [104, p. 154 Ex. 10]); hence $G$ has a normal 2-subgroup $N$. By [67, Theorem 11.74], $N$ has a unique fixed point $P$ on $\mathcal{H}_{64}$, which is $\mathbb{F}_{64^2}$-rational. By Lemma 2.3.5, $G$ fixes $P$. From Theorem 2.3.11,

$$14 = \frac{(64-2^w)(64-(\gcd(3,65)-1)2^v)}{2\cdot 48},$$

with $v+w=4$. By direct computation, this is not possible.

**Case $|G|=50$.** By Sylow's Third Theorem and Schur-Zassenhaus Theorem, $G$ is a semidirect product $G = S_5 \rtimes C_2$. By Theorem 2.3.9, $\Delta = i\cdot 65 + (24-i)\cdot 0 + n_2\cdot 66 + (25-n_2)\cdot 1$ with $0\leq i\leq 24$ and $n_2\in\{1,5,25\}$. This contradicts (2.24).

**Case $|G|=52$.** By Sylow's Third Theorem, $n_{13}=1$, a contradiction to Lemma 2.3.8.

**Case $|G|=56$.** By Sylow's Third Theorem, $n_2=1$ or $n_7=1$. Suppose that $n_2=1$, so that $G=S_2\rtimes C_7$. Then $S_2$ fixes an $\mathbb{F}_{64^2}$-rational point $P\in\mathcal{H}_{64}$, and $G$ fixes $P$ by Lemma 2.3.5. By Theorem 2.3.11,

$$14 = \frac{(64-2^w)(64-(\gcd(7,65)-1)2^v)}{2\cdot 56},$$

with $v+w=2$; this is impossible. The case $n_7=1$ is impossible by Lemma 2.3.8.

**Case $|G|=60$.** By [100, Problem 6.16], either $n_5=1$ or $G$ is isomorphic to the alternating group $A_5$. The case $n_5=1$ is impossible by Lemma 2.3.8; hence $G\cong A_5$. By Theorem 2.3.9, $\Delta = 15\cdot 66 + 20\cdot 2 + i\cdot 65 + (24-i)\cdot 0$, with $0\leq i\leq 24$. This contradicts (2.24).

**Case $|G|=63$.** By Theorem 2.3.9, $\Delta = 62\cdot 2$, a contradiction to (2.24).

**Case $|G|=64$.** By Theorem 2.3.10, $14 = 2^{6-v-1}(2^{6-w}-1)$ with $0\leq v,w\leq 5$. Hence, $v=4$ and $w=3$. Then, by Theorem 2.3.10 and Lemma 2.3.4, $G$ has

7 elements of type (C) and 56 elements of type (D). By Theorem 2.3.9, $\Delta = 7 \cdot 66 + 56 \cdot 2$. This contradicts (2.24).

**Case $|G| = 65$.** By Lemma 2.3.4, any nontrivial element $\sigma \in G$ is either of type (A) or of type (B1). If a generator of the cyclic group $G$ is of type (A), then any element is of type (A) and $\Delta = 64 \cdot 65$ by Theorem 2.3.9, contradicting (2.24). If the 48 generators of $G$ are of type (B1), then $\Delta \leq 16 \cdot 65$ by Theorem 2.3.9. This contradicts (2.24).

**Case $|G| = 70$.** By Sylow's Third Theorem, $n_5 = n_7 = 1$ and $n_2 \in \{1, 5, 7, 35\}$; hence, $G = C_{35} \rtimes C_2$. By Theorem 2.3.9, $\Delta = n_2 \cdot 66 + (35 - n_2) \cdot 1 + 30 \cdot 2 + i \cdot 65 + (4 - i) \cdot 0$ with $0 \leq i \leq 4$. This contradicts (2.24).

**Case $|G| = 72$.** By [91, Theorem 1], $G$ has a characteristic 3-subgroup $N$. By Lemma 2.3.7, the elements of $N$ are of type (B2) with a common fixed triangle $T$. By Lemma 2.3.5, $G$ acts on $T$. By the orbit-stabilizer theorem, $G$ contains a 2-element fixing $T$ pointwise, contradicting Lemma 2.3.4.

**Case $|G| = 74$.** For any prime power $q$, $\mathrm{PSU}(3, q)$ has index $\gcd(3, q + 1)$ in $\mathrm{PGU}(3, q)$. This implies that, for any maximal subgroup $M \neq \mathrm{PSU}(3, q)$ of $\mathrm{PGU}(3, q)$, $|M|$ divides three times the order of a maximal subgroup of $\mathrm{PSU}(3, q)$. By Theorem 1.2.6, 74 does not divide three times the order of any maximal subgroup of $\mathrm{PSU}(3, 64)$, a contradiction.

**Case $|G| = 75$.** By Sylow and Schur-Zassenhaus theorems, $G$ is a semidirect product $G = S_5 \rtimes C_3$. By Theorem 2.3.9, $\Delta = i \cdot 65 + (24 - i) \cdot 0 + j \cdot 2 + (50 - j) \cdot 3$ with $0 \leq i \leq 24$ and $0 \leq j \leq 50$. This contradict (2.24).

**Case $|G| = 78$.** By Sylow's Third Theorem, $n_{13} = 1$; by Lemma 2.3.5, $G$ acts on the fixed points of $S_{13}$. Every nontrivial element $\sigma \in S_{13}$ generates $S_{13}$ and is either of type (A) or (B1). Hence, all nontrivial elements of $G$ either are of type (A), or act on a common triangle $T$. In the former case, $G$ contains a 2-element of type (A), contradicting Lemma 2.3.4. In the latter case, by the orbit-stabilizer theorem, the subgroup $H$ of $G$ fixing $T$ pointwise contains a 2-element or a 3-element. This contradicts Lemma 2.3.4.

**Case $|G| = 80$.** By [91, Theorem 1], $G$ has a characteristic 2-subgroup $N$. By Lemma 2.3.5, $G$ fixes the unique fixed point of $N$ on $\mathcal{H}_{64}$, which is $\mathbb{F}_{64^2}$-rational. By Theorem 2.3.11,

$$14 = \frac{(64 - 2^w)(64 - (\gcd(5, 65) - 1)2^v)}{2 \cdot 80}$$

with $v + w = 4$, which is impossible.

**Case $|G| = 84$.** By Sylow's theorems, $n_7 = 1$, a contradiction to Lemma 2.3.8.

**Case $|G| = 90$.** Since $|G| \equiv 2 \pmod 4$, $G$ has a normal subgroup $N$ of index 2 (see [96, Ex. 4.3]). By Sylow's Third Theorem, $N$ has a characteristic 5-subgroup $C_5$, so that $C_5$ is normal in $G$ and $n_5 = 1$. Also, $n_3 = 1$. Then $G$ is a semidirect product $G = C_5 \times S_3 \rtimes C_2$. By Theorem 2.3.9, $\Delta = 4 \cdot i + 40 \cdot 2 + n_2 \cdot 66 + (45 - n_2) \cdot 1$, with $i \in \{0, 65\}$ and $1 < n_2 \mid 45$. This contradicts (2.24).

**Case** $|G| = 91$. By Theorem 2.3.9, $\Delta = 78 \cdot 2 + 12 \cdot i$ with $i \in \{0, 65\}$, contradicting (2.24).

**Case** $|G| = 96$. By [91, Theorem 1], $G$ has a characteristic 2-subgroup $N$. By Lemma 2.3.5, $G$ fixes the unique fixed point of $N$ on $\mathcal{H}_{64}$, which is $\mathbb{F}_{64^2}$-rational. By Theorem 2.3.11,

$$14 = \frac{(64 - 2^w)(64 - (\gcd(3, 65) - 1)2^v)}{2 \cdot 91}$$

with $v + w = 5$, which is impossible.

**Case** $|G| = 100$. By Sylow's Third Theorem, $n_5 = 1$. By Lemma 2.3.6, the fixed points of $S_5$ are the vertices of a triangle $T$. By Lemma 2.3.5, $G$ acts on $T$. By the orbit-stabilizer theorem, $G$ contains a 2-element fixing $T$ pointwise. This contradicts Lemma 2.3.4.

**Case** $|G| = 104$. By Sylow's theorems $n_{13} = 1$, contradicting Lemma 2.3.8.

**Case** $|G| = 105$. By Sylow's Third Theorem, $n_5 \in \{1, 21\}$. All elements of a $S_5$ are of the same type, either (A) or (B1). Then, by Theorem 2.3.9, $\Delta = 4i \cdot 65 + 4(n_5 - i) \cdot 0 + (104 - 4n_5) \cdot 2$, with $0 \leq i \leq n_5$. This contradicts (2.24).

**Case** $|G| = 109$. By Theorem 2.3.9, $\Delta = 108 \cdot 3$. This contradicts (2.24).

**Case** $|G| = 111$. By Sylow and Schur-Zassenhaus theorems, $n_{37} = 1$, $n_3 \in \{1, 37\}$, and $G$ is a semidirect product $G = C_{37} \rtimes C_3$. By Lemma 2.3.4, $G$ has no elements of order $37 \cdot 3$. Hence, $n_3 = 37$. By Theorem 2.3.9, $\Delta = 36 \cdot 3 + 74 \cdot 2$. This contradicts (2.24).

**Case** $|G| = 112$. By [91, Theorem 1], $G$ has a characteristic 2-subgroup $N$. By Lemma 2.3.5, $G$ fixes the unique fixed point of $N$ on $\mathcal{H}_{64}$, which is $\mathbb{F}_{64^2}$-rational. By Theorem 2.3.11,

$$14 = \frac{(64 - 2^w)(64 - (\gcd(7, 65) - 1)2^v)}{2 \cdot 112}$$

with $v + w = 4$, which is a contradiction.

**Case** $|G| = 117$. By Sylow and Schur-Zassenhaus theorems, $G$ is a semidirect product $G = C_{13} \rtimes S_3$. Since 13 is prime, the nontrivial elements of $C_{13}$ are of the same type (A) or (B1). By Theorem 2.3.9, $\Delta = 12 \cdot i + 104 \cdot 2$ with $i \in \{0, 65\}$. Then $i = 65$ by (2.24), i.e. the nontrivial elements of $C_{13}$ are homologies, with a common center $P \notin \mathcal{H}_{64}$ and axis $\ell$. By Lemma 2.3.5, $G$ fixes $P$ and acts on $\ell$. By Lemma 2.3.4, the nontrivial elements of $S_3$ are of type (B2) and fix two $\mathbb{F}_{64^2}$-rational points $Q, R \in \ell \cap \mathcal{H}_{64}$. Let $\mathcal{H}_{64}$ have Norm-Trace equation (1.4). Since $\mathrm{PGU}(3, q)$ is 2-transitive on the $\mathbb{F}_{64^2}$-rational points of $\mathcal{H}_{64}$, we can assume that $Q = (1 : 0 : 0)$ and $R = (0 : 0 : 1)$. Then $C_{13} = \{\mathrm{diag}(1, \lambda, 1) \mid \lambda^{13} = 1\}$ and

$S_3 = \{\mathrm{diag}(a^{65}, a, 1) \mid a^9 = 1\} = C_9$; see [47]. Hence, $G$ is abelian and is the direct product $G = C_{13} \times C_9$. Let $\bar{G} \leq \mathrm{PGU}(3, 64)$ be the group $\bar{G} = C_{65} \times C_9$, where $C_{65}$ is generated by $\mathrm{diag}(1, \bar{\lambda}, 1)$, with $\bar{\lambda}$ a primitive 65-th root of unity. Then $G$ is a normal subgroup of $\bar{G}$ of index 5, so that $\bar{G}/G \leq \mathrm{Aut}(\mathcal{H}_{64}/G)$ has order 5. Also, $\bar{G}/G$ has two $\mathbb{F}_8$-rational fixed places on $\mathcal{H}_{64}/G$, namely the ones lying under $Q$ and $R$. This is inconsistent with the structure of the automorphism group of $\mathcal{S}_8$. In fact, by [67, Theorems 12.13 and A.12], any subgroup of $\mathrm{Aut}(\mathcal{S}_8)$ of order 5 is a Singer group acting semiregularly on the $\mathbb{F}_8$-rational places of $\mathcal{S}_8$.

**Case $|G| = 120$.** By [96, Ex. 8.19], either $n_5 = 1$, or $G$ has a normal 2-subgroup, or $G$ is isomorphic to the symmetric group $S_5$. The case $n_5 = 1$ is impossible by Lemma 2.3.8. Hence, $n_5 = 6$. Suppose that $G$ has a normal 2-subgroup $N$. By Lemma 2.3.5, $G$ fixes the unique fixed point of $N$ on $\mathcal{H}_{64}$. Then any 5-element of $G$ is of type (A) by Lemma 2.3.4. By Theorem 2.3.9, $\Delta \geq 24 \cdot 65$; this contradicts (2.24). Suppose that $G \cong S_5$. Then $G$ contains 25 involutions. By Theorem 2.3.9, $\Delta \geq 25 \cdot 66$. This contradicts (2.24).

**Case $|G| = 126$.** Since $|G| \equiv 2 \pmod 4$, $G$ has a normal subgroup $N$ of index 2. Then $G$ is a semidirect product $G = N \rtimes C_2$. By Theorem 2.3.9, $\Delta = 62 \cdot 2 + n_2 \cdot 66 + (63 - n_2) \cdot 1$. This contradicts (2.24).

**Case $|G| = 128$.** By Theorem 1.2.6, $G$ fixes an $\mathbb{F}_{64^2}$-rational point of $\mathcal{H}_{64}$. Then, by Theorem 2.3.10, $14 = 2^{6-v-1}(2^{6-w} - 1)$ with $0 \leq v, w \leq 5$. Hence, $v = 4$, $w = 3$. By theorem 2.3.10, $G$ contains exactly $2^3 - 1$ involutions. By Theorem 2.3.9, $\Delta = 7 \cdot 66 + 120 \cdot 1$. This contradicts (2.24).

**Case $|G| = 130$.** By Sylow's Third Theorem, $n_{13} = 1$, $n_5 \in \{1, 26\}$, and $n_2 \in \{1, 5, 13, 65\}$. By (2.24), $\Delta = 650$. Hence, by Theorem 2.3.9, the nontrivial elements of $S_{13}$ are of type (B1). We remark that if $x$ is an element of type (C) normalizing an element $y$ of type (A) or (B1), then the element $yx$ is of type (E). If $n_5 = 1$, then $G$ is a semidirect product $G = C_{65} \rtimes C_2$; hence, $n_2 = 1$ by the above remark. If $n_5 = 26$, then $G$ contains 12 elements of order 13, $4 \cdot 26$ elements of order 5, and 12 elements of type (E) by the above remark. Hence, $n_2 = 1$. Therefore $G$ contains a unique involution $\sigma$. By Lemma 2.3.5, $S_{13}$ fixes the unique fixed point of $\sigma$ on $\mathcal{H}_{64}$. This contradicts Lemma 2.3.4.

**Case $|G| = 140$.** By Sylow's theorems $n_7 = 1$, contradicting Lemma 2.3.8.

**Case $|G| = 144$.** By Theorem 2.3.9, $\Delta = i \cdot 66 + j \cdot 1 + k \cdot 2$ with $i + j + k = 143$. Here, $i$ is the number of involutions in $G$, $j$ is the number of elements of order 6 or 18 in $G$, and $k$ is the number of elements of order 3, 9, or 4 in $G$. Suppose $i = 1$. Then, by Lemma 2.3.5, $G$ fixes the unique fixed point of the involution on $\mathcal{H}_{64}$, which is $\mathbb{F}_{64^2}$-rational. By Theorem 2.3.11,

$$14 = \frac{(64 - 2^w)(64 - (\gcd(9, 65) - 1)2^v)}{2 \cdot 144}$$

with $v+w=4$, hence $w=0$. By Theorem 2.3.11, $G$ has no involutions, which is impossible. Then $i \geq 2$ and thus by (2.24), we have $i=2$ and $k=13$. This implies that $G$ contains 2 involutions and at most 13 elements of order 4. Hence, $G$ has a unique Sylow 2-subgroup $S_2$. Then, by Lemma 2.3.5, $G$ fixes the unique fixed point of $S_2$ on $\mathcal{H}_{64}$. As before, this yields a contradiction by Theorem 2.3.11.

**Case** $|G| = 148$**.** By Theorem 1.2.6, $|G|$ does not divide three times the order of any maximal subgroup of $\mathrm{PSU}(3,64)$. Hence, $G$ is not contained in any maximal subgroup of $\mathrm{PGU}(3,64)$, a contradiction.

**Case** $|G| = 150$**.** By Lemma 2.3.6, $G$ contains 8 elements of type (A). Hence, by Theorem 2.3.9, $\Delta \geq 8 \cdot 65$. This contradicts (2.24).

This completes the proof of Theorem 2.3.1.

It may be noticed in the above proof that the hypothesis $g=14$ together with the $\mathbb{F}_{64^2}$-maximality of $\mathcal{S}_8$ are sufficient to get a contradiction for $|G| \neq 117$. Instead, a group $G$ of order 117 with the required ramification exists, and we gave an explicit construction. Such a group $G$ is uniquely determined up to conjugation. Using MAGMA [16], we found a plane model of $\mathcal{H}_{64}/G$ over $\mathbb{F}_2$, as well as a nonsingular model of $\mathcal{H}_{64}/G$ in $\mathrm{PG}(13,2)$.

**Proposition 2.3.13.** *Let $\mathcal{X}$ be an $\mathbb{F}_{64^2}$-maximal curve of genus* 14. *If $\mathcal{X}$ is Galois covered by $\mathcal{H}_{64}$ then $\mathcal{X} \cong \mathcal{H}_{64}/G$ where $G$ is a cyclic group $G \leq \mathrm{PGU}(3,64)$ of order* 117*, and a plane model of $\mathcal{X}$ over $\mathbb{F}_2$ is the (singular) plane curve*

$$X^7Y^5 + X + Y^5 = 0,$$

*while a nonsingular model in $\mathbb{P}^{13}$ of $\mathcal{X}$ over $\mathbb{F}_2$ is the image of $\mathcal{X}$ under the morphism*

$$\varphi : \mathcal{X} \to \mathbb{P}^{13}, \quad (x,y,1) \mapsto (x,y,xy,x^2y,y^2,xy^2,x^2y^2,x^3y^2,y^3,xy^3,x^2y^3,x^3y^3,x^4y^3,1).$$

### 2.3.3 Proof of Theorem 2.3.2

By contradiction, let $\mathcal{R}_3 \cong \mathcal{H}_{27}/G$ for $G \leq \mathrm{PGU}(3,27)$. The order of $\mathrm{PGU}(3,27)$ is equal to $2^5 \cdot 3^9 \cdot 7^2 \cdot 13 \cdot 19 \cdot 37$. From the Riemann-Hurwitz formula,

$$12 < \frac{|\mathcal{H}_{27}(\mathbb{F}_{27^2})|}{|\mathcal{R}_3(\mathbb{F}_{27^2})|} \leq |G| \leq \frac{2g(\mathcal{H}_{27})-2}{2g(\mathcal{R}_3)-2} \leq 25.$$

Since $|G|$ divides $|\mathrm{PGU}(3,27)|$,

$$|G| \in \{13,14,16,18,19,21,24\}.$$

The different divisor has degree

$$\Delta = (2g(\mathcal{H}_{27})-2) - |G|(2g(\mathcal{R}_3)-2) = 700 - 28 \cdot |G|. \tag{2.25}$$

**Case** $|G| = 13$**.** By Theorem 2.3.9, $\Delta = 12 \cdot 2$. This contradicts (2.25).

**Case** $|G| = 14$**.** By Sylow and Schur-Zassenhaus theorems, $G$ is a semidirect product $G = C_7 \rtimes C_2$. All nontrivial elements of $C_7$ are of the same type, which is either (A) or (B1) by Lemma 2.3.4. Therefore, by Theorem 2.3.9, $\Delta = 6 \cdot i + 7 \cdot 28$, with $i \in \{0, 28\}$. This contradicts (2.25).

**Case** $|G| = 16$**.** PGU(3, 27) has just three conjugacy classes of subgroups of order 16, which are isomorphic either to the Iwasawa group $M_{16} = \langle x, y \mid x^8 = y^2 = 1, yxy^{-1} = x^5 \rangle$, or to the direct product $C_4 \times C_4$, or to the central product $D_8 \circ C_4 = \langle \alpha, \beta, \gamma \mid \alpha^4 = \beta^2 = 1, \beta\alpha\beta^{-1} = \alpha^{-1}, \alpha^2 = \gamma^2, \alpha\gamma = \gamma\alpha, \beta\gamma = \gamma\beta \rangle$.

Suppose $G \cong M_{16}$. By MAGMA computation, the normalizer $N$ of $G$ in PGU(3, 27) has order 224, and the quotient group $N/G \leq \mathrm{Aut}(\mathcal{H}_{27}/G)$ is a cyclic group of order 14. On the other hand, the subgroups of $R(3) \cong \mathrm{P\Gamma L}(2, 8)$ of order 14 are not abelian, a contradiction.

Suppose $G \cong C_4 \times C_4$. By MAGMA computation, the normalizer $N$ of $G$ in PGU(3, 27) has order 4704. Hence, the group $N/G \leq \mathrm{Aut}(\mathcal{H}_{27}/G)$ has order 294, which does not divide the order of $R(3)$. This contradicts $\mathcal{H}_{27}/G \cong \mathcal{R}_3$.

Suppose $G \cong D_8 \circ C_4$. By MAGMA computation, the normalizer $N$ of $G$ in PGU(3, 27) has order 672, and the group $N/G \leq \mathrm{Aut}(\mathcal{H}_{27}/G)$ is isomorphic to $C_{21} \rtimes C_2$. On the other hand, the subgroups of $R(3)$ of order 42 have no cyclic subgroups of order 21, a contradiction.

**Case** $|G| = 18$**.** By Sylow's Third Theorem, $n_3 = 1$. By [67, Theorem 11.74], $S_3$ has a unique fixed point $P$ on $\mathcal{H}_{27}$, which is $\mathbb{F}_{27^2}$-rational. By Lemma 2.3.5, $G$ fixes $P$. Then, by Theorem 2.3.11,

$$15 = \frac{(27 - 3^w)(27 - (\gcd(2, 28) - 1)3^v)}{2 \cdot 18}$$

with $v + w = 2$, which is impossible.

**Case** $|G| = 19$**.** By Theorem 2.3.9, $\Delta = 18 \cdot 3$. This contradicts (2.25).

**Case** $|G| = 21$**.** By Sylow and Schur-Zassenhaus theorems, $G$ is a semidirect product $G = C_7 \rtimes C_3$. All nontrivial elements of $C_7$ are of the same type, which is either (A) or (B1) by Lemma 2.3.4. Thus, by Theorem 2.3.9, $\Delta = 6 \cdot i + 2n_3 \cdot 29 + (14 - 2n_3) \cdot 1$, with $i \in \{0, 28\}$. This contradicts (2.25).

**Case** $|G| = 24$**.** Since 3 divides $|G|$, we have $\Delta \geq 29$ by Theorem 2.3.9. This contradicts (2.25).

This completes the proof of Theorem 2.3.2.

It may be noticed in the above proof that the hypothesis $g = 15$ together with the $\mathbb{F}_{27^2}$-maximality of $\mathcal{R}_3$ rule out all cases but $|G| = 16$. For this exception, three cases are treated separately.

- $G \cong M_{16}$. Then $G$ has 3 involutions, 4 elements of order 4, and 8 elements of order 8. By Theorem 2.3.9, the quotient curve $\mathcal{H}_{27}/G$ has genus 18.

- $G \cong C_4 \times C_4$. By the Riemann-Hurwitz formula, $\mathcal{H}_{27}/G$ has genus 15. Also, $G$ has 9 elements of type (A) and 6 elements of type (B1). Hence, $G$ fixes the vertices of a triangle $T$. Let $\mathcal{H}_{27}$ have equation (1.3). Up to conjugation, $T$ is the fundamental triangle and $G = \{\mathrm{diag}(\lambda, \mu, 1) \mid \lambda^4 = \mu^4 = 1\}$. Therefore a (singular) plane model of $\mathcal{H}_{27}/G$ is $X^7 + Y^7 + 1 = 0$.

- $G \cong D_8 \circ C_4$. By the Riemann-Hurwitz formula, $\mathcal{H}_{27}/G$ has genus 15. Also, $G$ contains 9 elements of type (A) and 6 elements of type (B1). In particular, the non-central involutions of $D_8$ are non-commuting elements of type (A). Thus, the generator $y$ of the center $C_4$ is not of type (B1). Hence, $y$ is of type (A). Let $\mathcal{H}_{27}$ have Fermat equation (1.3). Up to conjugation, the generators of $G$ are $\alpha : (X, Y, T) \mapsto (Y, -X, T)$, $\beta = \mathrm{diag}(1, -1, 1)$, and $\gamma = \mathrm{diag}(\lambda, \lambda, 1)$, where $\lambda^2 = -1$. A plane model of $\mathcal{H}_{27}/G$ is obtained by MAGMA computation, as follows.

**Proposition 2.3.14.** *Let $\mathcal{X}$ be an $\mathbb{F}_{27^2}$-maximal curve of genus 15. If $\mathcal{X}$ is Galois covered by $\mathcal{H}_{27}$ then $\mathcal{X} \cong \mathcal{H}_{27}/G$ where $G \leq \mathrm{PGU}(3, 27)$ has order 16, and one of the following cases occurs.*

- *$G \cong C_4 \times C_4$ and a plane model for $\mathcal{X}$ is given by the affine equation*

$$X^7 + Y^7 + 1 = 0\,.$$

- *$G \cong D_8 \circ C_4$ and a plane model for $\mathcal{X}$ is given by the affine equation*

$$X^{28}+X^{27}+X^{26}+2X^{23}+2X^{22}+X^{21}+2X^{12}Y^{14}+X^{10}Y^{14}+2X^7Y^{14}+Y^{28} = 0.$$

### 2.3.4 Galois subcovers of $\mathcal{H}_{27}$

Theorem 2.3.15 shows the complete spectrum of genera of Galois subcovers of $\mathcal{H}_{27}$, consisting of integers $g$ which are the genera of a quotient curve $\mathcal{H}_{27}/G$ with $G$ ranging on the set of all subgroups of $PGU(3, 27)$.

**Theorem 2.3.15.** *The spectrum of genera of Galois subcovers of $\mathcal{H}_{27}$ is*

$$\Sigma_{27} = \{0, 1, 3, 4, 5, 6, 7, 9, 10, 12, 13, 15, 16, 17, 18, 19, 24, 25,$$
$$26, 27, 36, 39, 43, 51, 52, 78, 85, 108, 117, 169, 351\}.$$

The proof relies on the results of Section 2.3.1. A case-by-case analysis of all integers $g$ with $1 < g \leq g(\mathcal{H}_{27})$ is combined with

$$\frac{19684}{730 + 54g} = \frac{|\mathcal{H}_{27}(\mathbb{F}_{27^2})|}{|\mathcal{H}_{27}/G(\mathbb{F}_{27^2})|} \leq |G| \leq \frac{2g(\mathcal{H}_{27}) - 2}{2g(\mathcal{H}_{27}/G) - 2} = \frac{700}{2g - 2}\,, \tag{2.26}$$

which bounds the order of a putative group $G \leq \mathrm{PGU}(3,27)$ such that $\mathcal{H}_{27}/G$ has genus $g$. This leads us to look inside the structure of the groups $G$ satisfying (2.26) and compute the genus of $\mathcal{H}_{27}/G$, for $g > 1$. These results are summarized in Theorem 2.3.15. For each $g > 1$ in $\Sigma_{27}$, Tables 2.2 and 2.3 provide a classification of the groups $G$ for which $\mathcal{H}_{27}/G$ has genus $g$.

Table 2.2: Quotient curves $\mathcal{H}_{27}/G$ of genus $g \geq 17$

| $g$ | $\|G\|$ | structure of $G$ |
|---|---|---|
| 351 | 1 | trivial group. |
| 169 | 2 | $G = C_2 = \langle\sigma\rangle$, $\sigma$ of type (A). |
| 117 | 3 | $G = C_3 = \langle\sigma\rangle$, $\sigma$ of type (D). |
| 108 | 3 | $G = C_3 = \langle\sigma\rangle$, $\sigma$ of type (C). |
| 85 | 4 | $G = C_4 = \langle\sigma\rangle$, $\sigma$ of type (B1). |
| 78 | 4 | $G = C_4 = \langle\sigma\rangle$, $\sigma$ of type (A). |
| 52 | 6 | $G = C_6 = \langle\sigma\rangle$, $\sigma$ of type (E). |
| | | $G = Sym(3) = \langle\alpha\rangle \rtimes \langle\beta\rangle$, $\alpha$ of type (C), $\beta$ of type (A). |
| 51 | 7 | $G = C_7 = \langle\sigma\rangle$, $\sigma$ of type (B1). |
| 43 | 8 | $G = Q_8$ quaternion group, 1 element of type (A), 6 elements of type (B1). |
| 39 | 7 | $G = C_7 = \langle\sigma\rangle$, $\sigma$ of type (A). |
| | 8 | $G = C_8 = \langle\sigma\rangle$, $\sigma$ of type (B2). |
| | 9 | $G = C_3 \times C_3 = \langle\alpha\rangle \times \langle\beta\rangle$, $\alpha$ and $\beta$ of type (D). |
| 36 | 8 | $G = C_4 \times C_2 = \langle\alpha\rangle \times \langle\beta\rangle$, $\alpha$ of type (B1), $\beta$ of type (A). |
| | 8 | $G = D_8$ dihedral group, involutions of type (A), 2 elements of type (B1). |
| | 9 | $G = C_3 \times C_3 = \langle\alpha\rangle \times \langle\beta\rangle$, $\alpha$ of type (C), $\beta$ of type (D). |
| 27 | 9 | $G = C_3 \times C_3 = \langle\alpha\rangle \times \langle\beta\rangle$, $\alpha$ and $\beta$ of type (C). |
| | 13 | $G = C_{13} = \langle\sigma\rangle$, $\sigma$ of type (B2). |
| 26 | 12 | $G = Alt(4)$, involutions of type (A), other elements of type (D). |
| 25 | 14 | $G = C_{14} = \langle\sigma\rangle$, $\sigma$ of type (B1). |
| 24 | 12 | $G = C_{12} = \langle\sigma\rangle$, $\sigma$ of type (E). |
| 19 | 14 | $G = C_{14} = \langle\sigma\rangle$, $\sigma$ of type (B1), $\sigma^2$ of type (A). |
| 18 | 16 | $G = M_{16}$, 5 elements of type (A), 2 elements of type (B1), 8 elements of type (B2). |
| 18 | 19 | $G = C_{19} = \langle\sigma\rangle$, $\sigma$ of type (B3). |
| 17 | 21 | $G = C_7 \rtimes C_3 = \langle\alpha\rangle \rtimes \langle\beta\rangle$, $\alpha$ of type (B1), $\beta$ of type (B2). |

Table 2.3: Quotient curves $\mathcal{H}_{27}/G$ of genus $3 \leq g \leq 16$

| $g$ | $\lvert G\rvert$ | structure of $G$ |
|---|---|---|
| 16 | 18 | $G = C_3 \times (C_3 \rtimes C_2) = \langle\alpha\rangle \times (\langle\beta\rangle \rtimes \langle\gamma\rangle)$,<br>$\alpha$ of type (C), $\beta$ of type (D), $\gamma$ of type (A). |
| 15 | 16 | $G = C_4 \times C_4 = \langle\alpha\rangle \times \langle\beta\rangle$, $\alpha$ and $\beta$ of type (A). |
|  | 16 | $G = D_8 \circ C_4 = (\langle\alpha\rangle \rtimes \langle\beta\rangle) \circ \langle\gamma\rangle$, $\alpha$ of type (B1), $\beta$ and $\gamma$ of type (A). |
| 13 | 14 | $G = C_{14} = \langle\sigma\rangle$, $\sigma$ of type (A). |
|  | 18 | $G = C_3 \times (C_3 \rtimes C_2) = \langle\alpha\rangle \times (\langle\beta\rangle \rtimes \langle\gamma\rangle)$, $\alpha$ and $\beta$ of type (D), $\gamma$ of type (A). |
|  | 18 | $G = C_3 \times (C_3 \rtimes C_2) = \langle\alpha\rangle \times (\langle\beta\rangle \rtimes \langle\gamma\rangle)$, $\alpha$ and $\beta$ of type (C), $\gamma$ of type (A). |
|  | 26 | $G = C_{26} = \langle\sigma\rangle$, $\sigma$ of type (E). |
|  | 27 | $G = (C_3 \times C_3) \rtimes C_3 = (\langle\alpha\rangle \times \langle\beta\rangle) \rtimes \langle\gamma\rangle$, $\alpha$, $\beta$, $\gamma$ of type (D). |
|  | 28 | $G = C_{28} = \langle\sigma\rangle$, $\sigma$ of type (B1), 1 element of type (A). |
| 12 | 21 | $G = C_{21} = \langle\sigma\rangle$, $\sigma$ of type (E). |
|  | 24 | $G = C_3 \rtimes C_8 = \langle\alpha\rangle \rtimes \langle\beta\rangle$, $\alpha$ of type (C), $\beta$ of type (B2). |
|  | 27 | $G = C_3 \times (C_3 \times C_3) = \langle\alpha\rangle \times (\langle\beta\rangle \times \langle\gamma\rangle)$, $\alpha$ of type (C), $\beta$ and $\gamma$ of type (D). |
|  | 28 | $G = C_{28} = \langle\sigma\rangle$, $\sigma$ of type (B1), 3 elements of type (A). |
|  | 28 | $G = C_{14} \times C_2 = \langle\alpha\rangle \times \langle\beta\rangle$, $\alpha$ of type (B1), $\beta$ of type (A), 3 elements of type (A). |
| 10 | 24 | $G \cong \mathrm{SL}(2,3)$, 1 element of type (A), 6 elements of type (B1),<br>8 elements of type (C), 8 elements of type (E). |
| 9 | 37 | $G = C_{37} = \langle\sigma\rangle$, $\sigma$ of type (B3). |
| 7 | 26 | $G = C_{13} \rtimes C_2 = \langle\alpha\rangle \rtimes \langle\beta\rangle$, $\alpha$ of type (B2), $\beta$ of type (A). |
|  | 28 | $G = C_{28} = \langle\sigma\rangle$, $\sigma$ of type (B1), 14 elements of type (A). |
|  | 52 | $G = C_{13} \rtimes C_4 = \langle\alpha\rangle \rtimes \langle\beta\rangle$, $\alpha$ of type (B2), $\beta$ of type (B1). |
| 6 | 28 | $G = C_{14} \times C_2 = \langle\alpha\rangle \times \langle\beta\rangle$, $\alpha$ and $\beta$ of type (A), 15 elements of type (A). |
|  | 32 | $G = C_4 \wr C_2 = \langle\alpha\rangle \wr \langle\beta\rangle$ wreath product,<br>13 elements of type (A), 10 elements of type (B1), 8 elements of type (B2). |
|  | 52 | $G = C_{52} = \langle\sigma\rangle$, $\sigma$ of type (B2), 3 elements of type (A). |
|  | 57 | $G = C_{19} \rtimes C_3 = \langle\alpha\rangle \rtimes \langle\beta\rangle$, $\alpha$ of type (B3), $\beta$ of type (D). |
| 5 | 48 | $G = (C_4 \times C_4) \rtimes C_3 = (\langle\alpha\rangle \times \langle\beta\rangle) \rtimes \langle\gamma\rangle$, $\alpha$ and $\beta$ of type (A), $\gamma$ of type (D). |
| 4 | 42 | $G = C_{42} = \langle\sigma\rangle$, $\sigma$ of type (E). |
|  | 48 | $G = (D_8 \circ C_4) \rtimes \langle\sigma\rangle$, $\sigma$ of type (C). |
|  | 54 | $G = (C_3 \times C_3 \rtimes C_3) \rtimes \langle\sigma\rangle$, $\sigma$ of type (A). |
|  | 56 | $G = Q_8 \times \langle\sigma\rangle$, $\sigma$ of type (A). |
|  | 72 | $G = C_4 \times C_2 \rtimes (\langle\alpha\rangle \times \langle\beta\rangle)$, $\alpha$ and $\beta$ of type (D). |
|  | 81 | $G = C_3 \times C_3 \times C_3 \times C_3 = \langle\alpha\rangle \times \langle\beta\rangle \times \langle\gamma\rangle \times \langle\delta\rangle$, $\alpha$ of type (C), $\beta, \gamma, \delta$ of type (D). |
| 3 | 49 | $G = C_7 \times C_7 = \langle\alpha\rangle \times \langle\beta\rangle$, $\alpha$ and $\beta$ of type (A). |
|  | 56 | $G = \langle\sigma\rangle \rtimes D_8$, $\sigma$ of type (A). |
|  | 63 | $G = C_7 \times C_3 \times C_3 = \langle\alpha\rangle \times \langle\beta\rangle \times \langle\gamma\rangle$, $\alpha$ of type (A), $\beta$ and $\gamma$ of type (C). |
|  | 72 | $G = C_3 \times C_3 \rtimes C_8 = \langle\alpha\rangle \times \langle\beta\rangle \rtimes \langle\gamma\rangle$, $\alpha$ and $\beta$ of type (C), $\gamma$ of type (B2). |
|  | 81 | $G = C_3 \times C_3 \times C_3 \times C_3 = \langle\alpha\rangle \times \langle\beta\rangle \times \langle\gamma\rangle \times \langle\delta\rangle$, $\alpha, \beta$ of type (C), $\gamma, \delta$ of type (D). |
|  | 91 | $G = C_{91} = \langle\sigma\rangle$, $\sigma$ of type (B2). |
|  | 104 | $G = C_{13} \rtimes C_8 = \langle\alpha\rangle \rtimes \langle\beta\rangle$, $\alpha$ and $\beta$ of type (B2), or $G = C_{104} = \langle\sigma\rangle$, $\sigma$ of type (B2). |
|  | 111 | $G = C_{37} \rtimes C_3 = \langle\alpha\rangle \rtimes \langle\beta\rangle$, $\alpha$ of type (B3), $\beta$ of type (D). |
|  | 112 | $G = C_7 \times C_4 \times C_4 = \langle\alpha\rangle \times \langle\beta\rangle \times \langle\gamma\rangle$, $\alpha$ of type (B1), $\beta$ and $\gamma$ of type (A). |

Theorem 2.3.15 shows that some quotient curves of $\mathcal{R}_3$ happen not be Galois subcovers of $\mathcal{H}_{27}$. A partial list of them is given in the following proposition.

**Corollary 2.3.16.** *The quotient curves $\mathcal{R}_3/G_1$, $\mathcal{R}_3/G_2$, and $\mathcal{R}_3/G_3$ are not Galois subcovers of $\mathcal{H}_{27}$ for the groups $G_1, G_2, G_3$ defined as follows.*

- *The maximal subgroups $G_1 \leq R(3)$ of order 24 centralizing an involution $\sigma \in R(3)$, which are isomorphic to $\langle\sigma\rangle \times A_4$.*
- *The groups $G_2 \leq R(3)$ of order 6 which are isomorphic to $S_3$.*
- *The cyclic groups $G_3 \leq R(3)$ of order 6.*

*Proof.* From previous work of Çakçak and Özbudak, each of the quotient curves $\mathcal{R}_3/G_1$, $\mathcal{R}_3/G_2$, and $\mathcal{R}_3/G_3$ has genus 2; see [18, Sec. 4.1.1, p. 150] for $\mathcal{R}_3/G_1$, [18, Sec. 4.2, pp. 163-164] for $\mathcal{R}_3/G_2$, and [18, Sec. 4.4, pp. 171] for $\mathcal{R}_3/G_3$. On the other hand, Theorem 2.3.15 shows that no $\mathbb{F}_{27^2}$-maximal curve of genus 2 is a Galois subcover of $\mathcal{H}_{27}$. □

## 2.4 On certain Galois covers of the Suzuki and Ree curves

The results of this section are the object of [55]. Notation and results of Section 1.2 are used. We consider two families of maximal curves $\tilde{\mathcal{S}}_q$ and $\tilde{\mathcal{R}}_q$ which are cyclic covers of the Suzuki curve $\mathcal{S}_q$ and the Ree curve $\mathcal{R}_q$, respectively. The curves $\tilde{\mathcal{S}}_q$ and $\tilde{\mathcal{R}}_q$ are analogous to the GK cover $\mathcal{GK}_q$ of the Hermitian curve $\mathcal{H}_q$, and have been constructed by Skabelund in [105], as follows.

Let $q_0 = 2^s$ with $s \geq 1$ and $q = 2q_0^2 = 2^{2s+1}$. The curve

$$\tilde{\mathcal{S}}_q : \begin{cases} W^m = X^q + X \\ Y^q + Y = X^{q_0}(X^q + X) \end{cases},$$

where $m = q - 2q_0 + 1$, is $\mathbb{F}_{q^4}$-maximal ([105, Theorem 3.1]). Clearly, $\tilde{\mathcal{S}}_q$ is a Galois cover of the Suzuki curve $\mathcal{S}_q$ with equation (1.6).

Now let $q_0 = 3^s$ with $s \geq 1$ and $q = 3q_0^2 = 3^{2s+1}$. The curve

$$\tilde{\mathcal{R}}_q : \begin{cases} W^m = X^q - X \\ Z^q - Z = X^{2q_0}(X^q - X) \\ Y^q - Y = X^{q_0}(X^q - X) \end{cases},$$

where $m = q - 3q_0 + 1$, is $\mathbb{F}_{q^6}$-maximal ([105, Theorem 4.1]). Clearly, $\tilde{\mathcal{R}}_q$ is a Galois cover of the Ree curve $\mathcal{R}_q$ with equation (1.7).

In [105, Lemmas 3.3 and 4.2] the automorphism groups $S(q)$ and $R(q)$ of the curves $\mathcal{S}_q$ and $\mathcal{R}_q$ were lifted to subgroups of the full automorphism groups $\mathrm{Aut}(\tilde{S}_q)$ and $\mathrm{Aut}(\tilde{R}_q)$ of the covers $\tilde{\mathcal{S}}_q$ and $\tilde{\mathcal{R}}_q$, respectively. We show that the lifted groups actually coincide with the full automorphism groups of the curves $\tilde{\mathcal{S}}_q$ and $\tilde{\mathcal{R}}_q$. More specifically, we prove the following theorems.

**Theorem 2.4.1.** *The automorphism group of $\tilde{\mathcal{S}}_q$ is a direct product $\tilde{S}(q) \times C_m$, where $\tilde{S}(q)$ is isomorphic to $S(q) = \mathrm{Aut}(\mathcal{S}_q)$ and $C_m$ is a cyclic group of order $m = q - 2q_0 + 1$.*

**Theorem 2.4.2.** *The automorphism group of $\tilde{\mathcal{R}}_q$ is a direct product $\tilde{R}(q) \times C_m$, where $\tilde{R}(q)$ is isomorphic to $R(q) = \mathrm{Aut}(\mathcal{R}_q)$ and $C_m$ is a cyclic group of order $m = q - 3q_0 + 1$.*

In the proofs of Theorems 2.4.1 and 2.4.2 we will use results on curves having automorphism groups for which the classical Hurwitz bound does not hold.

We also prove the following results, which provide new families of maximal curves which are Galois covered by the Hermitian curve.

**Theorem 2.4.3.** *For any $q$, $\tilde{\mathcal{S}}_q$ is not Galois covered by $\mathcal{H}_{q^2}$.*

**Theorem 2.4.4.** *For any $q$, $\tilde{\mathcal{R}}_q$ is not Galois covered by $\mathcal{H}_{q^3}$.*

Sections 2.4.1 and 2.4.2 prove Theorems 2.4.1 and 2.4.2, respectively, while Section 2.4.3 proves Theorems 2.4.3 and 2.4.4.

### 2.4.1 The automorphism group of $\tilde{\mathcal{S}}_q$

Let $S(q)_\infty = \{\psi_{a,b,c} \mid a, b, c \in \mathbb{F}_q, a \neq 0\}$ and $\phi$ be the generators of $S(q)$, as described in Proposition 1.2.8. By [105, Section 3], the automorphism group of $\tilde{\mathcal{S}}_q$ admits the following subgroups:

- A cyclic group $C_m$ generated by the automorphism $\gamma_\lambda : (x, y, w) \mapsto (x, y, \lambda w)$, where $\lambda \in \mathbb{F}_{q^4}$ is a primitive $m$-th root of unity.
- A group $LS(q)$ lifted by $S(q)$ and generated by the automorphisms $\tilde{\psi}_{a,b,c}$ $(a, b, c \in \mathbb{F}_q,\ a \neq 0)$ together with an involution $\tilde{\phi}$. Here, $\tilde{\psi}_{a,b,c}(x, y) := \psi_{a,b,c}(x, y)$ and $\tilde{\psi}_{a,b,c}(w) := \delta w$, where $\delta^m = a$. Similarly, $\tilde{\phi}(x, y) := \phi(x, y)$, and $\tilde{\phi}(w) := w/\beta$.

**Lemma 2.4.5.** *The group $LS(q)$ contains a subgroup $\tilde{S}(q)$ isomorphic to $S(q)$.*

*Proof.* Let $\Delta := \{(\tilde{\psi}_{a,b,c})^m \mid a,b,c \in \mathbb{F}_q, a \neq 0\} \leq LS(q)$. By direct checking, the map $\psi_{a,b,c} \mapsto (\tilde{\psi}_{a,b,c})^m$ is an isomorphism between $S(q)_\infty$ and $\Delta$. Moreover, the action of $\Delta$ on the set $\mathcal{O}$ of $\mathbb{F}_q$-rational places of $\tilde{\mathcal{S}}_q$ is equivalent to the action of $S(q)_\infty$ on the non-tame short orbit of $S(q)$. Let $\tilde{S}(q)$ be the subgroup of $LS(q)$ generated by $\Delta$ and $\tilde{\phi}$. The action of $S(q)_\infty$ and $\phi$ on the non-tame short orbit of $S(q)$ is equivalent to the action of $\Delta$ and $\tilde{\phi}$ on $\mathcal{O}$, respectively. Hence, $\Delta$ coincides with the stabilizer in $\tilde{S}(q)$ of a point in $\mathcal{O}$. This implies that $\tilde{S}(q)$ acts 2-transitively on $\mathcal{O}$ and the stabilizer in $\tilde{S}(q)$ of two distinct places of $\mathcal{O}$ is cyclic. Since $|\mathcal{O}|$ is not a power of 2, $\tilde{S}(q)$ has no regular normal subgroups by [15, Theorem 1.7.6]. Therefore we apply [75, Theorem 1.1] to conclude that $\tilde{S}(q) \cong \mathrm{Aut}(\mathcal{S}_q)$. □

**Lemma 2.4.6.** *The normalizer of $C_m$ in $\mathrm{Aut}(\tilde{\mathcal{S}}_q)$ is the direct product $\tilde{S}(q) \times C_m$.*

*Proof.* It is easily checked that $\gamma_\lambda$ commutes with $(\tilde{\psi}_{a,b,c})^m$ and with $\tilde{\phi}$ on the rational functions $x$, $y$ and $w$. Therefore, $\tilde{S}(q) \times C_m$ is a subgroup of the normalizer $N$ of $C_m$ in $\mathrm{Aut}(\tilde{\mathcal{S}}_q)$; in particular, $N/C_m$ has a subgroup isomorphic to $S(q)$. Also, the quotient curve $\tilde{\mathcal{S}}_q/C_m$ is birationally equivalent to $\mathcal{S}_q$. Then $N/C_m$ is isomorphic to a subgroup of $S(q)$. Therefore $N/C_m \cong S(q)$, whence the thesis. □

**Corollary 2.4.7.** *The group $LS(q)$ coincides with the normalizer of $C_m$ in $\mathrm{Aut}(\tilde{\mathcal{S}}_q)$.*

*Proof.* The group $C_m$ is contained in $LS(q)$ as it is generated by $\tilde{\psi}_{1,0,0}$. Also, $C_m$ commutes with $LS(q)$. Hence, the claim follows from Lemma 2.4.6. □

Being $\tilde{\mathcal{S}}_q$ an $\mathbb{F}_{q^4}$-maximal curve, we can apply the results in [51] on zero 2-rank curves. By direct computations $|\mathrm{Aut}(\tilde{\mathcal{S}}_q)| \geq |LS(q)| \geq 72(g(\tilde{\mathcal{S}}_q)-1)$, thus by [51, Theorem 5.1] we conclude that $\mathrm{Aut}(\tilde{\mathcal{S}}_q)$ is non-solvable. By [51, Theorem 6.1], the commutator $\mathrm{Aut}(\tilde{\mathcal{S}}_q)'$ of $\mathrm{Aut}(\tilde{\mathcal{S}}_q)$ is one of the following groups:

$$\mathrm{PSL}(2,n),\ \mathrm{PSU}(3,n),\ \mathrm{SU}(3,n),\ S(n) \quad \text{with} \quad n = 2^r \geq 4.$$

Also, $\mathrm{Aut}(\tilde{\mathcal{S}}_q)'$ contains $G' = \tilde{S}(q)$.

**Lemma 2.4.8.** $\mathrm{Aut}(\tilde{\mathcal{S}}_q)' = \tilde{S}(q)$.

*Proof.* Since $\tilde{S}(q) \leq \mathrm{Aut}(\tilde{\mathcal{S}}_q)'$, we discard the cases $\mathrm{PSL}(2,2^r)$, $\mathrm{PSU}(3,2^r)$, $\mathrm{SU}(3,2^r)$:

i) $\tilde{S}(q)$ has elements of order 4, while $\mathrm{PSL}(2,2^r)$ has not by Theorem 1.2.7. Hence, $\mathrm{Aut}(\tilde{\mathcal{R}}_q)' \neq \mathrm{PSL}(2,2^r)$.

ii) By Theorem 1.2.9, $\tilde{S}(q)$ has subgroups of type $\Sigma \rtimes C_4$, where $\Sigma$ is generated by a tame element of order $q + 2q_0 + 1$. On the contrary, in $\mathrm{PSU}(3, 2^r)$ no non-tame element $\sigma$ of order 4 can normalize a tame element $\tau$; otherwise, $\sigma$ acts on the fixed points of $\tau$ and in particular $\sigma$ fixes a point $P$ and a line $\ell$ not through $P$, a contradiction to Lemma 2.3.4. Hence, $\tilde{G}' \neq \mathrm{PSU}(3, 2^r)$.

iii) If $\tilde{G}' = \mathrm{SU}(3, 2^r)$, then $\mathrm{SU}(3, 2^r)$ has a subgroup of type $\Sigma \rtimes C_4$, where $\Sigma$ is cyclic of order $q + 2q_0 + 1$. This implies that $\mathrm{PSU}(3, 2^r)$ has a subgroup of type $\bar{\Sigma} \rtimes C_4$, where $\bar{\Sigma}$ is cyclic of order $(q + 2q_0 + 1)/\gcd(3, 2^r + 1)$. This is impossible as shown at point ii). Hence, $\tilde{G}' \neq \mathrm{SU}(3, 2^r)$.

Therefore $\mathrm{Aut}(\tilde{\mathcal{S}}_q)' = \tilde{S}(2^r)$. If $2^r > q$, then $2^r \geq q^3$ and by direct computation $|\mathrm{Aut}(\tilde{\mathcal{S}}_q)'| > 8g(\tilde{\mathcal{S}}_q)^3$, a contradiction to [67, Theorem 11.116]. Hence, $\mathrm{Aut}(\tilde{\mathcal{S}}_q)' = \tilde{S}(q)$. □

Finally we prove Theorem 2.4.1. By Lemma 2.4.8 and [51, Theorem 6.2], we have that $\mathrm{Aut}(\tilde{\mathcal{S}}_q) \cong \tilde{S}(q) \times C$, where $C$ is a cyclic group of odd order. More specifically, $C$ is the subgroup of $\mathrm{Aut}(\tilde{\mathcal{S}}_q)$ fixing pointwise the set $\mathcal{O}$ of $\mathbb{F}_q$-rational places of $\tilde{\mathcal{S}}_q$. Then $C_m \subseteq C$, and hence $C = C_m$ by Corollary 2.4.7. Therefore, Theorem 2.4.1 is proved.

**Remark 2.4.9.** *Theorem* 2.4.1 *shows that* $\mathrm{Aut}(\tilde{\mathcal{S}}_q)$ *is exactly the lifting* $LS(q)$ *obtained as a cyclic extension of the automorphism group of the Suzuki curve* $\mathcal{S}_q$.

### 2.4.2 The automorphism group of $\tilde{\mathcal{R}}_q$

Let $R(q)_\infty = \{\psi_{a,b,c,d} \mid a, b, c, d \in \mathbb{F}_q, a \neq 0\}$ and $\phi$ be the generators of $R(q)$, as described in Proposition 1.2.10. By [105, Section 4], the automorphism group of $\tilde{\mathcal{R}}_q$ admits the following subgroups:

- A cyclic group $C_m$ generated by the automorphism $\gamma_\lambda : (x, y, w) \mapsto (x, y, \lambda w)$, where $\lambda \in \mathbb{F}_{q^6}$ is a primitive $m$-th root of unity.

- A group $LR(q)$ lifted by $R(q)$ and generated by the automorphisms $\tilde{\psi}_{a,b,c,d}$ ($a, b, c, d \in \mathbb{F}_q$, $a \neq 0$) together with an involution $\tilde{\phi}$. Here, $\tilde{\psi}_{a,b,c,d}(x, y, z) := \psi_{a,b,c,d}(x, y, z)$ and $\tilde{\psi}_{a,b,c,d}(w) := \delta w$, where $\delta^m = a$. Similarly, $\tilde{\phi}(x, y, z) := \phi(x, y, z)$, and $\tilde{\phi}(w) := w/w_8$.

We recall some results on large automorphism groups of curves that will be used in the proof of Theorem 2.4.2.

**Theorem 2.4.10.** ([67, Theorems 11.56 and 11.116]) *Let $\mathcal{X}$ be an irreducible curve of genus $g \geq 2$ such that $|Aut(\mathcal{X})| > 84(g-1)$. Then $Aut(\mathcal{X})$ has at most three short orbits, as follows:*

*i)* *exactly three short orbits, two tame and one non-tame, and* $|\mathrm{Aut}(\mathcal{X})| \leq 24g^2$*;*

*ii)* *exactly two short orbits, both non-tame, and* $|\mathrm{Aut}(\mathcal{X})| \leq 16g^2$*;*

*iii)* *only one short orbit which is non-tame, and* $|\mathrm{Aut}(\mathcal{X})| \leq g(2g-2)(4g+2)$ *(see* [67, page 515]*);*

*iv)* *exactly two short orbits, one tame and one non-tame. In this case* $|\mathrm{Aut}(\mathcal{X})| < 8g^3$*, with the following exceptions (see* [67, Theorem 11.126]*):*

- *$p = 2$ and $\mathcal{X}$ is isomorphic to the hyperelliptic curve $Y^2 + Y = X^{2^k+1}$ with genus $2^{k-1}$ ;*
- *$p > 2$ and $\mathcal{X}$ is isomorphic to the Roquette curve $Y^2 = X^q - X$ with genus $(q-1)/2$ ;*
- *$p \geq 2$ and $\mathcal{X}$ is isomorphic to the Hermitian curve $Y^{q+1} = X^q + X$ with genus $(q^2-q)/2$ ;*
- *$p = 2$ and $\mathcal{X}$ is isomorphic to the Suzuki curve $Y^q + Y = X^{q_0}(X^q + X)$ with genus $q_0(q-1)$ .*

**Remark 2.4.11.** *If $\mathcal{X}$ is the curve $\tilde{\mathcal{R}}_q$ and Case iv) of Theorem* 2.4.10 *occurs, then* $|\mathrm{Aut}(\tilde{\mathcal{R}}_q)| < 8g^3$*. In fact, since $p = 3$ and $g = \frac{3}{2}q_0(q-1)(q+q_0+1)$, $\tilde{\mathcal{R}}_q$ cannot satisfy any of the four exceptions.*

Theorem 2.4.12 provides a deeper analysis of Case *iv)* in Theorem 2.4.10; the bounds are taken from the proof of [67, Theorem 11.116].

**Theorem 2.4.12.** ([67, Theorem 11.116 and page 516]) *Suppose that Case iv) in Theorem* 2.4.10 *occurs. Then one of the following cases holds:*

1. $|\mathrm{Aut}(\mathcal{X})| \leq 8g(g-1)(g+1)$ *(see* [67, Eq. (11.169)]*).*
2. $\mathrm{Aut}(\mathcal{X})$ *contains $p$-elements stabilizing two distinct places.*
3. $|\mathrm{Aut}(\mathcal{X})| \leq 8(g+1)(g-1)$ *(see* [67, pages 524-525]*).*
4. *The non-tame short orbit of* $\mathrm{Aut}(\mathcal{X})$ *has length $p^k + 1$ for some $k$ (see* [67, Lemma 11.123]*).*

Cases *1.*, *3.*, and *4.* in Theorem 2.4.12 correspond to Case (iv1), (iv4), and (iv5) in [67, page 516], respectively; Case *2.* in Theorem 2.4.12 corresponds to Cases (iv2) and (iv3) in [67, page 516].

In analogy with Section 2.4.1, the following results hold. The proofs of Lemma 2.4.13, Lemma 2.4.14, and Corollary 2.4.15 are analogous to the proofs of Lemma 2.4.5, Lemma 2.4.6, and Corollary 2.4.7 in Section 2.4.1.

**Lemma 2.4.13.** *The group $LR(q)$ contains a subgroup $\tilde{R}(q)$ isomorphic to $R(q)$.*

**Lemma 2.4.14.** *The normalizer of $C_m$ in $\mathrm{Aut}(\tilde{\mathcal{R}}_q)$ is the direct product $\tilde{R}(q)\times C_m$.*

**Corollary 2.4.15.** *The group $LR(q)$ coincides with the normalizer of $C_m$ in $\mathrm{Aut}(\tilde{\mathcal{R}}_q)$.*

**Proposition 2.4.16.** *The group $LR(q)$ has exactly two short orbits $\mathcal{O}_T$ and $\mathcal{O}_{NT}$ in its action on $\tilde{\mathcal{R}}_q$. The orbit $\mathcal{O}_T$ is tame of size $(q^3+1)q^3(q-1)$, consisting of the places of $\tilde{\mathcal{R}}_q$ of degree 6; the orbit $\mathcal{O}_{NT}$ is non-tame, consisting of the $q^3+1$ $\mathbb{F}_q$-rational places of $\tilde{\mathcal{R}}_q$.*

*Proof.* The set $\mathcal{O}$ of the $\mathbb{F}_q$-rational places of $\tilde{\mathcal{R}}_q$ is the non-tame short orbit $\mathcal{O}_{NT}$ under $LR(q)$, since $C_m$ acts trivially on $\mathcal{O}$.

Let $\mathcal{O}_T \subseteq \tilde{\mathcal{R}}_q$ be the set of places of degree 6; we prove that $\mathcal{O}_T$ is a tame short orbit under $LR(q)$. Let $P \in \mathcal{O}_T$. Since $C_m$ is defined over $\mathbb{F}_{q^6}$, the place $Q \in \mathcal{R}_q$ lying under $P$ has degree 1, 2, 3, or 6. The places of $\mathcal{R}_q$ of degree 1 lie under a place in $\mathcal{O}_{NT}$, and $\mathcal{R}_q$ has no places of degree 2 or 3; therefore, $Q$ has degree 6. By the Fundamental Equality 1.1.1, we conclude that there are exactly $m$ places of $\tilde{\mathcal{R}}_q$ of degree 6 lying over a place of $\mathcal{R}_q$ of degree 6. By the $\mathbb{F}_{q^6}$-maximality of $\tilde{\mathcal{R}}_q$, we have that $|\mathcal{O}_T| = mq^3(q-1)(q+1)(q+3q_0+1)$; hence, $\mathcal{O}_T$ coincides with the set of places of $\tilde{\mathcal{R}}_q$ lying over a place of $\mathcal{R}_q$ of degree 6.

To show that $LR(q)$ is transitive on $\mathcal{O}_T$, let $P_1, P_2 \in \mathcal{O}_T$ with $P_1 \neq P_2$. If $P_1$ and $P_2$ are in the same $C_m$-orbit, the claim is proved. Otherwise, let $Q_1$ and $Q_2$ be the distinct places of $\mathcal{R}_q$ lying under $P_1$ and $P_2$, respectively. Since $Q_1$ and $Q_2$ are in the tame short orbit of $\mathcal{R}_q$ under $R(q)$, there exists $\sigma \in R(q)$ such that $\sigma(Q_1) = Q_2$. Let $\tilde{\sigma}$ be the induced automorphism of $\tilde{\mathcal{R}}_q$, and let $P_3 := \tilde{\sigma}(P_1)$. Then $P_3$ is in the $C_m$-orbit of $P_2$, because $\mathcal{S}_q$ is $\tilde{\mathcal{S}}_q/C_m$. Let $\tau \in C_m$ with $\tau(P_3) = P_2$; then $\tau\tilde{\sigma}(P_1) = P_2$.

Since $R(q)$ acts semiregularly on the places of $\mathcal{R}_q$ of degree greater than 6, $LR(q)$ acts semiregularly on $\tilde{\mathcal{R}}_q \setminus (\mathcal{O}_T \cup \mathcal{O}_{NT})$, and the thesis is proved. □

Let $\tilde{\mathcal{O}}_{NT}$ be the non-tame short orbit of $\tilde{\mathcal{R}}_q$ under $\mathrm{Aut}(\tilde{\mathcal{R}}_q)$ containing $\mathcal{O}_{NT}$.

**Lemma 2.4.17.** *The orbit $\tilde{\mathcal{O}}_{NT}$ coincides with $\mathcal{O}_{NT}$.*

*Proof.* Suppose by contradiction that $\mathcal{O}_{NT} \neq \tilde{\mathcal{O}}_{NT}$.

Firstly, suppose that $\tilde{\mathcal{O}}_{NT} \setminus \mathcal{O}_{NT}$ contains a long orbit under $LR(q)$. Then, for any $\mathbb{F}_q$-rational place $P \in \tilde{\mathcal{R}}_q$ we have

$$\begin{aligned}|\mathrm{Aut}(\tilde{\mathcal{R}}_q)| &= |\tilde{\mathcal{O}}_{NT}| \cdot |\mathrm{Aut}(\tilde{\mathcal{R}}_q)_P| \geq |LR(q)| \cdot |LR(q)_P| \\ &\geq (q^3+1)q^3(q-1)m \cdot q^3(q-1)m > 8g^3,\end{aligned}$$

where $g$ is the genus of $\tilde{\mathcal{R}}_q$ and $LR(q)_P$ denotes the stabilizer of $P$ in $LR(q)$. This is a contradiction to Theorem 2.4.10 and Remark 2.4.11, since $|\mathrm{Aut}(\tilde{\mathcal{R}}_q)| > 84(g-1)$.

Then $\tilde{\mathcal{O}}_{NT} \setminus \mathcal{O}_{NT}$ contains a short orbit under $LR(q)$ and $\tilde{\mathcal{O}}_{NT} = \mathcal{O}_{NT} \cup \mathcal{O}_T$ by Proposition 2.4.16.

If $\mathrm{Aut}(\tilde{\mathcal{R}}_q)_P \neq LR(q)_P$, then $|\mathrm{Aut}(\tilde{\mathcal{R}}_q)_P| \geq 2|LR(q)_P|$, and hence

$$|\mathrm{Aut}(\tilde{\mathcal{R}}_q)| = |\tilde{\mathcal{O}}_{NT}| \cdot |\mathrm{Aut}(\tilde{\mathcal{R}}_q)_P| \geq |\tilde{\mathcal{O}}_{NT}| \cdot 2|LR(q)_P| \geq |\mathcal{O}_T| \cdot 2q^3(q-1)m > 8g^3,$$

a contradiction to Theorem 2.4.10. Therefore, $\mathrm{Aut}(\tilde{\mathcal{R}}_q)_P = LR(q)_P$. This implies

$$|\mathrm{Aut}(\tilde{\mathcal{R}}_q)| = |\tilde{\mathcal{O}}_{NT}| \cdot |LR(q)_P| = (q^3+1)q^3(q-1)(q-3q_0+1)(q^4-q^3+1).$$

Note that the order of $|\mathrm{Aut}(\tilde{\mathcal{R}}_q)|$ is very close to $8g^3$.

Since $|\mathrm{Aut}(\tilde{\mathcal{R}}_q)| > g(2g-2)(4g+2)$, Cases *i)*, *ii)*, and *iii)* in Theorem 2.4.10 cannot occur, hence Case *iv)* holds and one of Cases *1.* - *4.* in Theorem 2.4.12 occurs.

- Since $|\mathrm{Aut}(\tilde{\mathcal{R}}_q)| > 8g(g-1)(g+1)$, Cases *1.* and *3.* cannot occur.
- Case *2.* cannot occur; in fact, $\tilde{\mathcal{R}}_q$ has zero $p$-rank, and hence any $p$-element in $\mathrm{Aut}(\tilde{\mathcal{R}}_q)$ has exactly one fixed place ([67, Lemma 11.129]).
- Case *4.* cannot occur, since $|\tilde{\mathcal{O}}_{NT}| = (q^3+1)(q^4-q^3+1) \neq 3^k+1$ for any $k$.

The claim follows. □

Finally we prove Theorem 2.4.2. Let $\alpha \in \mathrm{Aut}(\tilde{\mathcal{R}}_q)$, and define $T := \{\sigma \in \mathrm{Aut}(\tilde{\mathcal{R}}_q) \mid \sigma(P) = P \text{ for all } P \in \tilde{\mathcal{O}}_{NT}\}$ and $C'_m := \alpha C_m \alpha^{-1}$. Clearly, $T$ contains $C_m$ and $C'_m$. By [67, Lemma 11.129], $T$ is a tame subgroup of $\mathrm{Aut}(\tilde{\mathcal{R}}_q)$, which implies that $T$ is cyclic (see [67, Lemma 11.44]). Therefore $C'_m = C_m$, that is, $C_m$ is normal in $\mathrm{Aut}(\tilde{\mathcal{R}}_q)$. By Corollary 2.4.15, Theorem 2.4.2 follows.

**Remark 2.4.18.** *Theorem* 2.4.2 *shows that* $\mathrm{Aut}(\tilde{\mathcal{R}}_q)$ *is exactly the cyclic extension* $LR(q)$ *of the automorphism group* $R(q)$ *of the cyclic subcover* $\mathcal{R}_q$.

### 2.4.3 Non-existence of certain Galois coverings

Firstly, we prove that $\mathcal{S}_q$ is not Galois covered by $\mathcal{H}_{q^2}$ for any $q$, as stated in Theorem 2.4.3.

*Proof.* Suppose by contradiction that $\tilde{\mathcal{S}}_q$ is a Galois subcover of $\mathcal{H}_{q^2}$, that is, $\tilde{\mathcal{S}}_q \cong \mathcal{H}_{q^2}/G$ with $G \leq \mathrm{PGU}(3,q^2)$. The different divisor has degree

$$\Delta = (2g(\mathcal{H}_{q^2})-2) - |G|(2g(\tilde{\mathcal{S}}_q)-2) = q^4-q^2-2-|G|(q^3-2q^2+q-2)\,. \quad (2.27)$$

By the Riemann-Hurwitz formula,

$$\frac{q^6+1}{q^5-q^4+q^3+1} = \frac{|\mathcal{H}_{q^2}(\mathbb{F}_{q^4})|}{|\tilde{\mathcal{S}}_q(\mathbb{F}_{q^4})|} \leq |G| \leq \frac{2g(\mathcal{H}_{q^2})-2}{2g(\tilde{\mathcal{S}}_q)-2} = \frac{q^4-q^2-2}{q^3-2q^2+q-2}\,,$$

hence $q+1 \leq |G| \leq q+2$.

Assume $|G| = q+1$. By Theorem 2.3.9, we have $\Delta = q \cdot 2$. This contradicts Equation (2.27), which reads $\Delta = q^3+q$.

For $q > 8$, $|G| \neq q+2$ because $|G|$ divides $|\mathrm{PGU}(3,q^2)| = (q^6+1)q^6(q^4-1)$. For $q = 8$, assume $|G| = q+2 = 10$. By Lemma 2.3.4, the generator $\alpha$ of the unique Sylow 5-subgroup $C_5$ is either of type (A) or (B1); hence, $\alpha$ fixes a point $P$ and a line $\ell$ not through $P$. Since $C_5$ is normal in $G$, the generator $\beta$ of any Sylow 2-subgroup $C_2$ of $G$ fixes $P$ and $\ell$. Therefore, $\beta$ cannot be of type (D); thus, $\beta$ is of type (C). This implies that $\alpha$ is not of type (B1), and hence $\alpha$ is of type (A). Then $\Delta \geq 4 \cdot 65$ by Theorem 2.3.9, a contradiction to Equation (2.27). □

Now consider the curve $\tilde{\mathcal{R}}_q$. Suppose that $\tilde{\mathcal{R}}_q \cong \mathcal{H}_{q^3}/G$ for some $G \leq \mathrm{PGU}(3,q^3)$. The different divisor has degree

$$\Delta = (2g(\mathcal{H}_{q^3})-2) - |G|(2g(\tilde{\mathcal{R}}_q)-2) = q^6-q^3-2-|G|(q^4-2q^3+q-2)\,. \quad (2.28)$$

By the Riemann-Hurwitz formula,

$$\frac{q^9+1}{q^7-q^6+q^4+1} = \frac{|\mathcal{H}_{q^3}(\mathbb{F}_{q^6})|}{|\tilde{\mathcal{R}}_q(\mathbb{F}_{q^6})|} \leq |G| \leq \frac{2g(\mathcal{H}_{q^3})-2}{2g(\tilde{\mathcal{R}}_q)-2} = \frac{q^6-q^3-2}{q^4-2q^3+q-2}\,,$$

hence

$$q^2+q+1 \leq |G| \leq q^2+2q+4.$$

**Lemma 2.4.19.** *If $\tilde{\mathcal{R}}_q \cong \mathcal{H}_{q^3}/G$, then*

$$|G| \mid |\mathrm{PGU}(3,q^3)|\,, \quad q^2+q+1 \leq |G| \leq q^2+2q+4\,, \quad |G| \notin \{q^2+q+1, q^2+2q+1\}.$$

*Proof.* **Case $|G| = q^2 + q + 1$.** Since $|G|$ divides $q^3 - 1$ and is coprime to $q^3 + 1$, we have by Theorem 2.3.9 that $\Delta = 2(q^2 + q)$, a contradiction to Equation (2.28).

**Case $|G| = q^2 + 2q + 1 = (q + 1)^2$.** By Theorem 1.2.6 it can be shown that $\mathrm{PGU}(3, q^3)$ contains only two conjugacy classes of maximal subgroups whose order is divisible by $|G|$:

- The stabilizer $M_1$ of a self-conjugate triangle $T$, of order $|M_1| = 6(q^3 + 1)^2$.
- The stabilizer $M_2$ of a non-tangent line $\ell$, of order $|M_2| = q^3(q^6 - 1)(q + 1)$.

  The center $Z$ of $M_2$ has order $q^3 + 1$ and is a cyclic group of homologies acting trivially on $\ell$. The group $M_2/Z$ acts faithfully on $\ell$ as a linear group, hence it is isomorphic to a subgroup of $\mathrm{PGL}(2, q^6)$. $M_2/Z$ acts on the $q^3 + 1$ points of $\ell \cap \mathcal{H}_{q^3}$. From the structure of $M_2$, we have that $M_2 \cong \mathrm{PGL}(2, q^3)$, and the action of $M_2$ on $\ell \cap \mathcal{H}_{q^3}$ is equivalent to the action of $\mathrm{PGL}(2, q^3)$ in its natural 2-transitive permutation representation.

Suppose that $G \subseteq M_2$. The group $G/(Z \cap G)$ acts faithfully on $\ell$ and is isomorphic to a subgroup of $\mathrm{PGL}(2, q^3)$. Since $|G \cap Z|$ is a divisor of $q + 1$, we have that $|G/(G \cap Z)| = (q + 1)d$, where $d$ divides $q + 1$. We conclude that $|G/(G \cap Z)|$ is equal to $q + 1$ or $2(q + 1)$, since $|\mathrm{PGL}(2, q^3)| = q(q^2 - 1)$. Moreover, from Theorem 1.2.7, one of the following cases occurs:

- $G/(Z \cap G)$ is a cyclic Singer group fixing two points $P_1, P_2$ on $\ell \setminus \mathcal{H}_{q^3}$. The pole $P_3$ of $\ell$ is also fixed by $G$. Hence, $G$ fixes a self-conjugate triangle $T$.
- $G/(Z \cap G)$ is a dihedral group normalizing a cyclic Singer group $S$ of index 2, such that $S$ fixes two points $P_1, P_2$ on $\ell \setminus \mathcal{H}_{q^3}$. Also, $G/S$ interchanges $P_1$ and $P_2$, and $G$ fixes the pole $P_3$ of $P_1P_2$. Then $G$ fixes a self-conjugate triangle $T$.

Therefore, $G \subseteq M_1$. Up to conjugation, $\mathcal{H}_{q^3}$ has the Fermat equation (1.3) and $T$ is the fundamental triangle, so that

$$M_1 = \{\mathrm{diag}(\lambda, \mu, 1) \mid \lambda^{q^3+1} = \mu^{q^3+1} = 1\} \rtimes S_3,$$

where the symmetric group $S_3$ is given by the $3 \times 3$ permutation matrices. The only subgroup of order $(q + 1)^2$ in $M_1$ is

$$G = \{\mathrm{diag}(\lambda, \mu, 1) \mid \lambda^{q+1} = \mu^{q+1} = 1\} \cong C_{q+1} \times C_{q+1}.$$

With the notation of Lemma 2.3.4, $G$ contains exactly $3q$ elements of type (A) and $q^2 - q$ elements of type (B1). Then $\Delta = 3q(q^3+1)$ by Theorem 2.3.9. The same value for $\Delta$ is obtained by Equation (2.28), that is, the curves $\mathcal{H}_{q^3}/G$ and $\tilde{\mathcal{R}}_q$ actually have the same genus.

The group $G$ is normal in $M_1$, thus $M_1/G$ is an automorphism group of $\mathcal{H}_{q^3}/G$ of order $|M_1/G| = 6(q^2-q+1)^2$. Since $|M_1/G|$ is not a divisor of $|\mathrm{Aut}(\tilde{\mathcal{R}}_q)| = (q^3+1)q^3(q-1)(q-3q_0+1)$, we have $\mathcal{H}_{q^3}/G \not\cong \tilde{\mathcal{R}}_q$. □

By the proof of Lemma 2.4.19 the following remark is obtained.

**Remark 2.4.20.** *For any odd power $q \geq 27$ of 3, let $G \leq \mathrm{PGU}(3,q^3)$ with $|G| = (q+1)^2$ ($G$ is unique up to conjugation). Then the curves $\mathcal{H}_{q^3}/G$ and $\tilde{\mathcal{R}}_q$ have the same genus but are not isomorphic, as they have different automorphism groups.*

Finally, we prove that $\mathcal{R}_q$ is not Galois covered by $\mathcal{H}_{q^3}$ for any $q$, as stated in Theorem 2.4.4.

*Proof.* Suppose by contradiction that $\mathcal{R}_q$ is Galois covered by $\mathcal{H}_{q^3}$, that is, $\tilde{\mathcal{R}}_q \cong \mathcal{H}_{q^3}/G$ with $G \leq \mathrm{PGU}(3,q)$. By Lemma 2.4.19, the order of $G$ satisfies $q^2+q+2 \leq |G| \leq q^2+2q+4$ and $|G| \neq q^2+2q+1$. By Equation (2.28) $\Delta$ is a multiple of $q^3+1$. This fact, together with $3|G| < q^3+1$ and Theorem 2.3.9, implies that $i(\sigma) \in \{0, q^3+1\}$ for any nontrivial $\sigma \in G$, that is, $\sigma$ is of type (A) or (B1) and the order of $\sigma$ divides $q^3+1$.

From Theorem 1.2.6 it can be deduced that $G$ is contained in the stabilizer $N \leq \mathrm{PGU}(3,q^3)$ of a self-conjugate triangle, hence $G$ acts on three non-collinear points $\{P_1,P_2,P_3\}$ of $\mathrm{PG}(2,q^6) \setminus \mathcal{H}_{q^3}$. In fact, because of its order, $G$ can be only be contained in the following maximal subgroups of $\mathrm{PGU}(3,q^3)$ other than $N$:

1. The stabilizer of one point $P \in \mathcal{H}_{q^3}(\mathbb{F}_{q^6})$. In this case, $G$ cannot contain any element of type (B1) by Lemma 2.3.4. Hence $\Delta = (q^3+1)(|G|-1)$, exceeding the value of $\Delta$ in Equation (2.28).

2. The stabilizer of a point $P_1 \in \mathrm{PG}(2,q^6) \setminus \mathcal{H}_{q^3}$ and its non-tangent polar line $\ell$. In this case, by Theorem 1.2.7, either $G$ acts trivially on $\ell$, or $G$ fixes two points $P_2, P_3 \in \ell \setminus \mathcal{H}_{q^3}$. In the former case, $\Delta$ exceeds the value in Equation (2.28). In the latter case, $G$ acts on the self-conjugate triangle $\{P_1,P_2,P_3\}$.

3. A group isomorphic to $\mathrm{PGL}(2,q^3)$. In this case, by Theorem 1.2.7, $G$ contains a cyclic normal subgroup $G'$ of index 1 or 2 such that $G'$ exactly three points $\{P_1,P_2,P_3\}$, which are the vertices of a self-conjugate triangle $T$. Therefore $G$ acts on $\{P_1,P_2,P_3\}$.

4. A group isomorphic to $\mathrm{PGU}(3,q)$. This is impossible since $G$ cannot divide three times the order of any maximal subgroup of $\mathrm{PSU}(3,q)$, and hence the order of any maximal subgroup of $\mathrm{PGU}(3,q)$.

Note that, since $|G|$ is not divisible by 3, $G$ fixes at least one point in $\{P_1, P_2, P_3\}$, say $P_1$, and acts on $\{P_2, P_3\}$. Let $Z \leq N$ be the subgroup of homologies (that is, elements of type (A)) with center $P_1$ and axis $P_2P_3$; $Z$ is cyclic of order $q^3+1$ and is the center of $N$. By direct computation, there exists a divisor $d > 2$ of $q+1$ which is coprime to $|G|$. Then the normalizer of $G$ in $\mathrm{PGU}(3,q^3)$ contains the subgroup $D$ of $Z$ of order $d$. Therefore $D$ induces a cyclic automorphism group $\bar{D}$ of $\mathcal{H}_{q^3}/G \cong \tilde{\mathcal{R}}_q$ of order $d$ which fixes at least one point of $\tilde{\mathcal{R}}_q$. The automorphism group of $\tilde{\mathcal{R}}_q$ has exactly two short orbits $\mathcal{O}_T$ and $\mathcal{O}_{NT}$ of size $(q^3+1)q^3(q-1)$ and $q^3+1$; see Proposition 2.4.16. Then $d$ divides $|\mathrm{Aut}(\tilde{\mathcal{R}}_q)|/|\mathcal{O}_T|$ or $|\mathrm{Aut}(\tilde{\mathcal{R}}_q)|/|\mathcal{O}_{NT}|$. By direct checking, this is impossible. □

# Chapter 3

# Results on AG codes

In this chapter we investigate certain multi-point Algebraic-Geometric codes associated to Kummer curves and GK curves.

In Section 3.1 we consider Kummer extensions of the rational function field $\mathbb{F}_q(x)$, defined by $y^m = f(x)$, where the polynomial $f(T) \in \mathbb{F}_q[T]$ is separable and has degree coprime to $m$. We compute the number of Weierstrass gaps at two totally ramified places. Also, we give a criterion to find pure gaps at many totally ramified places and present families of pure gaps. We then apply our results to construct AG codes with good parameters and provide examples of Hermitian codes. The results of Section 3.1 are the object of [9].

In Section 3.2 we investigate multi-point AG codes associated to the GK curves $\mathcal{GK}_q$, starting from a divisor which is invariant under a large automorphism group of $\mathcal{GK}_q$. In this way, we construct families of AG codes with large automorphism groups. Using the Weierstrass semigroup at one $\mathbb{F}_{q^2}$-rational-point of $\mathcal{GK}_q$, the dimension of the codes is determined. The results of Section 3.2 are the object of [8].

## 3.1 Algebraic Geometric Codes on Many Points from Kummer Extensions

Throughout this section, $F$ is a function field over $\mathbb{F}_q$ defined as a Kummer extension of the rational function field $\mathbb{F}_q(x)$ by $y^m = f(x)$, where $f(x) \in \mathbb{F}_q[x]$ is a separable polynomial of degree $r$ coprime to $m$.

We investigate the Weierstrass semigroup at many totally ramified places, extending results by Castellanos, Masuda, and Quoos ([24]) and by Matthews ([41, Theorem 3.6]). In particular, we compute in Section 3.1.1 the number of gaps at two totally ramified places, and we give in Section 3.1.2 an arithmetic characterization of pure gaps at many points which provides families of pure gaps. We apply these results to improve the Singleton defect of certain differential AG codes $C_\Omega(D,G)$. In Example 3.1.12 we illustrate our achievements with AG codes on many points from the the Hermitian function field, and observe that the best improvements on the minimum distance with respect to the corresponding ones in the MinT's Tables [89] are obtained by two- or three-point codes.

### 3.1.1 The Weierstrass semigroup at two points

Let $P_1, P_2$ be places of $F$ which are totally ramified in $F|\mathbb{F}_q(x)$. As pointed out in Equation (1.2), the Weierstrass semigroup $H(P_1,P_2)$ is related to the set $\Gamma(P_1,P_2)$, and [24, Theorem 4.3] yields

$$\Gamma(P_\infty,P_1)=\left\{(mr-mj-ri,i+m(j-1))\,\middle|\,1\le i\le m-1-\left\lfloor\frac{m}{r}\right\rfloor,1\le j\le r-1-\left\lfloor\frac{ri}{m}\right\rfloor\right\},$$

where $P_\infty \neq P_1$ is the unique pole of $x$.

**Proposition 3.1.1.** *Let $P_1, P_2$ be two distinct places of $F$ totally ramified in $F|\mathbb{F}_q(x)$ and different from $P_\infty$. Then*

$$\Gamma(P_1,P_2)=\left\{\left(mi-j,m\left(\left\lceil\frac{rj}{m}\right\rceil-i\right)-j\right)\,\middle|\,1+\left\lfloor\frac{m}{r}\right\rfloor\le j\le m-1,1\le i\le\left\lceil\frac{rj}{m}\right\rceil-1\right\}.$$

*Proof.* For $\iota\in\{1,2\}$ let $\alpha_\iota\in\mathbb{F}_q$ be such that $P_\iota$ is the unique zero of $x-\alpha_\iota$ in $F$. Let $i,j$ be positive integers and $k=\left\lceil\frac{jr}{m}\right\rceil-i$, so that $(i+k)m\ge jr$. By [24, Prop. 3.1], the pole divisor of $\frac{y^j}{(x-\alpha_1)^i(x-\alpha_2)^k}$ is $(mi-j)P_1+(mk-j)P_2$. Also, for $j\in\left\{1+\left\lfloor\frac{m}{r}\right\rfloor,\dots,m-1\right\}$ and $h\in\left\{1,\dots,\left\lceil\frac{rk}{m}\right\rceil-1\right\}$, we have that $(mh-j)\in G(P_1)\cap G(P_2)$ by [24, Th. 3.2]. Hence, the set

$$\Gamma'=\left\{\left(mi-j,m\left(\left\lceil\frac{rj}{m}\right\rceil-i\right)-j\right)\;\middle|\;1+\left\lfloor\frac{m}{r}\right\rfloor\le j\le m-1,1\le i\le\left\lceil\frac{rj}{m}\right\rceil-1\right\}$$

is a subset of $G(P_1)\times G(P_2)\cap H(P_1,P_2)$. The cardinality of $\Gamma'$ is

$$|\Gamma'|=\sum_{k=1+\lfloor\frac{m}{r}\rfloor}^{m-1}\left(\left\lceil\frac{rk}{m}\right\rceil-1\right)=\left(\sum_{k=1+\lfloor\frac{m}{r}\rfloor}^{m-1}\left\lceil\frac{rk}{m}\right\rceil\right)-\left(m-\left\lfloor\frac{m}{r}\right\rfloor-1\right)$$

$$=\left(\sum_{k=0}^{m-1}\left\lceil\frac{rk}{m}\right\rceil\right)-\left\lfloor\frac{m}{r}\right\rfloor-\left(m-\left\lfloor\frac{m}{r}\right\rfloor-1\right)=-\sum_{k=0}^{m-1}\left\lfloor\frac{-rk}{m}\right\rfloor-m+1$$

$$=-(m-1)(-r-1)/2-m+1=(m-1)(r-1)/2=g,$$

using [59, Page 94]. Therefore $\Gamma'=\Gamma(P_1,P_2)$ by Lemma 1.1.43. □

From Proposition 3.1.1 we are able to compute the number of gaps at two totally ramified places in the case $m \equiv 1 \pmod{r}$.

**Theorem 3.1.2.** *Let $P_\infty$ be the pole of $x$ in $F$ and $P_1, P_2$ be distinct places of $F$ totally ramified in $F/\mathbb{F}_q(x)$ and different from $P_\infty$. If $m = ur + 1$ for some integer $u$, then*

$$|G(P_1, P_2)| = \frac{ur(r-1)(3ur^2 - 5ur + 4r + 4u - 2)}{12}, \textit{ and}$$
$$|G(P_\infty, P_1)| = \frac{ur(r-1)(3ur^2 - 3ur + 2r + 2)}{12}.$$

*Proof.* By Proposition 3.1.1,

$$\Gamma(P_1, P_2) = \left\{ \left( mi - j, m\left( \left\lceil \frac{rj}{m} \right\rceil - i \right) - j \right) \;\middle|\; 1 + u \le j \le m - 1, 1 \le i \le \left\lceil \frac{rj}{m} \right\rceil - 1 \right\}.$$

Setting $(i_0, j_0) \in \mathbb{N}^2$ with $1 + u \le j_0 \le m - 1$ and $1 \le i_0 \le \lceil \frac{rj_0}{m} \rceil - 1$; by Theorem 1.1.42, we need to count the number $r_{i_0,j_0}$ of pairs $(i_1, j_1) \in \mathbb{N}^2$ such that

$$\begin{gathered} 1 + u \le j_1 \le ru, \quad 1 \le i_1 \le \lceil \tfrac{rj_1}{m} \rceil - 1, \quad m\,(i_0 - i_1) < j_0 - j_1, \\ m\left( \lceil \tfrac{rj_1}{m} \rceil - \lceil \tfrac{rj_0}{m} \rceil + i_0 - i_1 \right) < j_1 - j_0. \end{gathered} \tag{3.1}$$

For $h \in \{0, 1\}$ write $j_h = k_h u + t_h$ with $k_h \in \{1, \ldots, r-1\}$ and $t_h \in \{1, \ldots, u\}$. Then $\lceil \frac{rj_h}{m} \rceil = k_h + 1$. We split $r_{i_0,j_0}$ in a number of cases:

- $j_1 = j_0$. Then (3.1) implies $i_0 + 1 \le i_1 \le k_1$.

- $j_1 > j_0$ and $k_1 = k_0$. Then (3.1) implies $1 \le t_0 \le u - 1$, $t_1 \ge t_0 + 1$, and $i_0 + 1 \le i_1 \le k_1$.

- $j_1 > j_0$ and $k_1 > k_0$. Then (3.1) implies $i_0 + k_1 - k_0 \le i_1 \le k_1$.

- $j_1 < j_0$ and $k_1 < k_0$. Then (3.1) implies $1 \le t_0, t_1 \le u$, $1 \le i_0 \le k_1$, and $i_0 \le i_1 \le k_1$.

- $j_1 < j_0$ and $k_1 = k_0$. Then (3.1) implies $2 \le t_0 \le u$, $t_1 \le t_0 - 1$, and $i_0 + 1 \le i_1 \le k_1$.

By direct computation, this yields

$$\begin{aligned} r(P_1,P_2) = &\sum_{(i_0,j_0)\in\Gamma(P_1,P_2)} r_{i_0,j_0} = \sum_{k_0=1}^{r-1}\sum_{t_0=1}^{u}\sum_{i_0=1}^{k_0}(k_0-i_0) + \sum_{k_0=1}^{r-1}\sum_{t_0=1}^{u-1}\sum_{t_1=t_0+1}^{u}\sum_{i_0=1}^{k_0}(k_0-i_0) \\ &+ \sum_{k_0=1}^{r-2}\sum_{t_0=1}^{u}\sum_{k_1=k_0+1}^{r-1}\sum_{t_1=1}^{u}\sum_{i_0=1}^{k_0}(k_0-i_0+1) + \sum_{k_0=2}^{r-1}\sum_{t_0=1}^{u}\sum_{k_1=1}^{k_0-1}\sum_{t_1=1}^{u}\sum_{i_0=1}^{k_1}(k_1-i_0+1) \\ &+ \sum_{k_0=1}^{r-1}\sum_{t_0=2}^{u}\sum_{t_1=1}^{t_0-1}\sum_{i_0=1}^{k_0}(k_0-i_0) = \frac{u^2(r-2)(r-1)r(r+3)}{12}. \end{aligned}$$

Also, by [24, Theorem 3.2], we have

$$\sum_{n\in G(P_1)} n = \sum_{n\in G(P_2)} n = \sum_{j=1+u}^{m-1}\sum_{i=1}^{\lceil \frac{rj}{m}\rceil -1}(mi-j) = \sum_{k=1}^{r-1}\sum_{t=1}^{u}\sum_{i=1}^{k-1}((ur+1)i-(ku+t)) \tag{3.2}$$

$$= \frac{ur(r-1)(2r^2u-2ru+2r-u-1)}{12}. \tag{3.3}$$

Therefore we obtain

$$|G(P_1,P_2)| = \sum_{n\in G(P_1)} n + \sum_{n\in G(P_2)} n - r(P_1,P_2) = \frac{ur(r-1)(3r^2u-5ru+4r+4u-2)}{12}.$$

By [24, Theorem 4.3],

$$\Gamma(P_\infty,P_1) = \left\{ (mr-mj-ri, m(j-1)+i) \,\middle|\, 1\le i\le m-1-u, 1\le j\le r-1-\left\lfloor \frac{ri}{m}\right\rfloor \right\}.$$

For $(i_0,j_0)\in\mathbb{N}^2$ with $1\le i_0\le m-1-u$ and $1\le j_0\le r-1-\left\lfloor\frac{ri_0}{m}\right\rfloor$, as above we need to count the number $s_{i_0,j_0}$ of pairs $(i_1,j_1)\in\mathbb{N}^2$ such that

$$\begin{gathered} 1\le i_1\le m-1-u, \quad 1\le j_1\le r-1-\left\lfloor\tfrac{ri_1}{m}\right\rfloor, \\ m(j_1-j_0) < r(i_0-i_1), \quad m(j_1-j_0) < (i_0-i_1). \end{gathered} \tag{3.4}$$

For $h\in\{0,1\}$ write $i_h = k_hu+t_h$, with $k_h\in\{0,\dots,r-2\}$ and $t_h\in\{1,\dots,u\}$. Then $\left\lfloor\frac{ri_h}{m}\right\rfloor = k_h$. We split $s_{i_0,j_0}$ in a number of cases:

- $i_1 = i_0$. Then (3.4) implies $1\le j_1\le j_0-1$.
- $i_1 > i_0$, $k_1 > k_0$, and $t_1\le t_0$. Then (3.4) implies $k_1-k_0+1\le j_0\le r-1-k_0$ and $1\le j_1\le k_0-k_1+j_0$.

- $i_1 > i_0$, $k_1 \geq k_0$, and $t_1 > t_0$. Then (3.4) implies $k_1 - k_0 + 2 \leq j_0 \leq r - 1 - k_0$ and $1 \leq j_1 \leq k_0 - k_1 - 1 + j_0$.
- $i_1 < i_0$ and $k_1 < k_0$. Then (3.4) implies $1 \leq j_1 \leq j_0$.
- $i_1 < i_0$, $k_1 = k_0$ and $t_1 < t_0$. Then (3.4) implies $1 \leq j_1 \leq j_0$.

By direct computation, this yields

$$\begin{aligned} r(P_\infty, P_1) = & \sum_{(i_0,j_0)\in\Gamma(P_\infty,P_1)} s_{i_0,j_0} = \sum_{k_0=0}^{r-2}\sum_{t_0=1}^{u}\sum_{j_0=1}^{r-1-k_0}(j_0-1) \\ & + \sum_{k_0=0}^{r-2}\sum_{t_0=1}^{u}\sum_{k_1=k_0+1}^{r-2}\sum_{t_1=1}^{t_0}\sum_{j_0=k_1-k_0+1}^{r-1-k_0}(k_0-k_1+j_0) \\ & + \sum_{k_0=0}^{r-2}\sum_{t_0=1}^{u}\sum_{k_1=k_0}^{r-2}\sum_{t_1=t_0+1}^{u}\sum_{j_0=k_1-k_0+2}^{r-1-k_0}(k_0-k_1-1+j_0) \\ & + \sum_{k_0=0}^{r-2}\sum_{t_0=1}^{u}\sum_{k_1=0}^{k_0-1}\sum_{t_1=1}^{u}\sum_{j_0=1}^{r-1-k_0} j_0 + \sum_{k_0=0}^{r-2}\sum_{t_0=1}^{u}\sum_{t_1=1}^{t_0-1}\sum_{j_0=1}^{r-1-k_0} j_0 \\ & = \frac{u(r-1)r(ur^2+r-u-5)}{12}. \end{aligned}$$

Also, by [24, Theorem 3.2], we have

$$\begin{aligned} \sum_{n\in G(P_\infty)} n & = \sum_{i=1}^{m-1-u}\sum_{j=1}^{r-1-\left\lfloor \frac{ri}{m}\right\rfloor}(mr-mj-ri) \\ & = \sum_{k=0}^{r-2}\sum_{t=1}^{u}\sum_{j=1}^{r-1-k}(mr-mj-r(ku+t)) = \frac{ur(r-1)(2ur^2-ur+r-2)}{12}, \end{aligned}$$

and $\sum_{n\in G(P_1)} n$ was computed in 3.3. Therefore we obtain

$$|G(P_1,P_2)| = \sum_{n\in G(P_1)} n - \sum_{n\in G(P_2)} n + r(P_1,P_2) = \frac{ur(r-1)(3r^2u-5ru+4r+4u-2)}{12}.$$

□

**Remark 3.1.3.** *If $F = \mathbb{F}_q(\mathcal{H}_q)$ is the function field of the Hermitian curve, then Theorem* 3.1.2 *was already obtained in* [41, Theorem 3.6]*. In fact, the places of $\mathbb{F}_q(\mathcal{H}_q)$ which are totally ramified in $\mathbb{F}_q(\mathcal{H}_q)/\mathbb{F}_{q^2}(x)$ are Weierstrass places.*

### 3.1.2 Pure gaps at many points and codes

Let $P_\infty, P_1, \dots, P_s$ ($s \geq 1$) be distinct places of $F$ which are totally ramified in $F|\mathbb{F}_q(x)$; here, $P_\infty$ is the pole of $x$. In this section we give arithmetic conditions which characterize the pure gaps at $P_1, \dots, P_s$ and at $P_\infty, P_1, \dots, P_s$. We use this characterization to determine explicit families of pure gaps at many points and apply it to construct AG codes with good parameters.

We start from a result by Maharaj. For any divisor $D$ of $F$ and a function field $E \subseteq F$, write $D = \sum_{R \in \mathbb{P}(E)} \sum_{Q \in \mathbb{P}(F),\, Q|R} n_Q\, Q$. We define the restriction of $D$ to $E$ as

$$D\Big|_E = \sum_{R \in \mathbb{P}(E)} \min \left\{ \left\lfloor \frac{n_Q}{e(Q|R)} \right\rfloor : Q|R \right\} R.$$

**Theorem 3.1.4** ([86, Theorem 2.2]). *For any divisor $D$ of $F$ that is invariant under the action of $Gal(F/\mathbb{F}_q(x))$, we have that*

$$\mathcal{L}(D) = \bigoplus_{t=0}^{m-1} \mathcal{L}\left( \left[D + (y^t)\right] \Big|_{\mathbb{F}_q(x)} \right) y^t,$$

*where $[D + (y^t)] \Big|_{\mathbb{F}_q(x)}$ denotes the restriction of the divisor $D + (y^t)$ to $\mathbb{F}_q(x)$.*

**Proposition 3.1.5.** *Under the above notation, let $s \leq r$. The $s$-tuple $(a_1, \dots, a_s) \in \mathbb{N}^s$ is a pure gap at $P_1, \dots, P_s$ if and only if, for every $t \in \{0, \dots, m-1\}$, exactly one of the following two conditions is satisfied:*

*i)* $\sum_{i=1}^s \left\lfloor \frac{a_i+t}{m} \right\rfloor + \left\lfloor \frac{-rt}{m} \right\rfloor < 0$;

*ii)* $\sum_{i=1}^s \left\lfloor \frac{a_i+t}{m} \right\rfloor + \left\lfloor \frac{-rt}{m} \right\rfloor \geq 0$ *and* $\left\lfloor \frac{a_i+t}{m} \right\rfloor = \left\lfloor \frac{a_i-1+t}{m} \right\rfloor$, *for all* $i = 1, \dots, s$.

*Proof.* Let $P_1, \dots, P_r$, be all the places of $F$ which are totally ramified in $F|\mathbb{F}_q(x)$ except $P_\infty$, that is, $P_i$ is the zero of $x - \alpha_i$, where $f(x) = \prod_{i=1}^r (x - \alpha_i)$ is the separable polynomial defining $F$ by $y^m = f(x)$. Then the divisor of $y$ in $F$ is $(y) = \sum_{i=1}^r P_i - rP_\infty$, and hence, for any $t \in \{0, \dots, m-1\}$,

$$\sum_{i=1}^s a_i P_i + (y^t) = \sum_{i=1}^s (a_i + t) P_i + \sum_{i=s+1}^r t P_i - rtP_\infty\,.$$

Let $Q_1, \dots, Q_r, Q_\infty$ be the places of $\mathbb{F}_q(x)$ lying under $P_1, \dots, P_r, P_\infty$, respectively. Then

$$\left[ \sum_{i=1}^s a_i P_i + (y^t) \right] \Big|_{K(x)} = \sum_{i=1}^s \left\lfloor \frac{a_i + t}{m} \right\rfloor Q_i + \left\lfloor \frac{-rt}{m} \right\rfloor Q_\infty.$$

Since

$$\mathcal{L}(\sum_{i=1}^{s} a_i P_i) = \bigoplus_{t=0}^{m-1} \mathcal{L}\left(\left[\sum_{i=1}^{s} a_i P_i + (y^t)\right]\Big|_{K(x)}\right) y^t,$$

by Theorem 3.1.4, we have

$$\ell\left(\sum_{i=1}^{s} a_i P_i\right) = \sum_{t=0}^{m-1} \ell\left(\sum_{i=1}^{s} \left\lfloor \frac{a_i+t}{m} \right\rfloor Q_i + \left\lfloor \frac{-rt}{m} \right\rfloor Q_\infty\right),$$

$$\ell\left(\sum_{i=1}^{s} (a_i-1) P_i\right) = \sum_{t=0}^{m-1} \ell\left(\sum_{i=1}^{s} \left\lfloor \frac{a_i-1+t}{m} \right\rfloor Q_i + \left\lfloor \frac{-rt}{m} \right\rfloor Q_\infty\right).$$

By Lemma 1.1.45, $(a_1, \ldots, a_s)$ is a pure gap at $P_1, \ldots, P_s$ if and only if

$$\ell\left(\sum_{i=1}^{s} \left\lfloor \frac{a_i+t}{m} \right\rfloor Q_i + \left\lfloor \frac{-rt}{m} \right\rfloor Q_\infty\right) - \ell\left(\sum_{i=1}^{s} \left\lfloor \frac{a_i-1+t}{m} \right\rfloor Q_i + \left\lfloor \frac{-rt}{m} \right\rfloor Q_\infty\right) = 0$$

for all $t \in \{0, \ldots, m-1\}$. Since $\mathbb{F}_q(x)$ has genus 0, this happens if and only if, for all $t \in \{0, \ldots, m-1\}$, either

$$\sum_{i=1}^{s} \left\lfloor \frac{a_i+t}{m} \right\rfloor + \left\lfloor \frac{-rt}{m} \right\rfloor < 0$$

or

$$\sum_{i=1}^{s} \left\lfloor \frac{a_i+t}{m} \right\rfloor + \left\lfloor \frac{-rt}{m} \right\rfloor \geq 0 \quad \text{and} \quad \sum_{i=1}^{s} \left\lfloor \frac{a_i+t}{m} \right\rfloor = \sum_{i=1}^{s} \left\lfloor \frac{a_i-1+t}{m} \right\rfloor.$$

□

**Proposition 3.1.6.** *Let $s \leq r$, then an $(s+1)$-tuple $(a_0, a_1, \ldots, a_s) \in \mathbb{N}^{s+1}$ is a pure gap at $P_\infty, P_1, \ldots, P_s$ if and only if, for every $t \in \{0, \ldots, m-1\}$, exactly one of the following two conditions is satisfied:*

*i)* $\sum_{i=1}^{s} \left\lfloor \frac{a_i+t}{m} \right\rfloor + \left\lfloor \frac{a_0-rt}{m} \right\rfloor < 0$*;*

*ii)* $\sum_{i=1}^{s} \left\lfloor \frac{a_i+t}{m} \right\rfloor + \left\lfloor \frac{a_0-rt}{m} \right\rfloor \geq 0$*,* $\left\lfloor \frac{a_0-rt}{m} \right\rfloor = \left\lfloor \frac{a_0-1-rt}{m} \right\rfloor$ *and* $\left\lfloor \frac{a_i+t}{m} \right\rfloor = \left\lfloor \frac{a_i-1+t}{m} \right\rfloor$ *for* $i = 1, \ldots, s$*.*

*Proof.* The proof is omitted being analogous to the proof of Proposition 3.1.5. □

We now present three families of pure gaps at two points for $m \equiv 1 \pmod r$.

**Proposition 3.1.7.** *Suppose that $m = ur + 1$ for some integer $u$. Then* *i)* $((r-1)m-2r,1)$ *is a pure gap at* $P_\infty, P_1$*;*

*ii)* $((r-2)m-r,b)$*, with* $b \in \{1,\dots,u+1\}$ *are pure gaps at* $P_\infty, P_1$*;*

*iii)* $((r-3)m+1+\alpha,1+\beta)$*, with* $\alpha \in \{0,\dots,2u-1\}$ *and* $\beta \in \{0,\dots,u-1\}$ *are pure gaps at* $P_1, P_2$*.*

*Proof.* Let $a = rm-m-2r$ and $t \in \{0,\dots,m-1\}$. We have $\lfloor \frac{a-rt}{m} \rfloor \neq \lfloor \frac{a-1-rt}{m} \rfloor$ if and only if $m$ divides $a-rt = (r-1)m-r(t+2)$, that is $t = m-2$. Also, $t = m-2$ implies $\left\lfloor \frac{a-qt}{q^\ell+1} \right\rfloor = -1$. For any $t \in \{0,\dots,m-2\}$ we have $\lfloor \frac{1+t}{m} \rfloor = \lfloor \frac{t}{m} \rfloor = 0$. We conclude that for any $t \in \{0,\dots,m-2\}$ either $\lfloor \frac{a-rt}{m} \rfloor + \lfloor \frac{1+t}{m} \rfloor < 0$ or $\lfloor \frac{a-rt}{m} \rfloor + \lfloor \frac{1+t}{m} \rfloor = \lfloor \frac{a-1-rt}{m} \rfloor + \lfloor \frac{t}{m} \rfloor$. For $t = m-1$, $\lfloor \frac{a-rt}{m} \rfloor + \lfloor \frac{1+t}{m} \rfloor = -2+1 = -1 < 0$. By Proposition 3.1.6, $(a,1)$ is a pure gap at $P_\infty, P_1$.

Now let $a = rm-2m-r$, $b \in \{1,\dots,u+1\}$, and $t \in \{0,\dots,m-1\}$. We have that $\lfloor \frac{b+t}{m} \rfloor \in \{0,1\}$, and $\lfloor \frac{b+t}{m} \rfloor = 1$ if and only if $t+b \geq m$, that is $t \in \{m-b,\dots,m-1\}$. In this case,

$$\left\lfloor \frac{a-rt}{m} \right\rfloor = \left\lfloor \frac{rm-2m-r-rt}{m} \right\rfloor = -2 + \left\lfloor \frac{rm-r-rt}{m} \right\rfloor = -2,$$

since $0 \leq rm-r-rt \leq r(b-1) \leq ru < m$. Hence, for all $t \in \{m-b,\dots,m-1\}$,

$$\left\lfloor \frac{a-rt}{m} \right\rfloor + \left\lfloor \frac{b+t}{m} \right\rfloor = -2+1 < 0.$$

For $t \in \{0,\dots,m-b-1\}$, we have that

$$\left\lfloor \frac{a-rt}{m} \right\rfloor + \left\lfloor \frac{b+t}{m} \right\rfloor = \left\lfloor \frac{a-rt}{m} \right\rfloor = \left\lfloor \frac{a-1-rt}{m} \right\rfloor = \left\lfloor \frac{a-1-rt}{m} \right\rfloor + \left\lfloor \frac{b-1+t}{m} \right\rfloor.$$

By Proposition 3.1.6, $(a,b)$ is a pure gap at $P_\infty, P_1$.

Finally let $t \in \{0,\dots,m-1\}$ and $(a_\alpha, b_\beta) = ((r-3)m+1+\alpha, 1+\beta)$ with $\alpha \in \{0,\dots,2u-1\}$ and $\beta \in \{0,\dots,u-1\}$. Note that $\lfloor \frac{a_\alpha+t}{m} \rfloor \neq \lfloor \frac{a_\alpha-1+t}{m} \rfloor$ if and only if $t = m-1-\alpha$, and $\lfloor \frac{b_\alpha+t}{m} \rfloor \neq \lfloor \frac{b_\alpha-1+t}{m} \rfloor$ if and only if $t = m-1-\beta$. Therefore,

$$\left\lfloor \frac{a_\alpha+t}{m} \right\rfloor + \left\lfloor \frac{b_\alpha+t}{m} \right\rfloor \neq \left\lfloor \frac{a_\alpha-1+t}{m} \right\rfloor + \left\lfloor \frac{b_\alpha-1+t}{m} \right\rfloor$$

if and only if $t = m-1-\alpha$ or $t = m-1-\beta$.

Suppose $t = m-1-\alpha$. Then

$$\left\lfloor \frac{-rt}{m} \right\rfloor = -r + \left\lfloor \frac{r(1+\alpha)}{m} \right\rfloor = \begin{cases} -r, & \alpha \leq u-1 \\ -r+1, & \alpha \geq u \end{cases},$$

$$\left\lfloor \frac{a_\alpha+t}{m} \right\rfloor = r-2, \quad \left\lfloor \frac{b_\beta+t}{m} \right\rfloor = 1 + \left\lfloor \frac{\beta-\alpha}{m} \right\rfloor = \begin{cases} 1, & \text{for } \beta \geq \alpha \\ 0, & \text{for } \beta < \alpha \end{cases}.$$

If $\alpha \geq u$, then

$$\left\lfloor \frac{-rt}{m} \right\rfloor + \left\lfloor \frac{a_\alpha + t}{m} \right\rfloor + \left\lfloor \frac{b_\beta + t}{m} \right\rfloor = (-r+1) + (r-2) + 0 < 0;$$

if $\alpha \leq u-1$, then

$$\left\lfloor \frac{-rt}{m} \right\rfloor + \left\lfloor \frac{a_\alpha + t}{m} \right\rfloor + \left\lfloor \frac{b_\beta + t}{m} \right\rfloor \leq -r + (r-2) + 1 < 0.$$

Suppose $t = m-1-\beta$. Then

$$\left\lfloor \frac{-rt}{m} \right\rfloor = -r + \left\lfloor \frac{r(1+\beta)}{m} \right\rfloor = -r,$$
$$\left\lfloor \frac{a_\alpha + t}{m} \right\rfloor = r - 2 + \left\lfloor \frac{\alpha - \beta}{m} \right\rfloor = \begin{cases} r-3, & \text{for } \alpha < \beta \\ r-2, & \text{for } \alpha \geq \beta \end{cases}, \qquad \left\lfloor \frac{b_\beta + t}{m} \right\rfloor = 1.$$

Hence,

$$\left\lfloor \frac{-rt}{m} \right\rfloor + \left\lfloor \frac{a_\alpha + t}{m} \right\rfloor + \left\lfloor \frac{b_\beta + t}{m} \right\rfloor \leq -r + (r-2) + 1 < 0.$$

The thesis follows from Proposition 3.1.5. □

We provide two families of pure gaps at many points for $m \equiv 1 \pmod r$.

**Proposition 3.1.8.** *Suppose that $m = ur + 1$ for some integer $u$, $s < r$, and $\alpha_i \in \{0, \dots, (s+1-i)u - 1\}$ for $i = 1, \dots, s$. Then $(a_1, \dots, a_s) = ((r-s-1)m + 1 + \alpha_1, 1 + \alpha_2, \dots, 1 + \alpha_s)$ is a pure gap at $P_1, \dots, P_s$.*

*Proof.* Suppose there exist $t \in \{0, \dots, m-1\}$ and $j \in \{1, \dots, s\}$ such that $\left\lfloor \frac{a_j + t}{m} \right\rfloor \neq \left\lfloor \frac{a_j - 1 + t}{m} \right\rfloor$. Thus $t = m - 1 - \alpha_j$. Let $h \in \{0, \dots, r-2\}$ be such that $hu \leq \alpha_j < (h+1)u$. We have

$$\left\lfloor \frac{-rt}{m} \right\rfloor = \left\lfloor \frac{-r(m-1-\alpha_j)}{m} \right\rfloor = -r + \left\lfloor \frac{r(1+\alpha_j)}{m} \right\rfloor = -r + h,$$
$$\left\lfloor \frac{a_1 + t}{m} \right\rfloor = \left\lfloor \frac{(r-s-1)m + 1 + \alpha_1 + m - 1 - \alpha_j}{m} \right\rfloor = \begin{cases} r-s, & \alpha_1 \geq \alpha_j \\ r-s-1, & \alpha_1 < \alpha_j \end{cases},$$

and, for $i > 1$,

$$\left\lfloor \frac{a_i + t}{m} \right\rfloor = \left\lfloor \frac{1 + \alpha_i + m - 1 - \alpha_j}{m} \right\rfloor = \begin{cases} 0, & \alpha_i < \alpha_j \\ 1, & \alpha_i \geq \alpha_j \end{cases}.$$

Since

$$\begin{aligned} |\{i \in \{2,\dots,s\} : \alpha_i \geq \alpha_j\}| &\leq s-1-|\{i \in \{2,\dots,s\} : (s+1-i)h-1 < uh\}| \\ &= s-1-h, \end{aligned}$$

this implies that

$$\left\lfloor \frac{-rt}{m} \right\rfloor + \left\lfloor \frac{a_1+t}{m} \right\rfloor + \sum_{i=2}^{m} \left\lfloor \frac{a_i+t}{m} \right\rfloor \leq (-r+h)+(r-s)+(s-1-h) < 0.$$

Hence, the thesis follows by Proposition 3.1.5. □

**Proposition 3.1.9.** *Suppose that $m = ur+1$ for some integer $u$, $s < r-1$, $\alpha \in \{0,\dots,s\}$, and $\beta_i \in \{0,\dots,iu-1\}$ for $i \in \{1,\dots,s\}$. Then $(a_0,a_1,\dots,a_s) = ((r-s-1)m-r+\alpha, 1+\beta_1,\dots,1+\beta_s)$ is a pure gap at $P_\infty, P_1,\dots,P_s$.*

*Proof.* Let $t \in \{0,\dots,m-2\}$, so that $t = ku+z$ with $k \in \{0,\dots,r-1\}$ and $z \in \{0,\dots,u-1\}$.

Suppose $\lfloor \frac{a_0-rt}{m} \rfloor \neq \lfloor \frac{a_0-1-rt}{m} \rfloor$. Then $m \mid (a_0-rt) = (r-s-k-1)m+\alpha+k-r(z+1)$. Since $|\alpha+k-r(z+1)| < m$, this implies $\alpha+k = r(z+1)$, whence $r \mid (\alpha+k)$. As $0 \leq \alpha, k \leq r-1$, and $r(z+1) > 0$, we have that $\alpha+k = r$ and $z = 0$. Hence, $t = m-1-\alpha u$. Then

$$\left\lfloor \frac{a_0-rt}{m} \right\rfloor = r-s-k-1 = \alpha-s-1.$$

Also, $1+\beta_i+t \leq m-1-(\alpha-j)u$ for all $i$. Thus $a_j+t \leq m-1$ for all $j \in \{1,\dots,\alpha\}$, so

$$\sum_{i=1}^{s} \left\lfloor \frac{a_i+t}{m} \right\rfloor \leq s-\alpha.$$

Therefore,

$$\sum_{i=1}^{s} \left\lfloor \frac{a_i+t}{m} \right\rfloor + \left\lfloor \frac{a_0-rt}{m} \right\rfloor < 0.$$

Now suppose $\lfloor \frac{a_i+t}{m} \rfloor \neq \left\lfloor \frac{a_j-1+t}{m} \right\rfloor$ for some $j \in \{1,\dots,s\}$. Since $1 \leq a_j+t < 2m$, this implies $t = m-a_j = m-1-\beta_j$. Let $h \in \{0, r-3\}$ be such that $hu \leq \beta_j < (h+1)u$. We have

$$\left\lfloor \frac{a_0-rt}{m} \right\rfloor = -s-1+\left\lfloor \frac{\alpha+r\beta_j}{m} \right\rfloor = -s-1+h$$

and, for $i > 0$,

$$\left\lfloor \frac{a_i + t}{m} \right\rfloor = 1 + \left\lfloor \frac{\beta_i - \beta_j}{m} \right\rfloor = \begin{cases} 0, & \beta_i < \beta_j \\ 1, & \beta_i \geq \beta_j \end{cases}.$$

Since

$$|\{i \in \{1, \ldots, s\} : \beta_i \geq \beta_j\}| \leq s - |\{i \in \{1, \ldots, s\} : ih - 1 < uh\}| = s - h,$$

this implies that

$$\left\lfloor \frac{a_0 - rt}{m} \right\rfloor + \sum_{i=1}^{m} \left\lfloor \frac{a_i + t}{m} \right\rfloor \leq (-s - 1 + h) + (s - h) < 0.$$

Finally, let $t = m - 1$. Then $\left\lfloor \frac{a_0 - rt}{m} \right\rfloor = -s - 1$ and $\left\lfloor \frac{a_i + t}{m} \right\rfloor = 1$ for all $i > 0$. Hence,

$$\left\lfloor \frac{a_0 - rt}{m} \right\rfloor + \sum_{i=1}^{m} \left\lfloor \frac{a_i + t}{m} \right\rfloor = (-s - 1) + s < 0.$$

The thesis follows by Proposition 3.1.6. □

By means of Theorem 1.1.46, the results on pure gaps of this section can be used in order to obtain AG codes with good parameters.

**Remark 3.1.10.** *For a Kummer extension $y^m = f(x)$, where $m = ur + 1$ and $s \leq r - 1$, consider the pure gaps $(a_1, \ldots, a_s) = ((r - s - 1)m + 1, 1, \ldots, 1)$ and $(b_1, \ldots, b_s) = ((r - s - 1)m + su, (s - 1)u, \ldots, u)$. Define the divisors $G = \sum_{i=1}^{s}(a_i + b_i - 1)P_i$ and $D$ as the sum of $n$ rational places of $F$ different from $P_1, \ldots, P_s$. Consider the $[n, k, d]$-code $C_\Omega(D, G)$.*

*Suppose $2g - 2 < \deg G < n$, then $k = n + g - 1 - \deg G$. Since $F$ has genus $g = ur(r-1)/2$ we have by Proposition* 3.1.8 *and Theorem* 1.1.46 *that the Singleton defect $\delta = n + 1 - k - d$ satisfies*

$$\delta \leq \frac{ur(r-1) - us(s+1)}{2}.$$

**Remark 3.1.11.** *For a Kummer extension $y^m = f(x)$, where $m = ur + 1$ and $s \leq r - 2$ consider the pure gaps $(a_0, a_1, \ldots, a_s) = ((r - s - 1)m - r, 1, \ldots, 1)$ and $(b_0, b_1, \ldots, b_s) = ((r - s - 1)m - r + s, u, \ldots, su)$. Define the divisors $G = (a_0 + b_0 - 1)P_\infty + \sum_{i=1}^{s}(a_i + b_i - 1)P_i$ and $D$ as the sum of $n$ rational places of $F$ different from $P_\infty, P_1, \ldots, P_s$ and consider the $[n, k, d]$-code $C_\Omega(D, G)$.*

Table 3.1: Results from Example 3.1.12

| $q^2$ | $s$ | $n$ | $k$ | $d \geq$ | improvement on $d$ compared with [89] |
|---|---|---|---|---|---|
| 16 | 1 | 64 | 48 | 12 | 1 |
| 16 | 2 | 63 | 55 | 6 | 0 |
| 25 | 1 | 125 | 97 | 20 | 1 |
| 25 | 2 | 124 | 106 | 12 | 1 |
| 49 | 2 | 342 | 295 | 30 | 3 |
| 49 | 3 | 341 | 307 | 20 | 1 |
| 64 | 1 | 512 | 430 | 56 | 1 |
| 64 | 2 | 511 | 445 | 42 | 3 |
| 64 | 3 | 510 | 459 | 30 | 2 |
| 64 | 4 | 509 | 472 | 20 | 0 |
| 81 | 3 | 727 | 656 | 42 | 3 |
| 81 | 4 | 726 | 671 | 30 | 0 |

*Suppose* $2g-2 < \deg G < n$, *then* $k = n + g - 1 - \deg G$. *Since* $F$ *has genus* $g = ur(r-1)/2$ *we have by Proposition* 3.1.9 *and Theorem* 1.1.46 *that the Singleton defect* $\delta$ *satisfies*

$$\delta \leq \frac{ur(r-1) - us(s+1)}{2} - s - 1.$$

We illustrate the results obtained with Hermitian codeson many points.

**Example 3.1.12.** *We apply Remark* 3.1.10 *to construct* $[n,k,d]$*-codes* $C_\Omega(D,G)$ *from the Hermitian function field* $\mathbb{F}_q(\mathcal{H}_q)$. *In this case we have* $r = q, u = 1, 1 \leq s \leq q-1$ *and* $\deg G = 2(q-s-1)(q+1) + s(s+1)/2$. *We choose* $s$ *such that* $2g-2 < \deg G < n$ *with* $n = q^3 + 1 - s$. *Then*

$$k = n + g - 1 - \deg G = q^3 - \frac{3}{2}q^2 + \Big(2s - \frac{1}{2}\Big)q - \frac{s^2 - s}{2} + 2,$$
$$d \geq \deg G - (2g-2) + s + \sum_{i=1}^{s}(b_i - a_i) = q^2 - (2s-1)q + s^2 - s.$$

Table 3.1 lists some AG codes from Example 3.1.12 with the same or better parameters with respect to the corresponding ones in the MinT's Tables [89].

Table 3.2: Parameters of the constructed codes

| Code | $n$ | $d$ | $m$ | $k$ |
|---|---|---|---|---|
| $C$<br>(Sect. 3.2.1) | $q^8-q^6+q^5-q^3$ | $d^*$ | $[q^2-1, q^5-q^3-1]$ | $m(q^3+1)+1-g$ |
| | | | $[2, q^2-1]$ | $k_0$ |
| $\bar{C}$<br>(Sect. 3.2.2) | $q^8-q^6+q^5$<br>$-(s+1)q^3$,<br>with $s>0$ | $\geq d^*$ | $\left[\frac{q^5-2q^3+q^2-1}{(s+1)q^3+1}, \frac{q^8-q^6+q^5-(s+1)q^3-1}{(s+1)q^3+1}\right]$ | $m(s+1)q^3+m+1-g$ |
| | | | $\left[2, \frac{q^8-q^6+q^5-(s+1)q^3}{(s+1)q^3(q^3+1)}\right]$ | $\bar{k}_0$ |
| $\tilde{C}$<br>(Sect. 3.2.2) | $q^8-q^6+q^5$<br>$-(s+1)q^3+1$ | $d^*$ | $\left[\frac{q^5-2q^3+q^2-1}{(s+1)q^3}, \frac{q^5-q^3+q^2}{s+1}-1\right]$ | $m(s+1)q^3+1-g$ |
| | | | $\left[2, \frac{q^5-q^3+q^2-(s+1)}{(s+1)(q^3+1)}\right]$ | $\tilde{k}_0$ |

## 3.2 Multi-Point AG Codes on the GK Maximal Curves

Curves with many $\mathbb{F}_q$-rational places with respect to their genus may give to AG codes with good parameters. For instance, AG codes with good parameters have been constructed from the Hermitian curve or the Suzuki curve; see [77, 87]. One- and two-point AG codes from the GK curve have been recently investigated by Fanali and Giulietti [37], and by Castellanos and Tizziotti [22].

In this Section we construct AG codes $C_{\mathcal{L}}(D,G)$ associated to the GK curve $\mathcal{GK}_q$ from divisors $G$ supported at many points. Choosing $G$ to be invariant under a large automorphism group of the curve, we obtain large automorphism groups for the code. The results are summarized in Tables 3.2 and 3.3, which lists the parameters of the $[n,k,d]_{q^6}$-codes constructed in the section. They depend on non-negative integers $m$, $s$, and $r := \gcd\left(s, \frac{q^2-q+1}{\gcd(3,q+1)}\right)$.

We make use of the results presented in Section 1.1.3 about the AG codes and in Section 1.2.1 about the GK curves.

Table 3.3: Automorphism groups of the constructed codes

| Code | $m$ | Automorphism group |
|---|---|---|
| $C$<br>(Sect. 3.2.1) | $[2, q^2-1]$ | $(\mathrm{Aut}(\mathcal{GK}_q) \rtimes \mathrm{Aut}(\mathbb{F}_{q^6})) \rtimes \mathbb{F}^*_{q^6}$ |
| $\bar{C}$<br>(Sect. 3.2.2) | $\left[2, \frac{q^8-q^6+q^5-(s+1)q^3}{(s+1)q^3(q^3+1)}\right]$ | $\big((\mathrm{SU}(3,q) \times C_r) \rtimes \mathrm{Aut}(\mathbb{F}_{q^6})\big) \rtimes \mathbb{F}^*_{q^6}$ |
| $\tilde{C}$<br>(Sect. 3.2.2) | $\left[2, \frac{q^5-q^3+q^2-(s+1)}{(s+1)(q^3+1)}\right]$ | $\big(((Q_{q^3} \rtimes H_{q^2-1}) \times C_{q^2-q+1}) \rtimes \mathrm{Aut}(\mathbb{F}_{q^6})\big) \rtimes \mathbb{F}^*_{q^6}$,<br>if $s = 0$ |
| | | $\big(((Q_{q^3} \rtimes H_{q^2-1}) \times C_{q^2-q+1}) \rtimes \mathrm{Aut}(\mathbb{F}_{q^6})\big) \rtimes \mathbb{F}^*_{q^6}$,<br>if $s > 0$ and $p \nmid m$ |

### 3.2.1 AG codes on the GK curves

Let $m \in \mathbb{N}$ and consider the sets

$$\mathcal{G} := \mathcal{GK}_q(\mathbb{F}_{q^2}), \quad \mathcal{D} := \mathcal{GK}_q(\mathbb{F}_{q^6}) \setminus \mathcal{G}.$$

Note that $\mathcal{G}$ is the intersection of $\mathcal{GK}_q$ with the plane $Z = 0$. Define the $\mathbb{F}_{q^6}$-divisors

$$G := \sum_{P \in \mathcal{G}} mP \quad \text{and} \quad D := \sum_{P \in \mathcal{D}} P,$$

which have degree $m(q^3+1)$ and $q^8 - q^6 + q^5 - q^3$, respectively. Denote by $C := C_{\mathcal{L}}(D, G)$ the associated functional AG code over $\mathbb{F}_{q^6}$ having length $n = q^8 - q^6 + q^5 - q^3$, dimension $k$, and minimum distance $d$. The designed minimum distance of $C$ is

$$d^* = n - \deg G = q^8 - q^6 + q^5 - q^3 - m(q^3+1).$$

**Lemma 3.2.1.** *There exist exactly $q^5 - q^3$ planes $\pi_a : X = a$, $a \in \mathbb{F}_{q^6}$, containing $q^3+1$ distinct $\mathbb{F}_{q^6}$-rational points of $\mathcal{GK}_q$. Their affine points give rise to a partition of $\mathcal{GK}_q(\mathbb{F}_{q^6}) \setminus \mathcal{GK}_q(\mathbb{F}_{q^2})$.*

*Proof.* Let $a \in \mathbb{F}_{q^6} \setminus \mathbb{F}_{q^2}$ be such that $\mathcal{GK}_q$ contains an $\mathbb{F}_{q^6}$-rational point $(a, b, c)$. Then $b, c \neq 0$, and $\pi_a \cap \mathcal{GK}_q$ has exactly $q^3 + 1$ affine distinct points, namely

$\pi_a \cap \mathcal{GK}_q = \{(a, \xi b, \eta c) \mid \xi^{q+1} = \eta^{q^2-q+1} = 1\}$. Now let $a \in \mathbb{F}_{q^2}$. Then $(a, b, c) \in \mathcal{GK}_q$ if and only if $b, c \in \mathbb{F}_{q^2}$ satisfy $b^{q+1} = a^q + a$ and $c = 0$. In particular, $\pi_a \cap \mathcal{GK}_q$ has either 1 or $q + 1$ affine points, according to $a^q + a = 0$ or $a^q + a \neq 0$, respectively. Therefore the number of planes $\pi_a$ intersecting $\mathcal{GK}_q$ in exactly $q^3 + 1$ $\mathbb{F}_{q^6}$-rational points is $|\mathrm{supp}(D)|/|\pi_a \cap \mathcal{GK}_q| = \frac{q^8-q^6+q^5-q^3}{q^3+1} = q^5 - q^3$. □

Now we show that the designed minimum distance is attained by $C$.

**Proposition 3.2.2.** *When $d^* > 0$, $C$ attains the designed minimum distance $d^*$.*

*Proof.* Take $m$ distinct elements $a_1 \ldots, a_m \in \mathbb{F}_{q^6} \backslash \mathbb{F}_{q^2}$ such that $|\pi_a \cap \mathcal{GK}_q| = q^3+1$, and let

$$f := \prod_{i=1}^{m} \left( \frac{x - a_i}{z} \right). \qquad (3.5)$$

Then the pole divisor of $f$ is $(f)_\infty = G$, thus $f \in \mathcal{L}(G)$. The weight of $e_D(f)$ is

$$w(e_D(f)) = n - m(q^3 + 1) = d^*.$$

□

The dimension of $C$ can be explicitly computed.

**Proposition 3.2.3.** *If $q^2 - 1 \leq m \leq q^5 - q^3 - 1$, then*

$$k = m(q^3 + 1) - \frac{1}{2}(q^5 - 2q^3 + q^2 - 2).$$

*Proof.* Since $n > \deg G > 2g - 2$, then by the Riemann-Roch Theorem we obtain $k = \deg G + 1 - g$. □

**Proposition 3.2.4.** *The code $C$ is monomially equivalent to the one-point code $C_\mathcal{L}(D, G')$, where $G' = m(q^3 + 1)P_\infty$.*

*Proof.* By direct checking, $G = G' + (z^m)$, and hence $\mathcal{L}(G') = \{f \cdot z^m \mid f \in \mathcal{L}(G)\}$. The codeword of $C_\mathcal{L}(D, G')$ associated to $f \cdot z^m$ is

$$((f z^m)(P_1), \ldots, (f z^m)(P_n)) = (f(P_1), \ldots, f(P_n)) \cdot M,$$

where $M$ is the diagonal matrix with diagonal entries $z(P_1)^m, \ldots, z(P_n)^m \in \mathbb{F}_{q^6}$. This means that $M$ defines a monomial equivalence between $C$ and $C_\mathcal{L}(D, G')$. □

**Corollary 3.2.5.** *If $1 \le m \le q^2-2$, then the dimension $k$ of $C$ is equal to*

$$k_0 = \begin{cases} \frac{1}{6}(m+1)(m+2)(m+3) & 1 \le m \le q-1, \\ \frac{1}{6}(q+1)(3m^2-3mq+9m+q^2-4q+6) & q \le m \le q^2-q, \\ \frac{1}{6}\big(-m^3+3m^2q^2-3mq^4+6mq^3+7m & \\ \quad +q^6-3q^5+6q^3-4q^2+6\big) & q^2-q+1 \le m \le q^2-2. \end{cases}$$

*Proof.* By the assumptions on $m$, $\deg(G) < n$; hence, $k = \ell(G)$ by Proposition 1.1.38. From Proposition 3.2.4, $k = \ell(G')$ with $G' = m(q^3+1)P_\infty$. This means that $k$ is equal to the number $k_0$ of non-gaps $h \in H(P_\infty)$ at $P_\infty$ satisfying $h \le mq^3$. From [50, Proposition 2], $k_0$ is the number of triples $(j_1, j_2, j_3) \in \mathbb{N}^3$ such that

$$j_2 \le q^2-q, \quad j_3 \le q-1, \quad j_1(q^3-q^2+q) + j_2q^3 + j_3(q^3+1) \le m(q^3+1).$$

Then

$$k_0 = \sum_{j_3=0}^{\min\{m,q-1\}} \sum_{j_2=0}^{\min\{m-j_3,q^2-q\}} \left( \left\lfloor \frac{(q^3+1)(m-j_3)-q^3j_2}{q^3-q^2+q} \right\rfloor + 1 \right)$$

$$= \sum_{j_3=0}^{\min\{m,q-1\}} \sum_{j_2=0}^{\min\{m-j_3,q^2-q\}} \left( \left\lfloor \frac{m-j_3-j_2}{q} + \frac{j_2}{q^3-q^2+q} \right\rfloor + m - j_3 - j_2 + 1 \right).$$

We have $\frac{j_2}{q^3-q^2+q} < \frac{1}{q}$. Hence, if $q \mid (m-j_3-j_2)$, then $\left\lfloor \frac{m-j_3-j_2}{q} + \frac{j_2}{q^3-q^2+q} \right\rfloor = \frac{m-j_3-j_2}{q}$; if $q \nmid (m-j_3-j_2)$, then $\frac{m-j_3-j_2}{q} + \frac{j_2}{q^3-q^2+q} < \frac{m-j_3-j_2}{q} + \frac{1}{q} \le \left\lceil \frac{m-j_3-j_2}{q} \right\rceil$. In any case

$$\left\lfloor \frac{m-j_3-j_2}{q} + \frac{j_2}{q^3-q^2+q} \right\rfloor = \left\lfloor \frac{m-j_3-j_2}{q} \right\rfloor$$

and therefore

$$k_0 = \sum_{j_3=0}^{\min\{m,q-1\}} \sum_{j_2=0}^{\min\{m-j_3,q^2-q\}} \left( \left\lfloor \frac{m-j_3-j_2}{q} \right\rfloor + m - j_3 - j_2 + 1 \right).$$

1. Case $1 \le m \le q-1$. Then

$$k_0 = \sum_{j_3=0}^{m} \sum_{j_2=0}^{m-j_3} (m-j_3-j_2+1) = \frac{(m+1)(m+2)(m+3)}{6}.$$

2. Case $q \leq m \leq q^2 - q$. Let $m - j_3 = u_{j_3} q + v_{j_3}$ with $0 \leq u_{j_3} \leq q-1$ and $0 \leq v_{j_3} \leq q-1$. Then

$$\sum_{j_2=0}^{m-j_3} \left\lfloor \frac{m-j_3-j_2}{q} \right\rfloor = (v_{j_3}+1)u_{j_3} + q \sum_{i=0}^{u_{j_3}-1} i = (v_{j_3}+1)u_{j_3} + q\frac{u_{j_3}(u_{j_3}-1)}{2}$$

and

$$k_0 = \sum_{j_3=0}^{q-1} \left( (v_{j_3}+1)u_{j_3} + q\frac{u_{j_3}(u_{j_3}-1)}{2} + \sum_{j_2=0}^{m-j_3} (m-j_3-j_2+1) \right)$$

$$= \sum_{j_3=0}^{q-1} \left( (v_{j_3}+1)u_{j_3} + q\frac{u_{j_3}(u_{j_3}-1)}{2} + \frac{(m-j_3+1)(m-j_3+2)}{2} \right).$$

Let $m = xq + y$ with $1 \leq x \leq q-1$ and $0 \leq y \leq q-1$. Then

$$k_0 = \sum_{j_3=0}^{y} \left( (y-j_3+1)x + q\frac{x(x-1)}{2} + \frac{(m-j_3+1)(m-j_3+2)}{2} \right)$$

$$+ \sum_{j_3=y+1}^{q-1} \left( (q+y-j_3+1)(x-1) + q\frac{(x-1)(x-2)}{2} + \frac{(m-j_3+1)(m-j_3+2)}{2} \right),$$

where the second summation is substituted by zero when $y = q-1$. Then

$$k_0 = x\frac{(y+1)(y+2)}{2} + q\frac{x(x-1)}{2}(y+1) + \frac{(m+1)(m+2)(m+3)}{6}$$

$$+(x-1)\frac{(q+y+2)(q-y-1)}{2} + q\frac{(x-1)(x-2)}{2}(q-1-y)$$

$$-\frac{(m-q+1)(m-q+2)(m-q+3)}{6}.$$

From $y = m - xq$ we obtain

$$k_0 = \frac{(q+1)(3m^2 - 3mq + 9m + q^2 - 4q + 6)}{6}.$$

3. Case $q^2 - q + 1 \leq m \leq q^2 - 2$, that is $m = (q-1)q + \alpha$ with $1 \leq \alpha \leq q-2$. Then

$$k_0 = \sum_{j_3=0}^{m-q^2+q} \sum_{j_2=0}^{q^2-q} \left( \left\lfloor \frac{m-j_3-j_2}{q} \right\rfloor + m - j_3 - j_2 + 1 \right)$$

$$+\sum_{j_3=m-q^2+q+1}^{q-1}\sum_{j_2=0}^{m-j_3}\left(\left\lfloor\frac{m-j_3-j_2}{q}\right\rfloor+m-j_3-j_2+1\right).$$

As above, let $m-j_3=u_{j_3}q+v_{j_3}$ with $0\leq u_{j_3}\leq q-1$ and $0\leq v_{j_3}\leq q-1$. Then

$$k_2:=\sum_{j_3=m-q^2+q+1}^{q-1}\sum_{j_2=0}^{m-j_3}\left(\left\lfloor\frac{m-j_3-j_2}{q}\right\rfloor+m-j_3-j_2+1\right)$$

$$=\sum_{j_3=m-q^2+q+1}^{q-1}\left((v_{j_3}+1)u_{j_3}+q\frac{u_{j_3}(u_{j_3}-1)}{2}+\sum_{j_2=0}^{m-j_3}(m-j_3-j_2+1)\right).$$

We have $j_3\in[m-q^2+q+1,q-1]$ if and only if $u_{j_3}=q-2$ and $v_{j_3}\in[\alpha+1,q-1]$. Therefore,

$$k_2=\sum_{v_{j_3}=\alpha+1}^{q-1}\left((v_{j_3}+1)(q-2)+q\frac{(q-2)(q-3)}{2}\right)+\sum_{j_3=m-q^2+q+1}^{q-1}\sum_{j_2=0}^{m-j_3}(m-j_3-j_2+1)$$

$$=\frac{(q+\alpha+2)(q-\alpha-1)(q-2)}{2}+\frac{(q-1-\alpha)q(q-2)(q-3)}{2}$$

$$+\frac{(q^2-q)(q^2-q+1)(q^2-q+2)}{6}-\frac{(m-q+1)(m-q+2)(m-q+3)}{6}$$

$$=\frac{(q^2-m-1)(m^2+mq^2-m+q^4-3q^3+4q^2+3q-6)}{6}.$$

$$k_1:=\sum_{j_3=0}^{\alpha}\sum_{j_2=0}^{q^2-q}\left(\left\lfloor\frac{m-j_3-j_2}{q}\right\rfloor+m-j_3-j_2+1\right)$$

$$=\sum_{j_3=0}^{\alpha}\sum_{i=\alpha-j_3}^{q^2-q+\alpha-j_3}\left\lfloor\frac{i}{q}\right\rfloor+\sum_{j_3=0}^{\alpha}\sum_{j_2=0}^{q^2-q}(m-j_3-j_2+1)$$

$$=\sum_{j_3=0}^{\alpha}\left((q-1)(\alpha-j_3+1)+\frac{q(q-1)(q-2)}{2}+\frac{(q^2-q+1)(m-2j_3+\alpha+2)}{2}\right)$$

$$=\frac{(q-1)(\alpha+1)(\alpha+2)}{2}+\frac{(\alpha+1)q(q-1)(q-2)}{2}+\frac{(q^2-q+1)(m+2)(\alpha+1)}{2}$$

$$=\frac{q(m-q^2+q+1)(mq+q+1)}{2}.$$

Finally

$$k_0=k_1+k_2=\frac{-m^3+3m^2q^2-3mq^4+6mq^3+7m+q^6-3q^5+6q^3-4q^2+6}{6}.$$

□

Let $H$ be the $\mathbb{F}_{q^2}$-divisor defined by $H = \sum_{P \in \mathcal{G}} P$, that is, $G = mH$.

**Proposition 3.2.6.** *If $m < q^5 - q^3 + q^2 - 2$, then the codes $C_\Omega(D, G)$ and $C_\mathcal{L}(D, (q^5 - q^3 + q^2 - m - 2)H)$ are monomially equivalent.*

*Proof.* From [98, Chapter 12.17], $C_\Omega(D, G) = C_\mathcal{L}(D, K + D - G)$ for any canonical divisor $K$. The function $z$ has valuation 1 at each affine $\mathbb{F}_{q^6}$-rational point of $\mathcal{GK}_q$, hence $z$ is a separating element for $\mathbb{K}(\mathcal{GK}_q)/\mathbb{K}$ by [107, Prop. 3.10.2]. Then $dz$ is non-zero by [107, Prop. 4.1.8 (c)]. It is easily checked that $(dz)$ is a one-point divisor at $P_\infty$. Therefore, we may choose $K = (dz) = (q^3 + 1)(q^2 - 2)P_\infty$.

It suffices to prove that $K + D - G \equiv (q^5 - q^3 + q^2 - m - 2)H$, that is,

$$K + D \equiv (q^5 - q^3 + q^2 - 2)H.$$

Let $\pi_{a_i}$, $i = 1, \ldots, q^5 - q^3$, be the $q^5 - q^3$ planes described in Lemma 3.2.1. Consider the function

$$f := \Big( \prod_{i=1}^{q^5-q^3} (x - a_i) \Big) \Big( \prod_{P \in \mathrm{supp}(G), P \neq P_\infty} \tau_P(x, y) \Big),$$

where $\tau_P(x, y) \in \mathbb{F}_{q^2}[x, y]$ has principal divisor $(\tau_P) = (q^3 + 1)P - (q^3 + 1)P_\infty$, that is, $\tau_P(X, Y)$ is the tangent plane to $\mathcal{GK}_q$ at $P$. Then

$$K + D - (q^5 - q^3 + q^2 - 2)H = div \left( \frac{f}{z^{q^5+q^2-1}} \right).$$

Hence the claim follows. □

We determine the automorphism group of $C$. To this aim, we prove a preliminary Lemma.

**Lemma 3.2.7.** *Let $m \geq 2$. For any $P, Q \in \mathcal{GK}_q$, $\ell(G - P) = \ell(G) - 1$ and $\ell(G - P - Q) = \ell(G) - 2$.*

*Proof.* When $P$ and $Q$ are affine points, we denote their coordinates by $(a, b, c)$ and $(\bar{a}, \bar{b}, \bar{c})$, respectively. We consider separately a number of cases and provide $f_1 \in \mathcal{L}(G) \setminus \mathcal{L}(G - P)$ and $f_2 \in \mathcal{L}(G - P) \setminus \mathcal{L}(G - P - Q)$. The function $z - c$, for $c^{(q^3+1)(q^2-1)} + c^{(q^3+1)(q^2-q)} + 1 = 0$, has exactly $q^3 + 1$ zeros, which are simple and $\mathbb{F}_{q^6}$-rational, and $P_\infty$ is its unique pole; see the proof of Lemma 3.2.12.

- Case $P, Q \notin \mathrm{supp}(G)$, $P \neq Q$. If $c \neq \bar{c}$, choose $f_1 = \frac{z-\alpha}{z}$ and $f_2 = \frac{z-c}{z}$ with $\alpha \neq c$. If $c = \bar{c}$, then $a \neq \bar{a}$; choose $f_1 = \frac{x-\alpha}{z^2}$ and $f_2 = \frac{x-a}{z^2}$ with $\alpha \neq a$.

- Case $P,Q \notin \mathrm{supp}(G)$, $P=Q$. Choose $f_1 = \frac{z-\alpha}{z}$ and $f_2 = \frac{z-c}{z}$ with $\alpha \neq c$.
- Case $P \in \mathrm{supp}(G)$, $Q \notin \mathrm{supp}(G)$, $P \neq P_\infty$. Choose $f_1 = \left(\frac{z-\bar{c}}{z-c}\right)^m$ and $f_2 = 1$.
- Case $P = P_\infty$, $Q \notin \mathrm{supp}(G)$. Choose $f_1 = \left(\frac{x}{z}\right)^m$ and $f_2 = 1$.
- Case $P,Q \in \mathrm{supp}(G) \setminus \{P_\infty\}$, $P \neq Q$. Choose $f_1 = \left(\frac{x-\alpha}{z-c}\right)^m$ and $f_2 = \left(\frac{x-a}{z-c}\right)^m$ with $\alpha \neq a$.
- Case $P = P_\infty$, $Q \in \mathrm{supp}(G) \setminus \{P_\infty\}$. Choose $f_1 = \left(\frac{x}{z}\right)^m$ and $f_2 = \left(\frac{z-\alpha}{z-\bar{c}}\right)^m$ with $\alpha \neq \bar{c}$.
- Case $P = Q \in \mathrm{supp}(G) \setminus \{P_\infty\}$. Choose $f_1 = \frac{z-\alpha}{(z-c)^m}$ and $f_2 = \frac{z-\alpha}{(z-c)^{m-1}}$ with $\alpha \neq c$.
- Case $P = Q = P_\infty$. Choose $f_1 = \left(\frac{x}{z}\right)^m$ and $f_2 = \left(\frac{x}{z}\right)^{m-1}$.

□

**Proposition 3.2.8.** *The automorphism group of $C$ has a subgroup isomorphic to*

$$(\mathrm{Aut}(\mathcal{GK}_q) \rtimes \mathrm{Aut}(\mathbb{F}_{q^6})) \rtimes \mathbb{F}_{q^6}^*.$$

*Proof.* The supports of the divisors $D$ and $G$ are orbits of the $\mathbb{F}_{q^6}$-rational group $\mathrm{Aut}(\mathcal{GK}_q)$; hence, $\mathrm{Aut}_{\mathbb{F}_{q^6},D,G}(\mathcal{GK}_q)$ is isomorphic to $\mathrm{Aut}(\mathcal{GK}_q)$.

By [50, Section 5], the number $N$ of points of $\mathcal{GK}_q$ fixed by a non-trivial element of $\mathrm{Aut}(\mathcal{GK}_q)$ is at most $q^3+1$. In fact, let $\sigma \in \mathrm{Aut}(\mathcal{GK}_q)$ be given as an element of $\mathrm{PGL}(4,q^6)$. If $\sigma \notin \mathrm{SU}(3,q)$, then $\sigma$ fixes the plane $Z=0$ and no other plane with equation $Z=c$; thus, $N \leq |\mathcal{GK}_q \cap (Z=0)| = q^3+1$. If $\sigma \in \mathrm{SU}(3,q)$ and $\sigma$ fixes no points of $\mathcal{GK}_q$ out of the plane $Z=0$, then $N \leq q+1$ by Lemma 2.3.4. If $\sigma \in \mathrm{SU}(3,q)$ and $\sigma$ fixes a point $P \in \mathcal{GK}_q$ out of the plane $Z=0$, then the induced automorphism $\sigma$ of the Hermitian curve $\mathcal{H}_q : Y^{q+1} = X^q + X$ in the plane $Z=0$ fixes a point $\bar{P} \in \mathcal{H}_q$ which is $\mathbb{F}_{q^6}$-rational but not $\mathbb{F}_{q^2}$-rational. By Lemma 2.3.4, $\sigma$ fixes exactly 3 such points $\bar{P}, \bar{Q}, \bar{R} \in \mathcal{H}_q$, which correspond to at most $N = 3(q^2-q+1)$ points of $\mathcal{GK}_q$.

Now the claim follows from Proposition 1.1.47, since $\deg(D) = n > N$. □

**Proposition 3.2.9.** *If $2 \leq m \leq q^2-1$, then the automorphism group of $C$ is*

$$\mathrm{Aut}(C) \cong (\mathrm{Aut}(\mathcal{GK}_q) \rtimes \mathrm{Aut}(\mathbb{F}_{q^6})) \rtimes \mathbb{F}_{q^6}^*.$$

*In particular,* $\mathrm{Aut}(C)$ *has order* $6q^3(q+1)^3(q-1)^2(q^2-q+1)^3(q^2+q+1)\log_p(q)$.

*Proof.* The following properties hold.

- The divisor $G$ is effective.
- By Lemma 3.2.7, $\ell(G-P)=\ell(G)-1$ and $\ell(G-P-Q)=\ell(G)-2$ for any $P,Q\in\mathcal{GK}_q$.
- Let $\Pi(\mathcal{GK}_q)$ be the plane model of $\mathcal{GK}_q$ given in [50, Theorem 4], which has degree $q^3+1$. The function field $\mathbb{K}(\Pi(\mathcal{GK}_q))$ is generated by the coordinate functions $x$ and $z$, hence also by $x':=x/z^2$ and $z':=1/z$. The pole divisors of $x'$ and $z'$ are
$$(z')_\infty=\sum_{P\in\mathcal{G},P\neq P_\infty}P\,,\quad (x')_\infty=\sum_{P\in\mathcal{G},P\neq P_\infty,P\neq O}2P\,,$$
where $O=(0,0,0)$. Thus $x',z'\in\mathcal{L}(G)$.
- The curve $\mathcal{GK}_q$ is defined over $\mathbb{F}_p$.
- The Frobenius morphism $\varphi_p:(x,z)\mapsto(x^p,z^p)$ on $\Pi(\mathcal{GK}_q)$ preserves $\mathcal{GK}_q(\mathbb{F}_{q^6})$ and $\mathcal{GK}_q(\mathbb{F}_{q^2})$, hence also the support $\mathcal{GK}_q(\mathbb{F}_{q^6})\setminus\mathcal{GK}_q(\mathbb{F}_{q^2})$ of $D$.
- The condition $n>\deg G\cdot\deg(\Pi(\mathcal{GK}_q))$ holds if and only if $m\leq q^2-1$.

Then by Theorem 1.1.49 we have
$$\mathrm{Aut}(C)\cong(\mathrm{Aut}^+_{\mathbb{F}_{q^6},D,G}(\mathcal{GK}_q)\rtimes\mathrm{Aut}(\mathbb{F}_{q^6}))\rtimes\mathbb{F}^*_{q^6}\,.$$
By Remark 1.1.48, $\mathrm{Aut}^+_{\mathbb{F}_{q^6},D,G}(\mathcal{GK}_q)\cong\mathrm{Aut}_{\mathbb{F}_{q^6},D,G}(\mathcal{GK}_q)$, and both coincide with $\mathrm{Aut}_{\mathbb{F}_{q^6}}(\mathcal{GK}_q)$. Since $\mathrm{Aut}(\mathcal{GK}_q)$ is defined over $\mathbb{F}_{q^6}$, the claim follows. □

We construct a lengthening of $C$ by extending $D$ to the support of $G$.

Define the $\mathbb{F}_{q^6}$-divisors $G':=G$ and $D':=\sum_{P\in\mathcal{GK}_q(\mathbb{F}_{q^6})}P$ having degree $m(q^3+1)$ and $q^8-q^6+q^5+1$, respectively. Denote by $C':=C_{ext}(D',G')$ the associated extended AG code over $\mathbb{F}_{q^6}$ having length $n'=q^8-q^6+q^5+1$, dimension $k'$, and designed minimum distance $d'^*=n'-\deg(G')=q^8-q^6+q^5-mq^3-m+1$.

**Lemma 3.2.10.** *Whenever $d'^*>0$, $C'$ attains the designed minimum distance $d'^*$.*

*Proof.* Let $f\in\mathcal{L}(G')$ be defined as in (3.5). The codewords $e'_{D'}\in C'$ and $e_D\in C$ have the same number $m(q^3+1)$ of zero coordinates, hence the weight of $e'_{D'}$ is $n'-\deg(G')=d'^*$. □

In particular, $n' - d' = n - d$. The proof of the following result is analogous to the one of Proposition 3.2.3.

**Proposition 3.2.11.** *If $q^2 - 1 \leq m \leq q^5 - q^3$, then $k' = m(q^3+1) - \frac{1}{2}(q^5 - 2q^3 + q^2 - 2)$.*

Therefore, if $q^2 - 1 \leq m \leq q^5 - q^3 - 1$, then $C$ and $C'$ have the same Singleton defect $\delta = n + 1 - k - d$.

### 3.2.2 Some other constructions

For $c \in \mathbb{F}_{q^6}$, let $\zeta_c$ be the plane with affine equation $Z = c$, and

$$\Gamma := \left\{ c \in \mathbb{F}_{q^6} \mid c^{(q^3+1)(q^2-1)} + c^{(q^3+1)(q^2-q)} + 1 = 0 \right\}, \quad \Gamma_0 := \Gamma \cup \{0\}.$$

**Lemma 3.2.12.** *The plane $\zeta_c$ contains $q^3 + 1$ $\mathbb{F}_{q^6}$-rational points of $\mathcal{GK}_q$ if and only if $c \in \Gamma_0$. The number of such planes is $q^5 - q^3 + q^2$, and their affine points form a partition of $\mathcal{GK}_q(\mathbb{F}_{q^6}) \setminus \{P_\infty\}$.*

*Proof.* For any $c$, $P_\infty \in \zeta_c$. We prove that the equations

$$y^{q^2} - y - c^{q^2-q+1} = 0\,, \quad x^q + x - y^{q+1} = 0$$

have $q^3$ solutions $(x, y) \in \mathbb{F}_{q^6}^2$ if and only if $c \in \Gamma_0$. By [66, Theorem 1.22], the equation

$$y^{q^2} - y - c^{q^2-q+1} = 0 \tag{3.6}$$

has $q^2$ distinct solutions $y \in \mathbb{F}_{q^6}$ if and only if

$$(c^{q^2-q+1})^{q^4} + (c^{q^2-q+1})^{q^2} + c^{q^2-q+1} = 0, \tag{3.7}$$

and the equation $x^q + x - y^{q+1} = 0$ has $q$ distinct solutions $x \in \mathbb{F}_{q^6}$ if and only if

$$-y^{q+1} + (y^{q+1})^q - (y^{q+1})^{q^2} + (y^{q+1})^{q^3} - (y^{q+1})^{q^4} + (y^{q+1})^{q^5} = 0. \tag{3.8}$$

Using (3.6), Equation (3.8) reads

$$c^{(q^3+1)q^2} + c^{(q^3+1)(q^2-q+1)} + c^{q^3+1} = 0. \tag{3.9}$$

By direct computation, every solution $c$ of Equation (3.9) is also a solution of Equation (3.7); also, $c \in \mathbb{F}_{q^6}$. Since the polynomial $c^{(q^3+1)(q^2-1)} + c^{(q^3+1)(q^2-q)} + 1$ is separable, the solutions are all distinct. By the Hasse-Weil bound, we have $|\mathcal{GK}_q(\mathbb{F}_{q^6}) \setminus \{P_\infty\}| = q^3|\Gamma_0|$, and the claim follows. □

**First construction**

Let $\bar{m}, \bar{s} > 0$ and take $\bar{s}+1$ distinct elements $c_0 = 0, c_1, \ldots, c_{\bar{s}} \in \Gamma_0$. Define the sets

$$\bar{\mathcal{G}} := \bigcup_{i=0}^{\bar{s}} (\mathcal{GK}_q \cap \zeta_{c_i}), \quad \bar{\mathcal{D}} := \mathcal{GK}_q(\mathbb{F}_{q^6}) \setminus \bar{\mathcal{G}},$$

and the $\mathbb{F}_{q^6}$-divisors

$$\bar{G} := \bar{m}\big(P_\infty + \sum_{P \in \bar{\mathcal{G}}, P \neq P_\infty} P\big), \quad \bar{D} := \sum_{P \in \bar{\mathcal{D}}} P,$$

which have degree $\bar{m} + \bar{m}(\bar{s}+1)q^3$ and $q^8 - q^6 + q^5 - (\bar{s}+1)q^3$, respectively. Denote by $\bar{C} := C_{\mathcal{L}}(\bar{D}, \bar{G})$ the associated functional AG code over $\mathbb{F}_{q^6}$ having length $\bar{n} = \deg \bar{D}$, dimension $\bar{k}$, and minimum distance $\bar{d}$. The designed minimum distance of $\bar{C}$ is

$$\bar{d}^* = n - \deg \bar{G} = q^8 - q^6 + q^5 - (\bar{m}+1)(\bar{s}+1)q^3 - \bar{m}$$

**Proposition 3.2.13.** *If* $\frac{q^5-2q^3+q^2-1}{(\bar{s}+1)q^3+1} \leq \bar{m} \leq \frac{q^8-q^6+q^5-(\bar{s}+1)q^3-1}{(\bar{s}+1)q^3+1}$, *then*

$$\bar{k} = \bar{m}\left(1 + (\bar{s}+1)q^3\right) - \frac{1}{2}\left(q^5 - 2q^3 + q^2 - 2\right).$$

*Proof.* The proof is analogous to the proof of Proposition 3.2.3. □

**Proposition 3.2.14.** *The code* $\bar{C}$ *is monomially equivalent to the one-point code* $C_{\mathcal{L}}(\bar{D}, \bar{G}')$, *where* $\bar{G}' = \bar{m}[(\bar{s}+1)q^3+1]P_\infty$.

*Proof.* The proof is analogous to the proof of Proposition 3.2.4, after replacing the function $z^m$ with $\prod_{i=0}^{\bar{s}}(z-c_i)^{\bar{m}}$. □

**Corollary 3.2.15.** *If* $1 \leq \bar{m} \leq \frac{q^5-2q^3+q^2-1}{(\bar{s}+1)q^3+1}$, *then* $\bar{k}$ *is equal to the number* $\bar{k}_0$ *of triples* $(j_1, j_2, j_3) \in \mathbb{N}^3$ *such that*

$$j_2 \leq q^2 - q, \quad j_3 \leq q-1, \quad j_1(q^3-q^2+q) + j_2 q^3 + j_3(q^3+1) \leq \bar{m}[(\bar{s}+1)q^3+1].$$

*Proof.* The proof is analogous to the proof of Corollary 3.2.5, using that $\bar{k} = \ell(\bar{G}')$ where $\bar{G}' = \bar{m}[(\bar{s}+1)q^3+1]P_\infty$. □

**Lemma 3.2.16.** *Let* $\bar{m} \geq 2$. *For any* $P, Q \in \mathcal{GK}_q$, $\ell(\bar{G}-P) = \ell(\bar{G}) - 1$ *and* $\ell(\bar{G}-P-Q) = \ell(\bar{G}) - 2$.

*Proof.* We argue as in the proof of Lemma 3.2.7. When $P, Q \neq P_\infty$, let $P = (a, b, c)$, $Q = (\bar{a}, \bar{b}, \bar{c})$. It is enough to prove the condition on two points, by providing two $\mathbb{F}_{q^6}$-linearly independent functions $f_1, f_2 \in \mathcal{L}(\bar{G})$ such that $f_1, f_2 \notin \mathcal{L}(\bar{G} - P - Q)$ and $f_1 + \lambda f_2 \notin \mathcal{L}(\bar{G} - P - Q)$ for any $\lambda \in \mathbb{F}_{q^6}$.

- Case $P \notin \mathrm{supp}(\bar{G})$ or $Q \notin \mathrm{supp}(\bar{G})$. Argue as in the proof of Lemma 3.2.7.
- Case $P, Q \in \mathrm{supp}(\bar{G}) \setminus \{P_\infty\}$, $P \neq Q$. If $c \neq \bar{c}$, assume without loss of generality that $c \neq 0$ and choose $f_1 = \left(\frac{z-c}{z}\right)^m$, $f_2 = \left(\frac{z-\alpha}{z}\right)^m$ with $\alpha \notin \{c, 0\}$. If $c = \bar{c}$, then $a \neq \bar{a}$ and choose $f_1 = \frac{x-a}{(z-c_i)^m}$, $f_2 = \frac{x-\bar{a}}{(z-c_i)^m}$ with $i \in \{0, 1, \ldots, \bar{s}\}$, $c_i \neq c$.
- Case $P = P_\infty$. Argue as in the proof of Lemma 3.2.7.
- Case $P = Q \in \mathrm{supp}(\bar{G}) \setminus \{P_\infty\}$. Choose $f_1 = \frac{z-\alpha}{z^m}$, $f_2 = \frac{z-\beta}{z^m}$ with $\alpha \neq \beta$ and $\alpha, \beta \notin \{c_0, c_1, \ldots, c_s\}$.

□

**Proposition 3.2.17.** *Let $2 \leq \bar{m} \leq \frac{q^8 - q^6 + q^5 - (\bar{s}+1)q^3}{(\bar{s}+1)q^3(q^3+1)}$ and $r = \gcd\left(\bar{s}, \frac{q^2-q+1}{\delta}\right)$, where $\delta = \gcd(3, q+1)$. Suppose that $\{c_1, \ldots, c_{\bar{s}}\}$ is closed under the Frobenius map $\varphi_p : c_i \mapsto c_i^p$ and under the scalar map $\Lambda : c_i \mapsto \lambda c_i$, where $\lambda^r = 1$. Then the automorphism group of $\bar{C}$ is*

$$\mathrm{Aut}(\bar{C}) \cong ((\mathrm{SU}(3, q) \times C_r) \rtimes \mathrm{Aut}(\mathbb{F}_{q^6})) \rtimes \mathbb{F}_{q^6}^*\,,$$

*of order $rq^3(q+1)^3(q-1)^2(q^2-q+1)^2(q^2+q+1)\log_p(q^6)$.*

*Proof.* We argue as in the proof of Proposition 3.2.9.

- The divisor $\bar{G}$ is effective.
- By Lemma 3.2.16, $\ell(\bar{G} - P) = \ell(\bar{G}) - 1$ and $\ell(\bar{G} - P - Q) = \ell(\bar{G}) - 2$ for any $P, Q \in \mathcal{GK}_q$.
- Let $\Pi(\mathcal{GK}_q)$ be the plane model of $\mathcal{GK}_q$ given in [50, Theorem 4], which has degree $q^3 + 1$. The function field $\mathbb{K}(\Pi(\mathcal{GK}_q))$ is generated by the functions $x' := x/z^2$ and $z' := 1/z$. We have $x', z' \in \mathcal{L}(\bar{G})$.
- The curve $\mathcal{GK}_q$ is defined over $\mathbb{F}_p$.
- The Frobenius morphism $\varphi_p : (x, z) \mapsto (x^p, z^p)$ on $\Pi(\mathcal{GK}_q)$ preserves the support of $\bar{G}$ by our assumptions; hence, $\varphi_p$ preserves also the support of $D$.

- The condition $\bar{n} > \deg \bar{G} \cdot \deg(\Pi(\mathcal{GK}_q))$ holds if and only if $m \leq \frac{q^8-q^6+q^5-(\bar{s}+1)q^3}{(\bar{s}+1)q^3(q^3+1)}$.

Then by Theorem 1.1.49 we have

$$\mathrm{Aut}(\bar{C}) \cong (\mathrm{Aut}^{+}_{\mathbb{F}_{q^6},\bar{D},\bar{G}}(\mathcal{GK}_q) \rtimes \mathrm{Aut}(\mathbb{F}_{q^6})) \rtimes \mathbb{F}^{*}_{q^6}\,.$$

By Remark 1.1.48, $\mathrm{Aut}^{+}_{\mathbb{F}_{q^6},\bar{D},\bar{G}}(\mathcal{GK}_q) \cong \mathrm{Aut}_{\mathbb{F}_{q^6},\bar{D},\bar{G}}(\mathcal{GK}_q)$. Since $\mathrm{Aut}(\mathcal{GK}_q)$ is defined over $\mathbb{F}_{q^6}$, we have that $\mathrm{Aut}^{+}_{\mathbb{F}_{q^6},\bar{D},\bar{G}}(\mathcal{GK}_q)$ coincides with the subgroup $S$ of $\mathrm{Aut}(\mathcal{GK}_q)$ stabilizing the support of $\bar{G}$. By the discussion after Lemma 8 in [50], $S$ is contained in the group $M \cong \mathrm{SU}(3,q) \times C_{(q^2-q+1)/\delta}$ defined in [50, Lemma 8]. In particular, $S$ contains a subgroup $\mathrm{SU}(3,q) \times C_r$. Since $s/r$ is coprime to $(q^2-q+1)/\delta$, $S$ cannot contain any subgroup $\mathrm{SU}(3,q) \times C_{r'}$ with $r \mid r'$ and $r' > r$. The claim follows. □

If we drop off the restriction on $\bar{m}$, we still have a (possibly proper) subgroup of $\mathrm{Aut}(\bar{C})$.

**Proposition 3.2.18.** *Let* $r = \gcd\left(\bar{s}, \frac{q^2-q+1}{\delta}\right)$ *where* $\delta = \gcd(3, q+1)$*. Suppose that* $\{c_1, \ldots, c_{\bar{s}}\}$ *is closed under the Frobenius map* $\varphi_p : c_i \mapsto c_i^p$ *and under the scalar map* $\Lambda : c_i \mapsto \lambda c_i$*, where* $\lambda^r = 1$*. If* $\bar{s} \leq q^5 - q^3 + q^2 - 3$*, then the automorphism group of* $\bar{C}$ *contains a subgroup isomorphic to*

$$((\mathrm{SU}(3,q) \times C_r) \rtimes \mathrm{Aut}(\mathbb{F}_{q^6})) \rtimes \mathbb{F}^{*}_{q^6}\,.$$

*Proof.* As in the proof of Proposition 3.2.17, we have

$$\mathrm{Aut}_{\mathbb{F}_{q^6},\bar{D},\bar{G}}(\mathcal{GK}_q) \cong \mathrm{SU}(3,q) \times C_r.$$

Any non-trivial element of $\mathrm{Aut}(\mathcal{GK}_q)$ has at most $N = q^3 + 1$ fixed points on $\mathcal{GK}_q$ (see the proof of Proposition 3.2.8). By the assumption on $\bar{s}$, this implies that $\bar{n} > N$. Therefore the claim follows from Proposition 1.1.47. □

### Second construction

Let $\tilde{m}, \tilde{s} \in \mathbb{N}$ and take $\tilde{s}+1$ distinct elements $c_0 = 0, c_1, \ldots, c_{\tilde{s}} \in \Gamma_0$. Define the sets

$$\tilde{\mathcal{G}} := \Big(\bigcup_{i=0}^{\tilde{s}} (\mathcal{GK}_q \cap \zeta_{c_i})\Big) \setminus \{P_\infty\}, \quad \tilde{\mathcal{D}} := \mathcal{GK}_q(\mathbb{F}_{q^6}) \setminus \tilde{\mathcal{G}},$$

and the $\mathbb{F}_{q^6}$-divisors

$$\tilde{G} := \sum_{P \in \tilde{\mathcal{G}}, P \neq P_\infty} \tilde{m}P, \quad \tilde{D} := \sum_{P \in \tilde{\mathcal{D}}} P,$$

which have degree $\tilde{m}(\tilde{s}+1)q^3$ and $q^8-q^6+q^5-(\tilde{s}+1)q^3+1$, respectively. Denote by $\tilde{C} := C_{\mathcal{L}}(\tilde{D},\tilde{G})$ the associated functional AG code over $\mathbb{F}_{q^6}$ having length $\tilde{n}=\deg \tilde{D}$, dimension $\tilde{k}$, and minimum distance $\tilde{d}$. The designed minimum distance of $\tilde{C}$ is

$$\tilde{d}^* = \tilde{n} - \deg \tilde{G} = q^8-q^6+q^5-(\tilde{m}+1)(\tilde{s}+1)q^3+1$$

**Proposition 3.2.19.** *When $\tilde{d}^*>0$, $\tilde{C}$ attains the designed minimum distance $\tilde{d}^*$.*

*Proof.* Since $\tilde{d}^*>0$, there exist $\tilde{m}(\tilde{s}+1)$ distinct elements $\gamma_1,\ldots,\gamma_{\tilde{m}(\tilde{s}+1)} \in \Gamma_0 \setminus \{c_0,c_1,\ldots,c_{\tilde{s}}\}$. Consider the function

$$\tilde{f} := \prod_{i=0}^{\tilde{s}}\prod_{j=1}^{\tilde{m}}\left(\frac{z-\gamma_{i\tilde{m}+j}}{z-c_i}\right).$$

The pole divisor of $\tilde{f}$ is $(f)_\infty = \tilde{G}$, thus $\tilde{f}\in\tilde{G}$. The weight of $e_{\tilde{D}}(\tilde{f})$ is

$$w(e_{\tilde{D}}(\tilde{f})) = \tilde{n} - \tilde{m}(\tilde{s}+1)q^3 = \tilde{d}^*.$$

□

**Proposition 3.2.20.** *If $\frac{q^5-2q^3+q^2-1}{(\tilde{s}+1)q^3} \le \tilde{m} \le \frac{q^5-q^3+q^2}{\tilde{s}+1}-1$, then*

$$\tilde{k} = \tilde{m}(\tilde{s}+1)q^3 - \frac{1}{2}\left(q^5-2q^3+q^2-4\right).$$

*Proof.* The proof is analogous to the proof of Proposition 3.2.3. □

**Proposition 3.2.21.** *The code $\tilde{C}$ is monomially equivalent to the extended one-point code $C_{ext}(\tilde{D},\tilde{G}')$, where $\tilde{G}'=\tilde{m}(\tilde{s}+1)q^3P_\infty$.*

*Proof.* By direct checking, $\tilde{G}=\tilde{G}'+(w)$ where $w=\prod_{i=0}^{\tilde{s}}(z-c_i)^{\tilde{m}}$. Hence, $\mathcal{L}(\tilde{G}')=\left\{f\cdot w \mid f\in\mathcal{L}(\tilde{G})\right\}$.

The codeword of $C_{ext}(\tilde{D},\tilde{G}')$ associated to $f\cdot w$ is

$$\big((w^{-1}fw)(P_\infty),(fw)(P_2),\ldots,(fw)(P_n)\big) = (f(P_\infty),f(P_2),\ldots,f(P_n))\cdot M,$$

where $M$ is the diagonal matrix with diagonal entries $1,w(P_2),\ldots,w(P_n)\in\mathbb{F}_{q^6}$. This means that $M$ defines a monomial equivalence between $\tilde{C}$ and $C_{ext}(\tilde{D},\tilde{G}')$. □

**Corollary 3.2.22.** *If $1\le\tilde{m}\le\frac{q^5-2q^3+q^2-1}{(\tilde{s}+1)q^3}$, then $\tilde{k}$ is equal to the number $\tilde{k}_0$ of triples $(j_1,j_2,j_3)\in\mathbb{N}^3$ such that*

$$j_2\le q^2-q,\quad j_3\le q-1,\quad j_1(q^3-q^2+q)+j_2q^3+j_3(q^3+1)\le\tilde{m}(\tilde{s}+1)q^3.$$

*Proof.* The proof is analogous to the proof of Corollary 3.2.5, where $G'$ is replaced by the one-point divisor $\tilde{G}' = \tilde{m}(\tilde{s}+1)q^3P_\infty$, which is equivalent to $\tilde{G}$ since $\tilde{G} = \tilde{G}' + div\left(\prod_{i=0}^{\tilde{s}}(z-c_i)^{\tilde{m}}\right)$. □

**Lemma 3.2.23.** *If $\tilde{m} \geq 2$ and $p \nmid \tilde{m}$, then for any $P, Q \in \mathcal{GK}_q$ we have $\ell(\tilde{G}-P) = \ell(\tilde{G}) - 1$ and $\ell(\tilde{G}-P-Q) = \ell(\tilde{G}) - 2$.*

*Proof.* As in the proof of Lemma 3.2.7, it suffices to provide two $\mathbb{F}_{q^6}$-linearly independent functions $f_1, f_2 \in \mathcal{L}(\bar{G})$ such that $f_1, f_2 \notin \mathcal{L}(\bar{G}-P-Q)$ and $f_1 + \lambda f_2 \notin \mathcal{L}(\bar{G}-P-Q)$ for any $\lambda \in \mathbb{F}_{q^6}$.

- Case $P, Q \neq P_\infty$. Argue as in the proof of Lemma 3.2.16.
- Case $P = P_\infty$, $P \neq Q$. Choose $f_1 = \frac{z-\alpha}{z}$ and $f_2 = \frac{z-\beta}{z}$, with $\alpha, \beta \neq 0$, $\alpha \neq \beta$.
- Case $P = Q = P_\infty$. Choose $f_1 = \left(\frac{z-\alpha}{z}\right)^m$ and $f_2 = \left(\frac{z-\beta}{z}\right)^m$, with $\alpha, \beta \neq 0$, $\alpha \neq \beta$. Since $p \nmid \tilde{m}$, we have $f_1 + \lambda f_2 \notin \mathcal{L}(\tilde{G} - 2P_\infty)$.

□

**Proposition 3.2.24.** *Let $2 \leq \tilde{m} \leq \frac{q^2-1}{\tilde{s}+1} - \frac{\tilde{s}}{(\tilde{s}+1)(q^3+1)}$ with $p \nmid \tilde{m}$, and $r = \gcd\left(\tilde{s}, \frac{q^2-q+1}{\delta}\right)$ where $\delta = \gcd(3, q+1)$. Suppose that $\{c_1, \ldots, c_{\tilde{s}}\}$ is closed under the Frobenius map $\varphi_p : c_i \mapsto c_i^p$ and under the scalar map $\Lambda : c_i \mapsto \lambda c_i$, where $\lambda^r = 1$. Then the automorphism group $\mathrm{Aut}(\tilde{C})$ of $\tilde{C}$ is isomorphic to*

$$(\mathrm{Aut}_{\mathbb{F}_{q^6},\tilde{D},\tilde{G}}(\mathcal{GK}_q) \rtimes \mathrm{Aut}(\mathbb{F}_{q^6})) \rtimes \mathbb{F}_{q^6}^* . \tag{3.10}$$

*If $\tilde{s} = 0$, then $\mathrm{Aut}_{\mathbb{F}_{q^6},\tilde{D},\tilde{G}}(\mathcal{GK}_q)$ has a normal subgroup $N$ of index $\delta$ with*

$$N \cong (Q_{q^3} \rtimes H_{q^2-1}) \times C_{(q^2-q+1)/\delta} .$$

*If $\tilde{s} > 0$, then*

$$\mathrm{Aut}_{\mathbb{F}_{q^6},\tilde{D},\tilde{G}}(\mathcal{GK}_q) \cong (Q_{q^3} \rtimes H_{q^2-1}) \times C_r .$$

*Here, $Q_{q^3}$ has order $q^3$ and is the unique Sylow $p$-subgroup of $\mathrm{Aut}(\tilde{C})$. The groups $H_i$ and $C_j$ are cyclic of order $i$ and $j$, respectively.*

*Proof.* As in the proof of Proposition 3.2.9, the following facts hold.

- The divisor $\tilde{G}$ is effective.
- By Lemma 3.2.23, we have $\ell(\tilde{G}-P) = \ell(\tilde{G}) - 1$ and $\ell(\tilde{G}-P-Q) = \ell(\tilde{G}) - 2$ for any $P, Q \in \mathcal{GK}_q$.

- The functions $x' := x/z^2, z' := 1/z \in \mathcal{L}(\tilde{G})$ generate the function field of the plane model $\Pi(\mathcal{GK}_q)$ of $\mathcal{GK}_q$ given in [50, Theorem 4].
- The curve $\mathcal{GK}_q$ is defined over $\mathbb{F}_p$.
- The Frobenius morphism $\varphi_p : (x,z) \mapsto (x^p, y^p)$ on $\Pi(\mathcal{GK}_q)$ preserves the support of $\tilde{D}$.
- Since $\tilde{m} \leq \frac{q^2-1}{\tilde{s}+1} - \frac{\tilde{s}}{(\tilde{s}+1)(q^3+1)}$, we have $\tilde{n} > \deg(\tilde{G}) \cdot \deg(\Pi(\mathcal{GK}_q))$.

Then by Theorem 1.1.49 we have

$$\mathrm{Aut}(\tilde{C}) \cong (\mathrm{Aut}^+_{\mathbb{F}_{q^6},\tilde{D},\tilde{G}}(\mathcal{GK}_q) \rtimes \mathrm{Aut}(\mathbb{F}_{q^6})) \rtimes \mathbb{F}^*_{q^6}\,.$$

By Remark 1.1.48, $\mathrm{Aut}^+_{\mathbb{F}_{q^6},\tilde{D},\tilde{G}}(\mathcal{GK}_q) \cong \mathrm{Aut}_{\mathbb{F}_{q^6},\tilde{D},\tilde{G}}(\mathcal{GK}_q)$. Since $\mathrm{Aut}(\mathcal{GK}_q)$ is defined over $\mathbb{F}_{q^6}$, we have that $\mathrm{Aut}^+_{\mathbb{F}_{q^6},\tilde{D},\tilde{G}}(\mathcal{GK}_q)$ coincides with the subgroup $S$ of $\mathrm{Aut}(\mathcal{GK}_q)$ stabilizing the support of $\tilde{G}$.

The claim follows by the properties of $\mathrm{Aut}(\mathcal{GK}_q)$ which have been proved in [50]. In particular, suppose $\tilde{s} = 0$. Then $\mathrm{supp}(\tilde{G}) \cup \{P_\infty\}$ is a unique orbit of $\mathrm{Aut}(\mathcal{GK}_q)$ by [50, Theorem 7]. Hence, $S$ is the stabilizer of $P_\infty$ in $\mathrm{Aut}(\mathcal{GK}_q)$, and the claim follows. Now suppose $\tilde{s} > 0$. Then $S$ is contained in the subgroup $(Q_{q^3} \rtimes H_{q^2-1}) \times C_{(q^2-q+1)/\delta}$ of the group $M \cong \mathrm{SU}(3,q) \times C_{(q^2-q+1)/\delta}$ defined in [50, Lemma 8]. By the assumptions on $\Lambda$, $S$ contains a subgroup $(Q_{q^3} \rtimes H_{q^2-1}) \times C_r$. Since $h$ is coprime to $(q^2-q+1)/\delta$, $S$ does not contain any cyclic group $C_{r'}$ with $C_r \subseteq C_{r'}$ and $r' > r$. The claim follows. □

**Proposition 3.2.25.** *Let $r = \gcd\left(\tilde{s}, \frac{q^2-q+1}{\delta}\right)$ where $\delta = \gcd(3, q+1)$. Suppose that $\{c_1, \ldots, c_{\tilde{s}}\}$ is closed under the Frobenius map $\varphi_p : c_i \mapsto c_i^p$ and under the scalar map $\Lambda : c_i \mapsto \lambda c_i$, where $\lambda^r = 1$. If $\tilde{s} \leq q^5 - q^3 + q^2 - 3$, then the automorphism group $\mathrm{Aut}(\tilde{C})$ of $\tilde{C}$ contains the subgroup*

$$(\mathrm{Aut}_{\mathbb{F}_{q^6},\tilde{D},\tilde{G}}(\mathcal{GK}_q) \rtimes \mathrm{Aut}(\mathbb{F}_{q^6})) \rtimes \mathbb{F}^*_{q^6}$$

*described in (3.10) and in the statement of Proposition 3.2.24.*

*Proof.* The proof is analogous to the proof of Proposition 3.2.18 and is then omitted. □

# Chapter 4

# New applications of the Hasse-Weil Bound in Finite Geometry and Permutation Polynomials

In this Chapter, the Hasse-Weil Bound and tools from the theory of algebraic curves over finite fields are used to investigate interesting objects which arise in other areas of discrete mathematics, namely in Finite Geometry and in Permutation Polynomials.

In the area of Finite Geometry, we construct in Section 4.1 complete $(k, 3)$-arcs in $\mathrm{PG}(2, q)$ starting from subsets of the quartic curve with affine equation $Y = X^4$, for $q$ a power of an odd prime $p \equiv 2 \pmod 3$. The order of magnitude of $k$ is smaller than $q$. This property significantly distinguishes the complete $(k, 3)$-arcs of Section 4.1 from the previously known infinite families, whose size differs from $q$ by at most $2\sqrt{q}$. The results of Section 4.1 are the object of [6]. Analogously, we construct in Section 4.2 complete $(k, 4)$-arcs in $\mathrm{PG}(2, q)$ starting from subsets of the quintic curve $Y = X^5$, whose size $k$ has order smaller than $q$. The results of Section 4.2 are the object of [10].

In the area of Permutation Polynomials, we investigate in Section 4.3 a particular class of complete permutation polynomials (shortly, CPPs) over finite fields, namely the monomial CPPs $ax^d$ of $\mathbb{F}_{q^n}$ with degree $d = (q^n - 1)/(q - 1) + 1$. The CPPs are studied in connection with exceptional polynomials. We characterize the CPPs $ax^d$ of $\mathbb{F}_{q^n}$ in the case $n + 1$ prime and $n^4 < q$, proving in this way a conjecture by Wu, Li, Helleseth, and Zhang. When $n + 1$ is a power of the characteristic we provide some new examples of CPPs. The results of Section 4.2 are the object of [5].

## 4.1 Complete $(k,3)$-arcs from quartic curves

A $(k,r)$-arc in $\mathrm{PG}(2,q)$ is a set of $k$ points no $(r+1)$ of which are collinear and such that there exist $r$ collinear points; see [66, Chapter 12] for a general introduction. A $(k,3)$-arc is said to be *complete* if it maximal with respect to set-theoretical inclusion.

From a Coding Theory point of view, complete $(k,r)$-arcs corresond to $[k,3,k-3]_q$-codes which cannot be extended to a code with the same minimum distance. In particular, $(k,3)$-arc correspond to AMDS (Almost Maximum Distance Separable) codes, i.e. codes having Singleton defect equal to 1, and to NMDS (Near Maximum Distance Separable) codes, i.e. AMDS codes such that the dual is also AMDS; see [32, 33].

In the case $r=2$, the theory is well developed and quite rich of constructions; see e.g. [66, Chapters 8-10]. On the other hand, for most $r>2$, the only known families consist of the set of $\mathbb{F}_q$-rational points of some irreducible curve of degree $r$, or arise from the theory of 2-character sets in $\mathrm{PG}(2,q)$. In particular, the unique infinite families of complete $(k,3)$-arcs known in literature come from cubic curves and have roughly $q$ points; see [68].

In this section we construct infinite families of complete $(k,3)$-arcs in $\mathrm{PG}(2,q)$, whose order of magnitude is asymptotically smaller than $q$. Our main result is the following.

**Theorem 4.1.1.** *Let $\sigma$ be a non-square power of a prime $p>2$, with $p\equiv 2 \pmod 3$. Define*

$$\tau(\sigma)=\begin{cases} \frac{p+5}{4} & \text{if } \sigma=p\,,\\ 2\left(\sqrt{\sigma}\,\frac{p-1}{\sqrt{p}}-p+3\right) & \text{if } \sigma>p\,.\end{cases}\,.$$

*Then, for all power $q$ of $\sigma$ with $q\geq 3600\,\sigma^6$, there exists a complete $(k,3)$-arc in $\mathrm{PG}(2,q)$ of size*

$$k\leq \frac{\tau(\sigma)}{\sigma}q+6\,.$$

Almost all the points of the $(k,3)$-arcs constructed in this section belong to the set of $\mathbb{F}_q$-rational points of the curve $\mathcal{Q}: Y=X^4$. The proof of their completeness is based on a classical idea going back to Segre [103] and Lombardo Radice [83]. We construct a curve $\mathcal{H}_P$ over $\mathbb{F}_q$ describing the collinearity condition of three points of $\mathcal{Q}$ and a point $P\in\mathrm{PG}(2,q)\setminus\mathcal{Q}$; we prove that $\mathcal{H}_P$ has an absolutely irreducible component defined over $\mathbb{F}_q$, and deduce that $P$ is collinear with three points in the arc.

Throughout the section, $p$ is an odd prime with $p\equiv 2 \pmod 3$, $\sigma=p^{h'}$ with $h'$ odd, $q=p^h$ with $h'<h$, $h'\mid h$, and $\mathbb{K}$ is the algebraic closure of $\mathbb{F}_p$.

### 4.1.1 $(k,3)$-arcs from quartic curves

Let $\mathcal{Q}$ be the plane quartic curve over $\mathbb{F}_q$ with affine equation $Y = X^4$. The following propositions show the collinearity condition of three and four points of the quartic $\mathcal{Q}$.

**Proposition 4.1.2.** *Let $A = (u,u^4)$, $B = (v,v^4)$, $C = (w,w^4)$ three distinct points of $\mathcal{Q}$. They are collinear if and only if $u^2+v^2+w^2+uv+uw+vw = 0$.*

*Proof.* $A,B,C$ are collinear if, and only if,

$$\det\begin{pmatrix} u & u^4 & 1 \\ v-u & v^4-u^4 & 0 \\ w-u & w^4-u^4 & 0 \end{pmatrix} = (v-u)(w-u)(w-v)[u^2+v^2+w^2+uv+uw+vw] = 0.$$

As $A,B,C$ are distinct, the assertion follows. □

**Proposition 4.1.3.** *Let $A = (u,u^4)$, $B = (v,v^4)$, $C = (w,w^4)$, $D = (t,t^4)$ four distinct points of $\mathcal{Q}$. They are collinear if, and only if,*

$$\begin{cases} u^2+v^2+w^2+uv+uw+vw = 0 \\ u+v+w+t = 0 \end{cases}.$$

*Proof.* By Proposition 4.1.2, the points $A,B,C,D$ are collinear if and only if

$$\begin{cases} u^2+v^2+w^2+uv+uw+vw = 0 \\ u^2+v^2+t^2+uv+ut+vt = 0 \end{cases}.$$

Since $w \neq t$, this is equivalent to

$$\begin{cases} u^2+v^2+w^2+uv+uw+vw = 0 \\ u+v+w+t = 0 \end{cases}.$$

□

Next we construct a $(k,3)$-arc contained in $\mathcal{Q}$ from a coset of an additive subgroup of $\mathbb{F}_q$. Let $M$ be the following additive subgroup of $\mathbb{F}_q$ of order $q/\sigma$ :

$$M := \{(a^\sigma - a) \ : \ a \in \mathbb{F}_q\}, \tag{4.1}$$

and consider

$$\mathcal{K}_t := \{(v,v^4) \mid v \in M+t\}, \tag{4.2}$$

where $t \notin M$.

**Proposition 4.1.4.** *The set $\mathcal{K}_t$ is a $(k,3)$-arc.*

*Proof.* By Proposition 4.1.3, if four distinct points $(a_i+t,(a_i+t)^4)$, $a_i \in M$, $i = 1,\ldots,4$, are collinear then $a_1+t+a_2+t+a_3+t+a_4+t = 0$, hence $-4t = a_1+a_2+a_3+a_4 \in M$. Since $p \neq 2$ and $M$ is closed under multiplication by elements of $\mathbb{F}_\sigma$, we have $t \in M$, a contradiction. □

### 4.1.2 Points off $\mathcal{Q}$ are covered by $\mathcal{K}_t$

**Proposition 4.1.5.** *Three distinct points $A = (u, u^4)$, $B = (v, v^4)$, $C = (w, w^4)$ of $\mathcal{Q}$ and $P = (a, b) \in \mathrm{AG}(2, q) \setminus \mathcal{Q}$ are collinear if and only if*

$$\begin{cases} u^2 + v^2 + w^2 + uv + uw + vw = 0 \\ a(u^2 + v^2)(u + v) - uv(u^2 + uv + v^2) - b = 0 \end{cases}.$$

*Proof.* The former equation is the collinearity condition for $A, B, C$, the latter is the collinearity condition for $A, B, P$, since

$$\det \begin{pmatrix} u & u^4 & 1 \\ v & v^4 & 1 \\ a & b & 1 \end{pmatrix} = (u - v)\left[a(u^2 + v^2)(u + v) - uv(u^2 + uv + v^2) - b\right].$$

□

In particular, if the points of $\mathcal{Q}$ have the form $A = (u + t, (u + t)^4)$, $B = (v + t, (v + t)^4)$, $C = (w + t, (w + t)^4)$, the conditions in Proposition 4.1.5 read

$$\begin{cases} w^2 + w(u + v + 4t) + 4t(u + v) + \\ +6t^2 + uv + u^2 + v^2 = 0 \\ \\ a(u^2 + v^2 + 2t^2 + 2tu + 2tv)(u + v + 2t) \\ -(u + t)(v + t)(u^2 + v^2 + uv + 3t^2 + 3t(u + v)) - b = 0 \end{cases}.$$

Then the following result holds.

**Corollary 4.1.6.** *A point $P = (a, b) \in \mathrm{AG}(2, q) \setminus \mathcal{Q}$ is collinear with three distinct points of $\mathcal{K}_t$ if and only if there exists a $\mathbb{F}_q$-rational affine point $(x, y, z)$, with $x^\sigma - x$, $y^\sigma - y$, $z^\sigma - z$ pairwise distinct, lying on the space curve $\mathcal{H}_P$ with equation*

$$\begin{cases} (Z^\sigma - Z)^2 + (Z^\sigma - Z)((X^\sigma - X) + (Y^\sigma - Y) + 4t) + 4t(X^\sigma - X + Y^\sigma - Y) + \\ +6t^2 + (X^\sigma - X)(Y^\sigma - Y) + (X^\sigma - X)^2 + (Y^\sigma - Y)^2 = 0 \\ \\ a((X^\sigma - X)^2 + (Y^\sigma - Y)^2 + 2t^2 + 2t(X^\sigma - X) + 2t(Y^\sigma - Y)) \cdot \\ \cdot (X^\sigma - X + Y^\sigma - Y + 2t) - (X^\sigma - X + t)(Y^\sigma - Y + t) \cdot ((X^\sigma - X)^2 + \\ +(Y^\sigma - Y)^2 + (X^\sigma - X)(Y^\sigma - Y) + 3t^2 + 3t(X^\sigma - X + Y^\sigma - Y)) - b = 0 \end{cases}. \tag{4.3}$$

Consider the following sequence of function field extensions:

$$\begin{tikzcd}[row sep=small]
F_5 = F_4(z) : z^\sigma - z = w \arrow[d, dash, "\sigma"'] \\
F_4 = F_3(w) : \left\{ \begin{array}{l} w^2 + w((x^\sigma - x) + (y^\sigma - y) + 4t) + 4t(x^\sigma - x + y^\sigma - y) \\ +6t^2 + (x^\sigma - x)(y^\sigma - y) + (x^\sigma - x)^2 + (y^\sigma - y)^2 = 0 \end{array} \right. \arrow[d, dash, "2"'] \\
F_3 = F_2(y) : y^\sigma - y = v \arrow[d, dash, "\sigma"'] \\
F_2 = F_1(x) : x^\sigma - x = u \arrow[d, dash, "\sigma"'] \\
F_1 = \mathbb{F}_q(u,v) : \begin{array}{l} a(u^2 + v^2 + 2t^2 + 2tu + 2tv)(u + v + 2t) + \\ -(u+t)(v+t)(u^2 + v^2 + uv + 3t^2 + 3t(u+v)) - b = 0 \end{array}
\end{tikzcd}$$

We are going to show that each extension $F_i : F_{i-1}$ is well defined and that the field of constants of each function field $F_i$ is $\mathbb{F}_q$. We will also estimate the genus $g_i$ of $F_i$. Finally, by using the Hasse-Weil bound, we will show that if $q$ is large enough with respect to $\sigma$, then $F_5$ has a large number of $\mathbb{F}_q$-rational places. By the equations defining $F_5$, this implies that the curve $\mathcal{H}_P$ possesses a large number of $\mathbb{F}_q$-rational points.

We will first show that $F_1$ is a function field with genus 3 whose field of constants is $\mathbb{F}_q$; see Proposition 4.1.8 below. Equivalently, the plane quartic curve with equation

$$\mathcal{H}_1 : \begin{array}{l} a(U^2 + V^2 + 2t^2 + 2tU + 2tV)(U + V + 2t) \\ -(U+t)(V+t)(U^2 + V^2 + UV + 3t^2 + 3t(U+V)) - b = 0 \end{array} \tag{4.4}$$

is non-singular. We start by investigating an auxiliary cubic curve.

**Lemma 4.1.7.** *Let $a, b \in \mathbb{F}_q$ with $b \neq 0$, $b \neq a^4$. The plane curve with equation*

$$a(C^2 + 2t^2 + 2tC - 2D)(C + 2t) - (D + tC + t^2)(C^2 - D + 3t^2 + 3tC) - b = 0 \tag{4.5}$$

*is absolutely irreducible and has genus $g_0 = 1$*

*Proof.* After the affine transformation $\xi = D + tC + t^2, \zeta = C + 2t$ Eq. (4.5) becomes $h_0(\xi, \zeta) = 0$ with

$$h_0(\xi, \zeta) = a\zeta^3 - \xi\zeta^2 - 2a\xi\zeta + \xi^2 - b.$$

Since $\partial_\xi h_0'(\xi, \zeta) = -\zeta^2 - 2a\zeta + 2\xi$ and $\partial_\zeta h_0'(\xi, \zeta) = 3a\zeta^2 - 2\xi\zeta - 2a\xi$, we have that the only three possibilities for an affine singular point are $(a^2(\sqrt{-2} \mp 1), \pm\sqrt{-2}a)$ and

$(0,0)$, which satisfy $h_0'(\xi,\zeta)=0$ if and only if $b=a^4$ or $b=0$. It is straightforward to check that the ideal points $(1:0:0),(a:1:0)$ are non-singular. Then the assertion follows. □

**Proposition 4.1.8.** *Let $a,b\in\mathbb{F}_q$ with $b\neq 0$, $b\neq a^4$. Let $\mathbb{F}_q(c,d)$ be the function field of the non-singular cubic curve with Eq. (4.5). Then the equations $u+v=c$, $uv=d$ define a function field $\mathbb{F}_q(u,v)$ of genus 3, with equation*

$$\begin{aligned}&a(u^2+v^2+2t^2+2tu+2tv)(u+v+2t)+\\&-(u+t)(v+t)(u^2+v^2+uv+3t^2+3t(u+v))-b=0\end{aligned}$$

*whose constant field is $\mathbb{F}_q$.*

*Proof.* Let $\mu=\frac{c^2}{4}-d\in\mathbb{F}_q(c,d)$. We are going to show that $\mu$ is a non-square in $\mathbb{K}(c,d)$. By substituting $D=C^2/4$ in (4.5) we obtain

$$-3/16C^4+(1/2a-3/2t)C^3+(3at-9/2t^2)C^2+(6at^2-6t^3)C+4at^3-b-3t^4=0 \quad (4.6)$$

Derivation with respect to $C$ gives $-\frac{3}{4}(C+2t)^2(C-2a+2t)$. Then, the only possible multiple solutions of (4.6) are $C=-2t$ and $C=2a-2t$. By straightforward computation, this actually happens only if $b=0$ or $b=a^4$, which is impossible. Therefore, there exist four distinct simple zeros of $\mu$ in $\mathbb{K}(c,d)$. Let $P_\infty$ and $Q_\infty$ be the placed centered at the ideal points $(0:1:0)$ and $(1:a-t:0)$, respectively. It is easily seen that $v_{P_\infty}(c^2-4d)=-2$ and $v_{Q_\infty}(c^2-4d)=-2$.

Then the extension $\mathbb{K}(c,d,\eta)|\mathbb{K}(c,d)$ with $\eta^2=\mu$ is a Kummer extension of degree 2 with genus

$$g_1=1+2(g_0-1)+\frac{1}{2}\sum_{P\in\mathbb{P}(\mathbb{K}(c,d))}(2-\gcd(2,v_P(\mu)))\deg(P)=1+\frac{1}{2}4=3.$$

Also, by Lemma 1.1.36, $\mathbb{F}_q$ is the constant field of $\mathbb{F}_q(u,v)$. To complete the proof, we only need to show that actually $\mathbb{K}(c,d)(\eta)$ coincides with $\mathbb{K}(u,v)$. This immediately follows from $u=\eta+c/2$ and $v=-\eta+c/2$. □

**Proposition 4.1.9.** *Let $a,b\in\mathbb{F}_q$ with $b\neq 0$, $b\neq a^4$ and $a\neq t$. The equation $x^\sigma-x=u$ defines an extension $F_2=F_1(x)$ with genus $g_2=5\sigma-2$ whose field of constants is $\mathbb{F}_q$.*

*Proof.* Let $\mathcal{H}_1$ be as in (4.4). By Proposition 4.1.8, $\mathcal{H}_1$ is a non-singular curve such that $F_1=\mathbb{F}_q(\mathcal{H}_1)$. Then places of $\mathbb{K}(u,v)$ can be identified with points of

$\mathcal{H}_1$. The ideal points of $\mathcal{H}_1$ are $P_1=(1:0:0)$, $Q_1=(0:1:0)$, $R_1=(1:\alpha:0)$ and $S_1=(\alpha:1:0)$, with $\alpha^2+\alpha+1=0$. The tangent lines at such points are

$$\begin{aligned}&\ell_{P_1}: V=(a-t), && \ell_{Q_1}: U=(a-t),\\ &\ell_{R_1}: U+(\alpha+1)V+\tfrac{(\alpha+2)(a+3t)}{3}=0 && \ell_{S_1}: U-\alpha V-\tfrac{(\alpha-1)(a+3t)}{3}=0.\end{aligned}$$

Here, the assumption $a\neq t$ assures that $U=0$ and $V=0$ are not tangent lines at the ideal points of $\mathcal{H}_1$; hence,

$$\begin{aligned}v_{P_1}(u)=v_{R_1}(u)=v_{S_1}(u)=-1,\quad v_{Q_1}(u)=0,\\ v_{Q_1}(v)=v_{R_1}(v)=v_{S_1}(v)=-1,\quad v_{P_1}(v)=0.\end{aligned}\tag{4.7}$$

Consider the function field $\mathbb{K}(u,v)(x)=\mathbb{K}(v,x)$ defined by $u=x^\sigma-x$. For each place centered at an affine point and for $Q_1$ there exists $\rho\in\mathbb{K}(u,v)$ such that the valuation of $u-(\rho^\sigma-\rho)$ at that place is non-negative; in fact, it is sufficient to consider $\rho=0$. Hence $\mathbb{K}(x,v)|\mathbb{K}(u,v)$ is a generalized Artin-Schreier extension and $[\mathbb{K}(x,v):\mathbb{K}(u,v)]=\sigma$. Moreover $P_1$, $R_1$, $S_1$ are the only totally ramified places;all other places are unramified. By Lemma 1.1.36, $\mathbb{F}_q$ is the full constant field of $F_2=\mathbb{F}_q(x,v)$. The genus is given by

$$g_2=\sigma g_1+\frac{\sigma-1}{2}\Big(-2+\sum_{P\in\mathbb{P}(\mathbb{K}(\mathcal{H}_1))}(m_P+1)\deg(P)\Big)=3\sigma+\frac{\sigma-1}{2}\left(-2+3(1+1)\right)=5\sigma-2.$$

□

From now on, denote by $P_2$, $R_2$, $S_2$ the places of $\mathbb{K}(x,y)$ lying over $P_1$, $R_1$, $S_1$, respectively. Also, let $Q_2^1,\ldots,Q_2^\sigma$ be the places lying over $Q_1$.

**Proposition 4.1.10.** *Let $a,b\in\mathbb{F}_q$ with $b\neq 0$, $b\neq a^4$ and $a\neq t$. The equation $y^\sigma-y=v$ defines an extension $F_3=F_2(y)$ with genus $g_3=6\sigma^2-2\sigma-1$ whose field of constants is $\mathbb{F}_q$.*

*Proof.* In $\mathbb{K}(x,v)$ we have

$$v_{P_2}(v)=0,\quad v_{Q_2^i}(v)=-1,\quad v_{R_2}(v)=v_{S_2}(v)=-\sigma.$$

The element $v-\alpha u\in\mathbb{K}(u,v)$ satisfies $v_{R_2}(v-\alpha u)=0$. Let $A\in\mathbb{K}$ be such that $A^\sigma=\alpha$ and consider $\rho=Ax$; then

$$v-(\rho^\sigma-\rho)=v-\alpha x^\sigma+Ax=v-\alpha x^\sigma+\alpha x-\alpha x+Ax=v-\alpha u-\alpha x+Ax.$$

Since $\alpha^2+\alpha+1=0$, we have that $A=\alpha$ if and only if $3\mid(\sigma-1)$. Then $A\neq\alpha$ by the assumptions on $\sigma$; in fact, $\sigma=p^{h'}$ with $h'$ odd and $p\equiv 2 \pmod{}$ imply that 3 does not divide $\sigma-1$. Thus, $v_{R_2}((A-\alpha)x)=-1$ and hence

$$v_{R_2}(v-((Ax)^\sigma-Ax))=v_{R_2}(x)=-1.$$

By taking $\rho = A^{-1}x$, the same argument yields $v_{S_2}(v - (\rho^\sigma - \rho)) = -1$. For the places centered at affine points and at $Q_2^i$, it is sufficient to choose $\rho = 0$. Then $\mathbb{K}(x,y)|\mathbb{K}(x,v)$ is a generalized Artin-Schreier extension with $[\mathbb{K}(x,y) : \mathbb{K}(x,v)] = \sigma$ and

$$\begin{aligned} g_3 &= \sigma g_2 + \frac{\sigma-1}{2}\Big(-2 + \sum_{P \in \mathbb{P}(\mathbb{K}(x,v))} (m_P + 1)\deg(P)\Big) \\ &= \sigma(5\sigma - 2) + \frac{\sigma-1}{2}(-2(\sigma-2)(1+1)) = 6\sigma^2 - 2\sigma - 1. \end{aligned}$$

By Lemma 1.1.36, $\mathbb{F}_q$ is the constant field of $F_3 = \mathbb{F}_q(x,y)$. □

In the extension $\mathbb{K}(x,y)|\mathbb{K}(x,v)$ the only totally ramified places are $Q_2^1, \ldots, Q_2^\sigma$, $R_2$ and $S_2$; let $Q_3^1, \ldots, Q_3^\sigma$, $R_3$ and $S_3$ be the places lying over them. All other places are unramified; denote by $P_3^i$ the places lying over $P_2$, $i = 1, \ldots, \sigma$.

**Proposition 4.1.11.** *Let $a, b \in \mathbb{F}_q$ with $b \neq 0$, $b \neq a^4$ and $a \neq t$. The equation*

$$\begin{gathered} w^2 + w((x^\sigma - x) + (y^\sigma - y) + 4t) + 4t(x^\sigma - x + y^\sigma - y) \\ +6t^2 + (x^\sigma - x)(y^\sigma - y) + (x^\sigma - x)^2 + (y^\sigma - y)^2 = 0 \end{gathered} \tag{4.8}$$

*defines an extension $F_4 = F_3(w)$ with genus $g_4 \leq 16\sigma^2 - 4\sigma - 3$ whose field of constants is $\mathbb{F}_q$.*

*Proof.* By the substitution $\theta = w + (x^\sigma - x + y^\sigma - y + 4t)/2$ we have $F_4 = F_3(\theta)$. By straightforward computations,

$$\theta^2 = -\frac{3}{4}(u+v)^2 + uv - 2t(u+v) - 2t^2 = -\frac{3}{4}\big(u - \beta_1 v + (1-\beta_1)t\big)\big(u - \beta_2 v + (1-\beta_2)t\big), \tag{4.9}$$

where $\beta_1, \beta_2$ are the two distinct solutions of $3T^2 + 2T + 3 = 0$. Let $h_1(U,V) = 0$ be the affine equation defining $\mathcal{H}_1$.

By straightforward computations, $h_1(\beta_1 V + (\beta_1 - 1)t, V) = 0$ if and only if

$$r(V) := (3 + 2\beta_1)(V+t)^4 + 2a(3 - \beta_1)(V+t)^3 - b = 0.$$

The coefficients of $r(V)$ are non-zero by the assumptions on $a$, $b$ and the characteristic $p$; as

$$r'(V) = 2(V+t)^2\left[2(3+2\beta_1)V + 3a(3-\beta_1)\right],$$

$(u - \beta_1 v + (1-\beta_1)t)$ provides at most one double zero of $\theta^2$ in $\mathbb{K}(u,v)$, so at least two simple zeros; the same holds for the second factor. The two factors have at most one common zero; then, there exists a zero $P$ of $\theta^2$ in $\mathbb{K}(u,v)$ with multiplicity 1, and hence $\theta^2$ is not a square in $\mathbb{K}(u,v)$. Let $P'$ be a place of $\mathbb{K}(x,y)$ lying over $P$; then $v_{P'}(\theta^2) \in \{1,\sigma,\sigma^2\}$ is odd, hence $\theta^2$ is not a square in $\mathbb{K}(x,y)$. Therefore $\mathbb{K}(x,y,\theta)|\mathbb{K}(x,y)$ is a Kummer extension. By (4.9), $\theta^2$ has valuation $-2$ at $P_1$, $Q_1$, $R_1$ and $S_1$; hence

$$v_{P_3^i}(\theta^2) = v_{Q_3^i}(\theta^2) = -2\sigma\,, \quad v_{R_3}(\theta^2) = v_{S_3}(\theta^2) = -2\sigma^2 \qquad (i = 1,\dots,\sigma). \quad (4.10)$$

The number of zeros of $\theta^2$ in $\mathbb{K}(x,y,\theta)$ is $\sigma^2$ times the number of its zeros in $\mathbb{K}(u,v)$, so at most $8\sigma^2$. Then

$$g_4 = 1 + 2(g_3 - 1) + \frac{1}{2}\sum_{P\in\mathbb{P}(\mathbb{K}(x,y))}(2 - r_P)\deg(P)$$

$$\leq 1 + 2(6\sigma^2 - 2\sigma - 2) + \frac{1}{2}8\sigma^2 = 16\sigma^2 - 4\sigma - 3.$$

Finally, by Lemma 1.1.36, $\mathbb{F}_q$ is the full constant field of $\mathbb{K}(x,y,\theta) = F_4$. □

Let $P_4^{i,j}$, $Q_4^{i,j}$, $R_4^j$ and $S_4^j$ $(j = 1,2)$ be the places of $\mathbb{K}(x,y,\theta)$ lying over the unramified places $P_3^i$, $Q_3^i$, $R_3$ and $S_3$, respectively.

**Proposition 4.1.12.** *Let $a,b \in \mathbb{F}_q$ with $b \neq 0$, $b \neq a^4$ and $a \neq t$. The equation $z^\sigma - z = w$ defines an extension $F_5 = F_4(z)$ with genus $g_5 \leq 30\sigma^3 - 12\sigma^2 - 4\sigma + 1$ whose field of constants is $\mathbb{F}_q$.*

*Proof.* Arguing as in the proof of Proposition 4.1.11, we have that $\mathbb{K}(u,v,\theta) : \mathbb{K}(u,v)$ is a Kummer extension of degree 2. The unique ramified places are the zeros of $\theta^2$ with odd multiplicity, and

$$g(\mathbb{K}(u,v,\theta)) \leq 1 + 2(g(\mathbb{K}(u,v)) - 1) + \frac{1}{2}\cdot 8 = 9.$$

Let $\tilde{P}_1^j$, $\tilde{Q}_1^j$, $\tilde{R}_1^j$ and $\tilde{R}_1^j$ $(j = 1,2)$ be the places of $\mathbb{K}(u,v,\theta)$ lying over $P_1$, $Q_1$, $R_1$ and $S_1$. Since $v_{\tilde{P}_1^j}(\theta^2) = -2$, we have $v_{\tilde{P}_1^j}(\theta) = -1 = v_{\tilde{P}_1^j}(u)$ and we can write $\theta = ku + \Phi$, for some $k \in \mathbb{K}$ and $\Phi \in \mathbb{K}(u,v,\theta)$ with $v_{\tilde{P}_1^j}(\Phi) \geq 0$. Thus,

$$v_{\tilde{P}_1^j}\left(\theta^2 - k^2u^2\right) = v_{\tilde{P}_1^j}\left(2ku\Phi + \Phi^2\right) \geq -1.$$

On the other hand, from (4.9) we have

$$v_{\tilde{P}_1^j}\left(\theta^2 - k^2u^2\right) = v_{\tilde{P}_1^j}\left(\left(-\frac{3}{4} - k^2\right)u^2 - \frac{3}{4}v^2 - \frac{1}{2}uv - 2t\,(u+v) - 2t^2\right)$$

and $v_{\tilde{P}_1^j}(u^2) = -2$, whereas, by (4.7), the other terms have valuation greater than or equal to $-1$ at $\tilde{P}_1^j$. Therefore the coefficient $(-3/4 - k^2)$ must vanish. By our assumptions on $\sigma$, $-3$ is not a square in $\mathbb{F}_\sigma$ (see Lemma 4.5 in [48]). Then $k \notin \mathbb{F}_\sigma$, and there exists a $\sigma$-th root $e_\sigma \in \mathbb{K}$ of $k$ with $e_\sigma \neq k$. Let $\rho = e_\sigma x$; then

$$\theta-(\rho^\sigma-\rho) = k(x^\sigma-x)+\Phi-e_\sigma^\sigma x^\sigma+e_\sigma x = (k-e_\sigma^\sigma)x^\sigma+(e_\sigma-k)x+\Phi = (e_\sigma-k)x+\Phi.$$

$\mathbb{K}(x,y,\theta)$ is the compositum of $\mathbb{K}(u,v,\theta)$ and $\mathbb{K}(x,y)$; hence, at the places $P_4^{i,j}$ over $P_1$ we have

$$v_{P_4^{i,j}}(\Phi) = e(P_4^{i,j} \mid \tilde{P}_1^j) \cdot v_{\tilde{P}_1^j}(\Phi) \geq 0\,, \qquad v_{P_4^{i,j}}(x) = e(P_4^{i,j} \mid P_3^i) \cdot v_{P_3^i}(x) = -1.$$

Therefore

$$v_{P_4^{i,j}}(\theta - (\rho^\sigma - \rho)) = -1. \tag{4.11}$$

Now we prove that

$$\mu\,\theta \neq \xi^p - \xi \quad \text{for all} \quad \xi \in \mathbb{K}(x,y,\theta), \mu \in \mathbb{F}_\sigma.$$

On the contrary, assume $\mu\,\theta = \xi^p - \xi$ with $\xi \in \mathbb{K}(x,y,\theta), \mu \in \mathbb{F}_\sigma$. From (4.11),

$$-1 = v_{P_4^{i,j}}(\mu\theta - (\mu\rho^\sigma - \mu\rho)) = v_{P_4^{i,j}}(\mu\theta - (w^\sigma - w)),$$

with $w = \mu\rho \in \mathbb{K}(x,y,\theta)$. Since

$$w^\sigma - w = \left(w^{\sigma/p} + w^{\sigma/p^2} + \ldots + w\right)^p - \left(w^{\sigma/p} + w^{\sigma/p^2} + \ldots + w\right),$$

we have

$$v_{P_4^{i,j}}(\xi^p - \xi - (\lambda^p - \lambda)) = -1,$$

where $\lambda = w^{\sigma/p} + w^{\sigma/p^2} + \ldots + w \in \mathbb{K}(u,v,\theta)$. But this is clearly impossible, since the valuation of $(\xi^p - \xi - (\lambda^p - \lambda))$ must be either non-negative or a multiple of $p$. Then we can apply Lemma 1.3 in [46] to conclude that $T^\sigma - T - \theta$ is irreducible over $\mathbb{K}(x,y,\theta)$, and $\mathbb{K}(x,y,z)|\mathbb{K}(x,y,\theta)$ is a Galois extension of degree $\sigma$. Also, by Lemma 1.1.36, $\mathbb{F}_q$ is the full constant field of $\mathbb{F}_q(x,y,z)$.

Finally we give a bound on $g_5$. By Castelnuovo's Inequality (see Theorem 3.11.3 in [107]),

$$\begin{aligned} g_5 \leq\ & [\mathbb{K}(x,y,z):\mathbb{K}(x,y)] \cdot g(\mathbb{K}(x,y)) + [\mathbb{K}(x,y,z):\mathbb{K}(u,v,z)] \cdot g(\mathbb{K}(u,v,z)) + \\ & + ([\mathbb{K}(x,y,z):\mathbb{K}(x,y)] - 1) \cdot ([\mathbb{K}(x,y,z):\mathbb{K}(u,v,z)] - 1)\ . \end{aligned}$$

We have

$$[\mathbb{K}(x,y,z):\mathbb{K}(x,y)] = [\mathbb{K}(x,y,z):\mathbb{K}(x,y,\theta)]\cdot[\mathbb{K}(x,y,\theta):\mathbb{K}(x,y)] = 2\sigma\,,$$

$$g(\mathbb{K}(x,y)) = 6\sigma^2-2\sigma-1\,.$$

Since $\{x,x^2,\ldots,x^\sigma\}$ is a basis of $\mathbb{K}(x,v,z)$ over $\mathbb{K}(u,v,z)$ and $\{y,y^2,\ldots,y^\sigma\}$ is a basis of $\mathbb{K}(x,y,z)$ over $\mathbb{K}(x,v,z)$, then $\{x^iy^j \mid i,j=1,\ldots,\sigma\}$ is a basis of $\mathbb{K}(x,y,z)$ over $\mathbb{K}(u,v,z)$ and $[\mathbb{K}(x,y,z):\mathbb{K}(u,v,z)]=\sigma^2$. Since $P_1$, $Q_1$, $R_1$, and $S_1$ do not ramify in $\mathbb{K}(u,v,\theta)|\mathbb{K}(u,v)$, then $\theta^2$ has valuation $-2$ at the places lying over them; hence,

$$v_{\tilde{P}_1^j}(\theta)=v_{\tilde{Q}_1^j}(\theta)=v_{\tilde{R}_1^j}(\theta)=v_{\tilde{S}_1^j}(\theta)=-1\,,\qquad \text{for } j=1,2\,,$$

whereas $\theta$ has non-negative valuation at any other place of $\mathbb{K}(u,v,\theta)$. Hence $\mathbb{K}(u,v,z)|\mathbb{K}(u,v,\theta)$, with $\theta=z^\sigma-z$, is a generalized Artin-Schreier extension of degree $\sigma$ and

$$g(\mathbb{K}(u,v,z)) = \sigma\, g(\mathbb{K}(u,v,\theta)) + \frac{\sigma-1}{2}\left(-2+\sum_{P\in\mathbb{P}(\mathbb{K}(u,v,\theta))}(m_P+1)\deg(P)\right)\le$$

$$\le 9\sigma+\frac{\sigma-1}{2}(-2+8(1+1)) = 16\sigma-7\,.$$

Therefore

$$g_5 \;\le\; 2\sigma(6\sigma^2-2\sigma-1)+\sigma^2(16\sigma-7)+(2\sigma-1)(\sigma^2-1) = 30\sigma^3-12\sigma^2-4\sigma+1\,.$$

□

**Theorem 4.1.13.** *Let $\mathcal{K}_t$ as in (4.2). If $q\ge 3600\,\sigma^6$ then $\mathcal{K}_t$ is a 3-arc which covers all points of* $\mathrm{AG}(2,q)\setminus\mathcal{Q}$ *except possibly those lying on the line $Y=0$.*

*Proof.* Let $P=(a,b)\in\mathrm{AG}(2,q)\setminus\mathcal{Q}$ and assume that $a\ne t$ and $b\ne 0$. We start by counting the number $Z_1$ of poles of $x^\sigma-x$, $y^\sigma-y$, and $z^\sigma-z$ in $F_5$. The poles of $x^\sigma-x$ are the places lying over $P_1$, $R_1$, and $S_1$ in $F_5|F_1$, and hence over $P_4^{i,j}$, $R_4^j$, and $S_4^j$ in $F_5|F_4$ ($i=1,\ldots,\sigma$, $j=1,2$). The extension $F_5|F_4$ has degree $\sigma$; then, by the Fundamental Equality 1.1.1, $x^\sigma-x$ has at most $\sigma(2\sigma+4)$ poles in $F_5$. By similar arguments it can be shown that the number of poles in $F_5$ is at most $\sigma(2\sigma+4)$ for $y^\sigma-y$ and at most $\sigma(4\sigma+4)$ for $z^\sigma-z$. Summing up,

$$Z_1\le\sigma(2\sigma+4)+\sigma(2\sigma+4)+\sigma(4\sigma+4)=8\sigma^2+12\sigma.$$

Now count the number $Z_2$ of zeros of $(x^\sigma - x) - (y^\sigma - y)$ in $F_5$. Clearly a place $P_5$ is a zero of $(x^\sigma - x) - (y^\sigma - y) = (x-y)^\sigma - (x-y)$ if and only if it is a zero of $x - y - \lambda$ for some $\lambda \in \mathbb{F}_\sigma$; then,

$$Z_2 \leq \sum_{\lambda \in \mathbb{F}_\sigma} \deg(x-y-\lambda)_0 = \sum_{\lambda \in \mathbb{F}_\sigma} \deg(x-y-\lambda)_\infty.$$

The poles of $x-y-\lambda$ are the places lying over $P_1$, $Q_1$, $R_1$, and $S_1$. Then, by the Fundamental Equality 1.1.1,

$$\deg(x-y-\lambda)_\infty = 4 \cdot [F_5 : F_1] = 8\sigma^3 \quad \text{for all} \quad \lambda \in \mathbb{F}_\sigma\,;$$

hence, $Z_2 \leq 8\sigma^4$. Therefore, if the number $N_q$ of $\mathbb{F}_q$-rational places of $F_5$ is greater than

$$8\sigma^4 + 8\sigma^2 + 12\sigma,$$

then there exists an $\mathbb{F}_q$-rational place $P$ of $F_5$ such that $(x(P), y(P), z(P))$ is a well-defined affine point of $\mathcal{H}_P$ with $x(P)^\sigma - x(P)$, $y(P)^\sigma - y(P)$, $z(P)^\sigma - z(P)$ pairwise distinct. By Hasse-Weil bound we have

$$N_q \;\geq\; q + 1 - 2g_5\sqrt{q} \;\geq\; q + 1 - 2(30\sigma^3 - 12\sigma^2 - 4\sigma + 1)\sqrt{q}.$$

From $q \geq 3600\,\sigma^6$ it follows that

$$q + 1 - 2(30\sigma^3 - 12\sigma^2 - 4\sigma + 1)\sqrt{q} \;\geq\; 8\sigma^4 + 8\sigma^2 + 12\sigma + 1,$$

and hence, by Corollary 4.1.6, the point $P$ is collinear with three distinct points of $\mathcal{K}_t$.

Assume now that $P = (t, b)$ with $b \neq 0$. Let $t' \in M + t$, with $t' \neq t$, and consider the curve $\mathcal{H}'_P$ obtained by replacing $t$ with $t'$ in Eq. (4.3). Arguing as above, $\mathcal{K}_{t'}$ covers the point $P$. But clearly $\mathcal{K}_t = \mathcal{K}_{t'}$, and the assertion follows. □

### 4.1.3 Constructions of 4-independent subsets

We now want to construct complete $(k,3)$-arcs from union of cosets $\mathcal{K}_t$; to this end, we will use the notion of a 4-independent subset of an elementary abelian $p$-group.

**Definition 4.1.14.** *Let $G$ be a finite abelian group and let $\mathcal{T}$ be a subset of $G$. If*

$$y_1 + y_2 + y_3 + y_4 \neq 0 \quad \textit{for all} \quad y_1, y_2, y_3, y_4 \in \mathcal{T},$$

*then $\mathcal{T}$ is said to be a* 4-independent subset *of $G$. An element $g \in G \backslash \mathcal{T}$ is* covered *by $\mathcal{T}$ if either $g \in \mathcal{T}$ or*

$$\textit{there exist } y_1, y_2, y_3 \in \mathcal{T} \textit{ such that } y_1 + y_2 + y_3 + g = 0.$$

In the remaining part of the section we construct 4-independent subsets of the abelian group $\mathbb{Z}_p^{h'}$, for $h'$ an odd integer and $p \geq 5$. We distinguish the cases $h' = 1$ and $h' \geq 3$. For a subset $A$ of a group $G$, let $s^\wedge A$ denote the $s$-fold sumset of $A$, that is,

$$s^\wedge = \{y_1 + \cdots + y_s \mid y_1, \ldots, y_s \in A\}.$$

In the following, let $[a, b]$ denote the set of elements in $\mathbb{Z}_p$ represented by integers $x$ with $a \leq x \leq b$.

**Proposition 4.1.15.** *Let $p \geq 29$ be a prime, with $p \equiv 1 \bmod 4$. Then*

$$\mathcal{T} = \{-1, 2\} \cup \left[4, \frac{p-1}{4}\right]$$

*is a 4-independent subset covering $\mathbb{Z}_p \setminus \{1\}$.*

*Proof.* The sum of four elements of $\mathcal{T}^* = \{2\} \cup \left[4, \frac{p-1}{4}\right]$ is contained in $[8, p-1]$ and therefore is different from 0. An easy check shows that if one or more of the four elements is $-1$, then it is not possible to obtain 0. Note that $p \geq 29$ guarantees that the element 4 is in $(-2 + \mathcal{T}^*)$. Then

$$3^\wedge\mathcal{T} = \{-3\} \cup (-2 + \mathcal{T}^*) \cup (-1 + 2^\wedge\mathcal{T}^*) \cup 3^\wedge\mathcal{T}^*$$

$$= \{-3\} \cup \{0\} \cup \left[2, \frac{p-9}{4}\right] \cup \{3\} \cup \left[5, \frac{p-3}{2}\right] \cup \{6\} \cup \left[8, 3\frac{p-1}{4}\right] = \{-3, 0\} \cup \left[2, 3\frac{p-1}{4}\right].$$

Hence, the set of covered elements contains

$$-3^\wedge\mathcal{T} = \{0, 3\} \cup \left[\frac{p-1}{4} + 1, p-2\right].$$

The non-covered element 1 cannot be added to $\mathcal{T}$ since $1 + 1 - 1 - 1 = 0$. □

**Proposition 4.1.16.** *Let $p > 29$ be a prime with $p \equiv 3 \bmod 4$. Then*

$$\mathcal{T} = \{-1, 2\} \cup \left[4, \frac{p-3}{4}\right]$$

*is a 4-independent subset of $\mathbb{Z}_p$ covering $\mathbb{Z}_p \setminus \left\{1, \frac{p+1}{4}, \frac{p+5}{4}\right\}$.*

*Proof.* The sum of four elements of $\mathcal{T}^* = \{2\} \cup \left[4, \frac{p-3}{4}\right]$ is contained in $[8, p-3]$, and therefore is different from 0. An easy check shows that if one or more of the four elements is $-1$, then it is not possible to obtain 0. From $p > 29$ it follows that the element 4 is in $(-2 + \mathcal{T}^*)$. Arguing as Proposition 4.1.15,

$$\begin{aligned} 3^\wedge\mathcal{T} &= \{-3\} \cup (-2+\mathcal{T}^*) \cup (-1 + 2^\wedge\mathcal{T}^*) \cup 3^\wedge\mathcal{T}^* = \\ &= \{-3\} \cup \{0\} \cup \left[2, \frac{p-11}{4}\right] \cup \{3\} \cup \left[5, \frac{p-5}{2}\right] \cup \{6\} \cup \left[8, 3\frac{p-3}{4}\right] \\ &= \{-3, 0\} \cup \left[2, 3\frac{p-3}{4}\right]. \end{aligned}$$

Then the the set of covered elements contains

$$-3^\wedge\mathcal{T} = \{0,3\} \cup \left[\frac{p+9}{4}, p-2\right].$$

Also, note that the non-covered elements $1, \frac{p+1}{4}, \frac{p+5}{4}$ cannot be added to $\mathcal{T}$ since

$$1+1-1-1=0, \quad \frac{p+1}{4}+\frac{p+1}{4}+\frac{p+1}{4}+\frac{p-3}{4} = p, \quad \frac{p+5}{4}+\frac{p+5}{4}+\frac{p-3}{4}+\frac{p-7}{4} = p.$$

□

We now consider the case $G = \mathbb{Z}_p^{h'}$ for $h' \geq 3$. Clearly, $G$ can be written as $G = A \times B \times C$, with $A = \mathbb{Z}_p$, $B = C = \mathbb{Z}_p^{\frac{h'-1}{2}}$. Let

$$\mathcal{T} = \mathcal{T}_1 \cup \mathcal{T}_2 \cup \mathcal{T}_3, \tag{4.12}$$

where $\mathcal{T}_1 = \{(a,1,1) \mid a \in A\}$, $\mathcal{T}_2 = \{(1,b,1) \mid b \in B \setminus \{-3\}\}$, $\mathcal{T}_3 = \{(1,1,c) \mid c \in C \setminus \{-3\}\}$. Here, 1 and $-3$ are viewed as elements of the additive group of the finite field $\mathbb{F}_{p^{\frac{h'-1}{2}}}$, which is isomorphic to $B$ and $C$.

**Proposition 4.1.17.** *Let $h' \geq 3$ and let $\mathcal{T}$ be as in (4.12). Then $\mathcal{T}$ is a 4-independent subset of $\mathbb{Z}_p^{h'}$ of size $2p^{\frac{h'-1}{2}}+p-4$ not covering at most $2\big(p^{\frac{h'+1}{2}}-p^{\frac{h'-1}{2}}\big)$ elements of $\mathbb{Z}_p^{h'}$.*

*Proof.* Consider four elements $t_1, t_2, t_3, t_4 \in \mathcal{T}$. If $t_1, t_2, t_3, t_4$ belong either to the same $\mathcal{T}_i$ or to exactly two distinct $\mathcal{T}_i$'s, then they all share 1 in one of the coordinates, and therefore $t_1+t_2+t_3+t_4 \neq (0,0,0)$ holds. Assume then that $t_1, t_2, t_3, t_4$ belong to all the three $\mathcal{T}_i$'s. If three of them belong to $\mathcal{T}_1 \cup \mathcal{T}_2$, then the remaining element has the third coordinate different from $-3$; therefore, $t_1+t_2+t_3+t_4 \neq (0,0,0)$ holds. Otherwise, three of them belong to $\mathcal{T}_1 \cup \mathcal{T}_3$, the remaining element has the second coordinate different from $-3$, and their sum cannot be equal to $(0,0,0)$. This proves that $\mathcal{T}$ is a 4-independent subset of $\mathbb{Z}_p^{h'}$. Now, let $t = (x,y,z) \in \mathbb{Z}_p^{h'} \setminus \mathcal{T}$ with $y \neq 1$ and $z \neq 1$, Then

$$(x,y,z) + (-2-x,1,1) + (1,-2-y,1) + (1,1,-2-z) = (0,0,0),$$

and hence $t$ is covered by $\mathcal{T}$. □

### 4.1.4 Construction of $(k, 3)$-arcs from union of cosets of $M$

We first fix two (not necessarily distinct) subsets $\mathcal{K}_{t_1}$ and $\mathcal{K}_{t_2}$, defined as in (4.2), and a point $P = (w, w^4)$ in $\mathcal{Q} \setminus (\mathcal{K}_{t_1} \cup \mathcal{K}_{t_2})$. Clearly $P$ belongs to some subset $\mathcal{K}_{t_P}$ for some $t_P \in \mathbb{F}_q$.

Let $P_1 = (x^\sigma - x + t_1, (x^\sigma - x + t_1)^4) \in \mathcal{K}_{t_1}$ and $P_2 = (y^\sigma - y + t_2, (y^\sigma - y + t_2)^4) \in \mathcal{K}_{t_2}$. By Proposition 4.1.2, the three points $P$, $P_1$, and $P_2$ are collinear if and only if

$$(x^\sigma-x+t_1)^2+(y^\sigma-y+t_2)^2+(x^\sigma-x+t_1)(y^\sigma-y+t_2)+w(x^\sigma-x+t_1+y^\sigma-y+t_2)+w^2 = 0. \tag{4.13}$$

**Proposition 4.1.18.** *Equation 4.13 defines a function field $L = \mathbb{F}_q(x, y)$ with genus $g = \sigma^2 - 1$ whose field of constants is $\mathbb{F}_q$.*

*Proof.* Consider first the plane curve $\Gamma_0$ with equation

$$f_0(U, V) = (U + t_1)^2 + (V + t_2)^2 + (U + t_1)(V + t_2) + w(U + t_1 + V + t_2) + w^2 = 0$$

The ideal points of $\Gamma_0$ are the simple points $R_1 = (1 : \alpha : 0)$ and $S_1 = (\alpha : 1 : 0)$, where $\alpha^2 + \alpha + 1 = 0$; all affine points are non-singular since $w \neq 0$. Then $\Gamma_0$ is an irreducible conic. Let $L_0 = \mathbb{F}_q(u, v)$ be the function field of $\Gamma_0$, where $f_0(u, v) = 0$. The rational function $u \in \mathbb{K}(u, v)$ has valuation $-1$ at $R_1$ and $S_1$, and non-negative valuation at the placed centered at affine points of $\Gamma_0$. Then $\mathbb{K}(x, v)|\mathbb{K}(u, v)$, with $u = x^\sigma - x$, is a generalized Artin-Schreier extension, and

$$g(\mathbb{K}(x, v)) = \sigma \cdot g(\mathbb{K}(u, v)) + \frac{\sigma - 1}{2}\Big(-2 + \sum_{P \in \mathbb{P}(\mathbb{K}(u,v))} (m_P + 1)\deg(P)\Big)$$

$$= \frac{\sigma - 1}{2}(-2 + 4) = \sigma - 1.$$

The places $R_1$ and $S_1$ are the unique totally ramified places; let $\overline{R}_1$ and $\overline{S}_1$ be the places lying over them. The other places are unramified. By Lemma 1.1.36, $\mathbb{F}_q$ is the constant field of $\mathbb{F}_q(u, v)$.

Now consider the element $v \in \mathbb{K}(x, v)$; we have $v_{\overline{R}_1}(v - \alpha u) = 0$. For $A \in \mathbb{K}$ such that $A^\sigma = \alpha$, let $\rho = Ax$; then

$$v - (\rho^\sigma - \rho) = v - \alpha x^\sigma + Ax = v - \alpha x^\sigma + \alpha x - \alpha x + Ax = v - \alpha u - \alpha x + Ax.$$

Since $\alpha^2 + \alpha + 1 = 0$, we have that $A = \alpha$ if and only if $3 \mid (\sigma - 1)$. Then $A \neq \alpha$ by our assumptions on $\sigma$, so $v_{\overline{R}_1}((A - \alpha)x) = -1$, and hence $v_{\overline{R}_1}(v - (\rho^\sigma - \rho)) = -1$.

By taking $\rho = A^{-1}x$, the same argument yields $v_{\overline{S}_1}(v-(\rho^\sigma-\rho)) = -1$. For the places centered at affine points it is sufficient to choose $\rho = 0$. Then $\mathbb{K}(x,y)|\mathbb{K}(x,v)$ is a generalized Artin-Schreier extension with $[\mathbb{K}(x,y) : \mathbb{K}(x,v)] = \sigma$; in this extension the unique totally ramified places are $\overline{R}_1$ and $\overline{S}_1$ while the others are unramified. Then,

$$g = \sigma \cdot g(\mathbb{K}(x,v)) + \frac{\sigma-1}{2}\Big( -2 + \sum_{P\in\mathbb{P}(x,v)} (m_P+1)\deg(P)\Big)$$

$$= \sigma(\sigma-1) + \frac{\sigma-1}{2}(-2+4) = \sigma^2-1.$$

By Lemma 1.1.36, $\mathbb{F}_q$ is the constant field of $L$. □

**Proposition 4.1.19.** *Assume that $q \geq 5\sigma^4$. Then $P$ is collinear with two distinct points $P_1 \in \mathcal{K}_{t_1}$ and $P_2 \in \mathcal{K}_{t_2}$.*

*Proof.* We are going to show that there exist $x_0, y_0 \in \mathbb{F}_q$ such that (4.13) holds for $x = x_0$ and $y = y_0$, and $x_0^\sigma - x_0 \neq y_0^\sigma - y_0$. We start by counting the number of poles of $x^\sigma - x = u$ and $y^\sigma - y = v$ in $L$. They are the places lying over the totally ramified places $R_1$ and $S_1$ in $L_1|L_0$; hence, the number of such poles is 2. Next we count the number $Z$ of zeros of $(x^\sigma - x) - (y^\sigma - y)$ in $L$. A place $P$ is a zero of $(x^\sigma - x) - (y^\sigma - y) = (x-y)^\sigma - (x-y)$ if and only if it is a zero of $x - y - \lambda$ for some $\lambda \in \mathbb{F}_\sigma$; then

$$Z \leq \sum_{\lambda\in\mathbb{F}_\sigma} \deg(x-y-\lambda)_0 = \sum_{\lambda\in\mathbb{F}_\sigma} \deg(x-y-\lambda)_\infty.$$

The poles of $x - y - \lambda$ are the places lying over $R_1$ and $S_1$ in $L_1|L_0$; then, by the Fundamental Equation 1.1.1,

$$\deg(x-y-\lambda)_\infty = 2 \cdot [L : L_0] = 2\sigma^2$$

for all $\sigma \in \mathbb{F}_\sigma$; hence, $Z \leq 2\sigma^3$.

Therefore, if the number $N_q$ of $\mathbb{F}_q$-rational places of $\Gamma$ is greater than $2\sigma^3 + \sigma$, then there exists an $\mathbb{F}_q$-rational place $P$ of $L$ such that the point $(x_0, y_0) = (x(P), y(P))$ is well-defined and $x_0^\sigma - x_0 \neq y_0^\sigma - y_0$. By the Hasse-Weil bound,

$$N_q \geq q + 1 - 2g\sqrt{q} = q + 1 - 2(\sigma^2-1)\sqrt{q}.$$

Our hypothesis $q \geq 5\sigma^4$ implies

$$q + 1 - 2g\sqrt{q} \geq 2\sigma^3 + 2 + 1.$$

This completes the proof. □

**Proposition 4.1.20.** *Assume that $q \geq 11\sigma^4$. Then $P$ is collinear with three distinct points $P_1 \in \mathcal{K}_{t_1}$, $P_2 \in \mathcal{K}_{t_2}$, and $P_3 \in \mathcal{Q}$.*

*Proof.* By Proposition 4.1.19, $P$ is collinear with two distinct points $P_1 \in \mathcal{K}_{t_1}$, $P_2 \in \mathcal{K}_{t_2}$. The line through $P_1$, $P_2$, and $P$ can be a tangent line to the curve $\mathcal{Q}$. Note that there are at most four tangent lines through $P$ to the curve $\mathcal{Q}$; in fact, imposing that $P$ lies on the tangent to $\mathcal{Q}$ at the point $(X, X^4)$ gives an equation in $X$ of degree 4. Since each tangent line can be obtained from two pairs, we need at least nine distinct pairs of points $P_1^i$, $P_2^i$ such that $P_1^i$ and $P_2^i$ are collinear with $P$ $(i = 1, \dots, 9)$. Arguing as in the proof of Proposition 4.1.19, it is sufficient to require that the number of $\mathbb{F}_q$-rational places of $L$ is greater than $9 \cdot 2\sigma^3 + 2 = 18\sigma^3 + 2$. This is implied by the Hasse-Weil bound, together with $q \geq 11\sigma^4$. □

Henceforth, $\mathcal{T}$ denotes a 4-independent subset of $\mathbb{F}_q/M$, for $M$ as in (4.1). Let

$$\mathcal{K}_{\mathcal{T}} = \bigcup_{M+t \in \mathcal{T}} \mathcal{K}_t. \tag{4.14}$$

**Proposition 4.1.21.** *The set $\mathcal{K}_{\mathcal{T}}$ is a $(k,3)$-arc.*

*Proof.* By Proposition 4.1.3, the sum of the first coordinate of 4 collinear points on $\mathcal{Q}$ is equal to 0. This is clearly impossible if the points belong to $\mathcal{K}_{\mathcal{T}}$, since $\mathcal{T}$ is a 4-independent subset of $\mathbb{F}_q/M$. □

**Proposition 4.1.22.** *Assume that $q \geq 11\sigma^4$. Let $Cov(\mathcal{T})$ be the set of all the elements of $\mathbb{F}_q/M$ covered by $\mathcal{T}$ as 4-independent subset. Then the points in*

$$\bigcup_{M+t \in Cov(\mathcal{T})} \mathcal{K}_t$$

*are covered by $\mathcal{K}_{\mathcal{T}}$.*

*Proof.* Let $P \in \mathcal{K}_{t_P}$ with $M + t_P \in Cov(\mathcal{T})$. Then there exist $M+t_1, M+t_2, M+t_3 \in \mathcal{T}$ such that $t_P + t_1 + t_2 + t_3 \in M$. Also, by Proposition 4.1.20, there exist three distinct points $P_1 \in \mathcal{K}_{t_1}$, $P_2 \in \mathcal{K}_{t_2}$, and $P_3 \in \mathcal{Q}$ which are collinear with $P$. Let $t_3'$ be such that $P_3 \in \mathcal{K}_{t_3'}$. By Proposition 4.1.3, $t_P + t_1 + t_2 + t_3' \in M$. Then $M + t_3 = M + t_3'$, that is, $\mathcal{K}_{t_3} = \mathcal{K}_{t_3'}$; hence, $P_1$, $P_2$, $P_3$ all belong to $\mathcal{T}$ and the assertion follows. □

**Theorem 4.1.23.** *Let $\mathcal{T}$ be a 4-independent subset of $\mathbb{F}_q/M$ of size $n$, not covering at most $m$ elements of $\mathbb{F}_q/M$. Let $\mathcal{K}_{\mathcal{T}}$ be as in (4.14). Assume that $q \geq 3600\,\sigma^6$. Then there exists a complete $(k,3)$-arc $\mathcal{K}$ with $\mathcal{K}_{\mathcal{T}} \subseteq \mathcal{K} \subseteq \mathcal{Q}$ of size at most*

$$(n+m)\frac{q}{\sigma}+6.$$

*Proof.* Fix a coset $M+t$ in $\mathcal{T}$. By Theorem 4.1.13 all the points of $\mathrm{PG}(2,q) \setminus \mathcal{Q}$ are covered by a $\mathcal{K}_t$ plus at most six points covering the lines $Y=0$ and $T=0$. By Proposition 4.1.22, there are at most $m\frac{q}{\sigma}$ affine points of $\mathcal{Q}$ not covered by $\mathcal{K}_{\mathcal{T}}$. This shows that there exists a complete $(k,3)$-arc $\mathcal{K}$ containing $\mathcal{K}_{\mathcal{T}}$ of size at most

$$|\mathcal{K}_{\mathcal{T}}| + m\frac{q}{\sigma}+6 = (n+m)\frac{q}{\sigma}+6.$$

□

We are finally in a position to prove Theorem 4.1.1. Identify the additive groups $\mathbb{Z}_p^{h'}$ and $\mathbb{F}_q/M$. From Propositions 4.1.15, 4.1.16, and 4.1.17 the following values of $n$ and $m$ occur in Theorem 4.1.23:

- for $\sigma = p$, $p \equiv 1 \pmod 4$, $p \geq 29$, we have $n = \frac{p-5}{4}$ and $m=1$;
- for $\sigma = p$, $p \equiv 3 \pmod 4$, $p > 29$, we have $n = \frac{p-7}{4}$ and $m=3$;
- for $\sigma \geq p^3$, we have $n = 2p^{\frac{h'-1}{2}} + p - 4$ and $m = 2\big(p^{\frac{h'+1}{2}} - p^{\frac{h'-1}{2}}\big)$.

## 4.2 Complete $(k,4)$-arcs from quintic curves

In this section we provide a new class of infinite families of complete $(k,4)$-arcs in $\mathrm{PG}(2,q)$. Our main result is the following.

**Theorem 4.2.1.** *Let $\sigma$ be a non-square power of a prime $p>3$, with $p \equiv 3 \pmod 4$. Define*

$$\tau(\sigma) = \begin{cases} \frac{p+4i-10}{5} & if \quad \sigma = p \geq 29,\ \sigma \equiv i \in \{1,2,3,4\} \pmod 5,\\ 2\sqrt{\frac{\sigma}{p}}+p-2 & if \quad \sigma \geq p^3. \end{cases}$$

*Then, for each power $q$ of $\sigma$ with $q \geq 580644\sigma^8$, there exists a complete $(k,4)$-arc in $\mathrm{PG}(2,q)$ of size*

$$k \leq \frac{\tau(\sigma)}{\sigma}q + 8.$$

The order of magnitude of the $(k,4)$-arcs constructed in Theorem 4.2.1 is significantly smaller than that of the previously known families. In fact, complete $(k,4)$-arcs arising from quartic curves have at least $q+1-6\sqrt{q}$ points. The size of the arcs of Theorem 4.2.1 is asymptotically smaller than $q$. For example, if $\sigma = p^3$ with $p > 83$, then $q = \sigma^9$ can be chosen and the bound on $k$ is roughly $q^{25/27}$.

This section is organized as follows. Section 4.2.1 shows how to construct complete $(k,4)$-arcs from quartic curves, with $k \geq q-6\sqrt{q}+1$. In Section 4.2.2 we construct a $(q/\sigma,4)$-arc $\mathcal{K}_e$ lying on $\mathcal{Q}$; it is associated to an additive subgroup $M$ with index $\sigma$ in $\mathbb{F}_q$. We show in Section 4.2.3 that under the conditions of Theorem 4.2.1, the 4-secants of $\mathcal{K}_e$ covers almost all points of $\mathrm{PG}(2,q) \setminus \mathcal{Q}$. To this end, we thoroughly investigate the curve $\mathcal{H}_P$ and its function field. A 5-independent subset in the factor group $\mathbb{F}_q/M$ is constructed in Section 4.2.4. This allows us to show in Section 4.2.5 how to cover the points of $\mathcal{Q}$, for $q$ large enough, by joining more copies of $\mathcal{K}_e$.

### 4.2.1 $(k,4)$-arcs from quartic curves

An absolutely irreducible quartic curve is always a $(k,4)$-arc. By the Hasse-Weil bound its size is lower bounded by $q-6\sqrt{q}+1$. In the following we show how to construct a complete $(k,4)$-arc starting from a particular quartic curve.

Let $q$ be a power of a prime $p > 3$ and $\mathcal{C} = \{(x,x^4) \mid x \in \mathbb{F}_q\}$ be the set of the $\mathbb{F}_q$-rational affine points of the plane curve with equation $Y = X^4$. As usual, $\mathbb{K}$ denotes the algebraic closure of $\mathbb{F}_q$.

**Proposition 4.2.2.** *Four distinct points $A = (u,u^4)$, $B = (v,v^4)$, $C = (w,w^4)$, $D = (t,t^4)$ of $\mathcal{C}$ and $P = (a,b) \in \mathrm{AG}(2,q) \setminus \mathcal{C}$ are collinear if and only if*

$$\begin{cases} u+v+w+t=0 \\ w^2+(u+v)w+u^2+uv+v^2=0 \\ a(u^2+v^2)(u+v)-uv(u^2+uv+v^2)-b=0 \end{cases} . \tag{4.15}$$

*Proof.* The claim follows from Propositions 4.1.3 and 4.1.5. □

**Proposition 4.2.3.** *Let $a,b \in \mathbb{F}_q$ with $b \neq a^4$. The equation $\ell_1(u,v) = 0$, where*

$$\ell_1(u,v) = a(u^2+v^2)(u+v) - uv(u^2+uv+v^2) - b, \tag{4.16}$$

*defines a function field $E_1 = \mathbb{F}_q(u,v)$ with genus at most 3 whose field of constants is $\mathbb{F}_q$.*

*Proof.* Let $\mathcal{E}_1$ be the plane quartic curve with affine equation $\ell_1(U,V) = 0$, with $\ell_1$ as in (4.16). If $b = 0$ then the affine point $O = (0,0)$ is an ordinary triple point and no lines through $O$ are contained in $\mathcal{E}_1$. Therefore $\mathcal{E}_1$ is absolutely irreducible. If $b \neq 0$ then it is easily seen that $\mathcal{E}_1$ is nonsingular, and hence irreducible with genus 3. Since $E_1$ is the function field $\mathbb{F}_q(\mathcal{E}_1)$ of $\mathcal{E}_1$, the claim follows. □

**Proposition 4.2.4.** *Let $a, b \in \mathbb{F}_q$ with $b \neq a^4$. The equation*

$$w^2 + (u+v)w + u^2 + uv + v^2 = 0 \tag{4.17}$$

*defines an extension $E_2 = E_1(w)$ with genus at most 9 whose constant field is $\mathbb{F}_q$.*

*Proof.* By the substitution $\psi = w + (u+v)/2$, we have $E_2 = E_1(\psi)$. By straightforward computation,

$$\psi^2 = -\frac{1}{4}\left(3u^2 + 2uv + 3v^2\right) = -\frac{3}{4}\left(u - \alpha_1 v\right)\left(u - \alpha_2 v\right),$$

where $\alpha_1, \alpha_2$ are the two distinct solutions of $3T^2 + 2T + 3 = 0$. From the assumptions on $a$, $b$, and the characteristic $p$, it is easily seen that the polynomial $\ell_1(\alpha_1 V, V)$ is not a square in $\mathbb{K}[V]$. Then $\psi^2$ has at least one zero in $\mathbb{K}(u,v)$ with odd multiplicity, and hence $\psi^2$ is not a square in $\mathbb{K}(u,v)$. Therefore $\mathbb{K}(u,v,w)|\mathbb{K}(u,v)$ is a Kummer extension of degree 2. By Lemma 1.1.36, $\mathbb{F}_q$ is the field of constants of $E_2 = \mathbb{F}_q(u,v,w)$. Since $\psi^2$ has at most 8 zeros in $\mathbb{K}(u,v)$ with odd multiplicity, the genus of $E_2$ is at most $1 + 2(3-1) + 8/2 = 9$. □

Let $E_3 = \mathbb{F}_q(u,v,w,t)$ with $u+v+w+t = 0$. Since $E_3 = E_2$, we have shown that $E_3$ is a function field with genus at most 9 and field of constants $\mathbb{F}_q$.

**Theorem 4.2.5.** *Assume that $q \geq 431$. Then there exists a complete $(q+2,4)$-arc $\mathcal{A}$ in $\mathrm{PG}(2,q)$ containing $\mathcal{C}$.*

*Proof.* Let $a, b \in \mathbb{F}_q$ with $b \neq a^4$. We count the number of poles and zeros of $u-v$, $u-w$, $u-t$, $v-w$, $v-t$, and $w-t$ in $\mathbb{K}(u,v,w,t) = \mathbb{K}(u,v,w)$. The poles lie over the four unramified places of $\mathbb{K}(u,v)$ centered at the ideal points of $\mathcal{E}_1$. Since $[\mathbb{K}(u,v,w,t) : \mathbb{K}(u,v)] = 2$, the number of poles of $u-v$, $u-w$, $u-t$, $v-w$, $v-t$, and $w-t$ in $\mathbb{K}(u,v,w,t)$ is 8. By [107, Th. 1.4.11], the number of zeros of $u-v$ in $\mathbb{K}(u,v,w,t)$ is at most 8; the same holds for $u-w$, $u-t$, $v-w$, $v-t$, and $w-t$.

Therefore, if the number $N_q$ of $\mathbb{F}_q$-rational places of $E_2$ is greater than $8+6\cdot 8 = 56$, then there exists an $\mathbb{F}_q$-rational place $Q$ of $E_3$ such that $P = (a,b) \in \mathrm{AG}(2,q)\backslash\mathcal{C}$ is collinear with four distinct points $(u(Q), u(Q)^4)$, $(v(Q), v(Q)^4)$, $(w(Q), w(Q)^4)$, $(t(Q), t(Q)^4)$ of $\mathcal{C}$. By Hasse-Weil bound,

$$N_q \geq q + 1 - 2g(E_3)\sqrt{q} \geq q + 1 - 18\sqrt{q};$$

thus, $N_q > 56$ by the hypothesis $q \geq 431$. We have shown that $\mathcal{C}$ is a $(q,4)$-arc which covers all the points of $\mathrm{PG}(2,q)$, except possibly the ideal line. Consider an ideal point $P_\infty = (1 : a : 0)$, with $a \neq 0$. The point $P_\infty$ is collinear with four distinct points of $\mathcal{C}$ if and only if there exist $u, v, w, t \in \mathbb{F}_q$ pairwise distinct such that

$$\begin{cases} u+v+w+t=0 \\ w^2+(u+v)w+u^2+uv+v^2=0 \\ u^3+u^2v+uv^2+v^3=a \end{cases} . \tag{4.18}$$

Arguing as above and using the Hasse-Weil bound, it can be proved that conditions (4.18) are satisfied for some distinct $u, v, w, t \in \mathbb{F}_q$, for each $a \in \mathbb{F}_q^*$. On the other side, the ideal points $(0 : 1 : 0)$ and $(1 : 0 : 0)$ are not collinear with four distinct points of $\mathcal{C}$. Therefore the claim is proved. □

### 4.2.2 $(k,4)$-arcs from quintic curves

Throughout the rest of Section 4.2, $p$ is an odd prime with $p > 5$ and $p \equiv 3 \pmod 4$, $\sigma = p^{h'}$ with $h'$ odd, and $q = p^h$ with $h > h'$ and $h' \mid h$. Moreover,

$$\mathcal{Q} = \{(x, x^5) \mid x \in \mathbb{F}_q\}$$

is the set of the $\mathbb{F}_q$-rational affine points of the plane curve with equation $Y = X^5$.

**Proposition 4.2.6.** *Let $A = (u,u^5)$, $B = (v,v^5)$, $C = (w,w^5)$, $D = (t,t^5)$ be four distinct points of $\mathcal{Q}$. They are collinear if and only if*

$$\begin{cases} w^3+w^2(u+v)+w(u^2+uv+v^2)+(u+v)(u^2+v^2)=0 \\ t^2+t(u+v+w)+u^2+v^2+w^2+uv+uw+vw=0 \end{cases} .$$

*Proof.* $A, B, C, D$ are collinear if and only if

$$\det\begin{pmatrix} u & u^5 & 1 \\ v-u & v^5-u^5 & 0 \\ w-u & w^5-u^5 & 0 \end{pmatrix} = \det\begin{pmatrix} u & u^5 & 1 \\ v-u & v^5-u^5 & 0 \\ t-u & t^5-u^5 & 0 \end{pmatrix} = 0,$$

that is

$$\begin{cases} (v-u)(w-u)(w-v)[w^3+w^2(u+v)+w(u^2+uv+v^2)+(u+v)(u^2+v^2)]=0 \\ (v-u)(t-u)(t-v)[t^3+t^2(u+v)+t(u^2+uv+v^2)+(u+v)(u^2+v^2)]=0 \end{cases} .$$

As $A, B, C, D$ are distinct, the assertion follows. □

**Proposition 4.2.7.** *Let $A = (u, u^5)$, $B = (v, v^5)$, $C = (w, w^5)$, $D = (t, t^5)$, $E = (r, r^5)$ be five distinct points of $\mathcal{Q}$. They are collinear if and only if*

$$\begin{cases} w^3 + w^2(u+v) + w(u^2+uv+v^2) + (u+v)(u^2+v^2) = 0 \\ t^2 + t(u+v+w) + u^2+v^2+w^2+uv+uw+vw = 0 \\ u+v+w+t+r = 0 \end{cases}.$$

*Proof.* By Proposition 4.2.6, the points $A, B, C, D, E$ are collinear if and only if

$$\begin{cases} w^3 + w^2(u+v) + w(u^2+uv+v^2) + (u+v)(u^2+v^2) = 0 \\ t^2 + t(u+v+w) + u^2+v^2+w^2+uv+uw+vw = 0 \\ r^2 + r(u+v+w) + u^2+v^2+w^2+uv+uw+vw = 0 \end{cases}.$$

Since $r \neq t$, the assertion follows. □

Now we construct a $(k, 4)$-arc contained in $\mathcal{Q}$ from a coset of an additive subgroup of $\mathbb{F}_q$. Let

$$M := \{(a^\sigma - a) \mid a \in \mathbb{F}_q\}, \tag{4.19}$$

and

$$\mathcal{K}_e := \{(v, v^5) \mid v \in M + e\}, \tag{4.20}$$

with $e \notin M$.

**Proposition 4.2.8.** *No five points of $\mathcal{K}_e$ are collinear.*

*Proof.* By Proposition 4.2.7, if five distinct points $(a_i + e, (a_i + e)^4)$, $a_i \in M$, $i = 1, \dots, 5$, are collinear then $a_1 + e + a_2 + e + a_3 + e + a_4 + e + a_5 + e = 0$, and hence $-5e = a_1 + a_2 + a_3 + a_4 + a_5 \in M$. Since $p \neq 5$ and $M$ is closed under addition by elements of $\mathbb{F}_\sigma$, we have $e \in M$, a contradiction. □

### 4.2.3 Points off $\mathcal{Q}$ are covered by $\mathcal{K}_e$

Consider a point $P = (a, b) \in \mathrm{AG}(2, q) \setminus \mathcal{Q}$. Arguing as in Proposition 4.2.7 we can prove the following.

**Proposition 4.2.9.** *Four distinct points $A = (u, u^4)$, $B = (v, v^4)$, $C = (w, w^4)$, $C = (t, t^4)$ of $\mathcal{Q}$ and $P = (a, b) \in \mathrm{AG}(2, q) \setminus \mathcal{Q}$ are collinear if and only if*

$$\begin{cases} w^3 + w^2(u+v) + w(u^2+uv+v^2) + (u+v)(u^2+v^2) = 0 \\ t^2 + t(u+v+w) + u^2+v^2+w^2+uv+uw+vw = 0 \\ b + uv(u^2+v^2)(u+v) - a(u^4+u^3v+u^2v^2+uv^3+v^4) = 0 \end{cases}.$$

*Proof.* The first two equations are the collinearity conditions for $A, B, C, D$, whereas the third is the collinearity condition for $A, B, P$, since

$$\det\begin{pmatrix} u & u^5 & 1 \\ v & v^5 & 1 \\ a & b & 1 \end{pmatrix} = (v-u)\left[b + uv(u^2+v^2)(u+v) - a(u^4+u^3v+u^2v^2+uv^3+v^4)\right].$$

□

In particular, if the points of $\mathcal{Q}$ have the form $A = (u+e, (u+e)^4)$, $B = (v+e, (v+e)^4)$, $C = (w+e, (w+e)^4)$, $D = (t+e, (t+e)^4)$, then the conditions in Proposition 4.2.9 read

$$\left\{\begin{array}{l} w^3 + w^2(u+v+5e) + w\left[u^2+uv+v^2+5e(u+v)+10e^2\right] \\ +(u+v)(u^2+v^2) + 5e(u^2+uv+v^2) + 9e^2(u+v) + 7e^3 = 0 \\[2ex] t^2 + t(u+v+w+5e) + u^2+v^2+w^2+uv+uw+vw \\ +e\left[3(u+v+w)+2(uv+uw+vw)\right] + 10e^2 = 0 \\[2ex] b + (u+e)(v+e)(u+v+2e)\left[u^2+v^2+2e(u+v)+e^2\right] - a\big[u^4+u^3v+u^2v^2 \\ +uv^3+v^4+5e(u+v)(u^2+v^2)+10e^2(u^2+uv+v^2)+9e^3(u+v)+4e^4\big] = 0 \end{array}\right. .$$

Therefore, the following result holds.

**Corollary 4.2.10.** *A point $P = (a,b) \in \mathrm{AG}(2,q) \setminus \mathcal{Q}$ is collinear with four distinct points of $\mathcal{K}_e$ if and only if there exists an $\mathbb{F}_q$-rational affine point $(x,y,z,r)$, with $x^\sigma - x$, $y^\sigma - y$, $z^\sigma - z$, $r^\sigma - r$ pairwise distinct, lying on the curve $\mathcal{H}_P$ with equations*

$$\mathcal{H}_P : \left\{\begin{array}{l} (Z^\sigma - Z)^3 + (Z^\sigma - Z)^2(X^\sigma - X + Y^\sigma - Y + 5e) + (Z^\sigma - Z)\big[(X^\sigma - X)^2 \\ +(X^\sigma - X)(Y^\sigma - Y) + (Y^\sigma - Y)^2 + 5e(X^\sigma - X + Y^\sigma - Y) + 10e^2\big] \\ +(X^\sigma - X + Y^\sigma - Y)\left[(X^\sigma - X)^2 + (Y^\sigma - Y)^2\right] + 5e\big[(X^\sigma - X)^2 \\ +(X^\sigma - X)(Y^\sigma - Y) + (Y^\sigma - Y)^2\big] + 9e^2(X^\sigma - X + Y^\sigma - Y) + 7e^3 = 0 \\[2ex] (R^\sigma - R)^2 + (R^\sigma - R)(X^\sigma - X + Y^\sigma - Y + Z^\sigma - Z + 5e) + (X^\sigma - X)^2 \\ +(Y^\sigma - Y)^2 + (Z^\sigma - Z)^2 + (X^\sigma - X)(Y^\sigma - Y) + (X^\sigma - X)(Z^\sigma - Z) \\ +(Y^\sigma - Y)(Z^\sigma - Z) + e\big[3(X^\sigma - X + Y^\sigma - Y + Z^\sigma - Z) \\ +2((X^\sigma - X)(Y^\sigma - Y) + (X^\sigma - X)(Z^\sigma - Z) + (Y^\sigma - Y)(Z^\sigma - Z))\big] + 10e^2 = 0 \\[2ex] b + (X^\sigma - X + e)(Y^\sigma - Y + e)(X^\sigma - X + Y^\sigma - Y + 2e)\big[(X^\sigma - X)^2 \\ +(Y^\sigma - Y)^2 + 2e(X^\sigma - X + Y^\sigma - Y) + e^2\big] - a\Big[(X^\sigma - X)^4 + (X^\sigma - X)^3 \cdot \\ \cdot (Y^\sigma - Y) + (X^\sigma - X)^2(Y^\sigma - Y)^2 + (X^\sigma - X)(Y^\sigma - Y)^3 + (Y^\sigma - Y)^4 \\ +5e(X^\sigma - X + Y^\sigma - Y)\left[(X^\sigma - X)^2 + (Y^\sigma - Y)^2\right] + 10e^2\big((X^\sigma - X)^2 \\ +(X^\sigma - X)(Y^\sigma - Y) + (Y^\sigma - Y)^2\big) + 9e^3(X^\sigma - X + Y^\sigma - Y) + 4e^4\Big] = 0 \end{array}\right. \tag{4.21}$$

Consider the following sequence of function fields:

$$\begin{tikzcd}[column sep=small]
F_7 = F_6(r) : \arrow[d, dash, "\sigma"] & r^\sigma - r = t \\
F_6 = F_5(t) : \arrow[d, dash, "2"] & \begin{array}{l} t^2 + t(x^\sigma - x + y^\sigma - y + z^\sigma - z + 5e) + (x^\sigma - x)^2 + (y^\sigma - y)^2 \\ +(z^\sigma - z)^2 + (x^\sigma - x)(y^\sigma - y) + (x^\sigma - x)(z^\sigma - z) + (y^\sigma - y)(z^\sigma - z) \\ +e\big[3(x^\sigma - x + y^\sigma - y + z^\sigma - z) + 2\big((x^\sigma - x)(y^\sigma - y) \\ +(x^\sigma - x)(z^\sigma - z) + (y^\sigma - y)(z^\sigma - z)\big)\big] + 10e^2 = 0 \end{array} \\
F_5 = F_4(z) : \arrow[d, dash, "\sigma"] & z^\sigma - z = w \\
F_4 = F_3(w) : \arrow[d, dash, "3"] & \begin{array}{l} w^3 + w^2(x^\sigma - x + y^\sigma - y + 5e) + w\big[(x^\sigma - x)^2 \\ +(x^\sigma - x)(y^\sigma - y) + (y^\sigma - y)^2 + 5e(x^\sigma - x + y^\sigma - y) + 10e^2\big] \\ +(x^\sigma - x + y^\sigma - y)((x^\sigma - x)^2 + (y^\sigma - y)^2) + 5e\big((x^\sigma - x)^2 \\ +(x^\sigma - x)(y^\sigma - y) + (y^\sigma - y)^2\big) + 9e^2(x^\sigma - x + y^\sigma - y) + 7e^3 = 0 \end{array} \\
F_3 = F_2(y) : \arrow[d, dash, "\sigma"] & y^\sigma - y = v \\
F_2 = F_1(x) : \arrow[d, dash, "\sigma"] & x^\sigma - x = u \\
F_1 = \mathbb{F}_q(u, v) : & \begin{array}{l} b + (u + e)(v + e)(u + v + 2e)\left[u^2 + v^2 + 2e(u + v) + e^2\right] \\ -a\big[u^4 + u^3v + u^2v^2 + uv^3 + v^4 + 5e(u + v)(u^2 + v^2) \\ \quad +10e^2(u^2 + uv + v^2) + 9e^3(u + v) + 4e^4\big] = 0 \end{array}
\end{tikzcd}$$

We are going to show that each extension $F_i : F_{i-1}$ is well-defined and that the field of constants of each function field $F_i$ is $\mathbb{F}_q$. We will also estimate the genus $g_i$ of $F_i$. Finally, by using the Hasse-Weil bound, we will show that if $q$ is large enough with respect to $\sigma$, then $F_7$ has a large number of $\mathbb{F}_q$-rational places. This implies that the curve $\mathcal{H}_P$ possesses a large number of $\mathbb{F}_q$-rational points.

First we show that $F_1$ is a function field with genus 6 whose constant field is $\mathbb{F}_q$. Equivalently, the quintic curve $\mathcal{H}_1$ with affine equation $G_1(U, V) = 0$, where

$$G_1(U, V) = b+(U+e)(V+e)(U+V+2e)\left[U^2 + V^2 + 2e(U + V) + e^2\right]-a\big[U^4+U^3V$$

$$+U^2V^2+UV^3+V^4+5e(U+V)(U^2+V^2)+10e^2(U^2+UV+V^2)+9e^3(U+V)+4e^4\big],$$

is absolutely irreducible and has genus 6.

**Proposition 4.2.11.** *Let $a, b \in \mathbb{F}_q$ with $b \neq 0$ and $b \neq a^5$. Then $\mathcal{H}_1$ is absolutely irreducible and has genus 6.*

*Proof.* The ideal points of $\mathcal{H}_1$ are $P_1 = (1 : 0 : 0)$, $Q_1 = (0 : 1 : 0)$, and $R_1^i = (1 : \xi^i : 0)$, $i \in \{1, 2, 3\}$, where $\xi$ is a primitive 4-th root of unity; being distinct, they are simple points. We have

$$\partial_U G_1(U, V) = (V - (a - e))\big(4(U + e)^3 + 3(U + e)^2(V + e) + 2(U + e)(V + e)^2 + (V + e)^3\big),$$

$$\partial_V G_1(U,V) = (U-(a-e))\big((U+e)^3+2(U+e)^2(V+e)+3(U+e)(V+e)^2+4(V+e)^3\big)\,.$$

Since $b \neq a^5$, no point $(U,V) \in \mathcal{H}_1$ has either $U = a-e$ or $V = a-e$. Also, the resultant of $\partial_U G_1(U,V)/\,(V-(a-e))$ and $\partial_V G_1(U,V)/\,(U-(a-e))$ with respect to $U$ is $2000(V+e)^9$ and $2000(U+e)^9$, respectively. Since $p > 5$, $\partial_U G_1(U,V) = \partial_V G_1(U,V) = 0$ if and only if $(U,V) = (-e,-e) \notin \mathcal{H}_1$. Therefore, $\mathcal{H}_1$ is non-singular, and hence absolutely irreducible with genus 6. □

**Proposition 4.2.12.** *Let $a, b \in \mathbb{F}_q$ with $b \neq 0$, $b \neq a^5$, and $a \neq e$. The equation $x^\sigma - x = u$ defines an extension $F_2 = F_1(x)$ with genus $g_2 = 9\sigma - 3$ whose field of constants is $\mathbb{F}_q$.*

*Proof.* By Proposition 4.2.11 $\mathcal{H}_1$ is non-singular with function field $F_1 = \mathbb{F}_q(\mathcal{H}_1)$. Thus, places of $\mathbb{K}(u,v)$ can be identified with points of $\mathcal{H}_1$. The tangent lines at the ideal points of $\mathcal{H}_1$ are

$$\ell_{P_1} : V = a-e, \qquad \ell_{Q_2} : U = a-e, \qquad \ell_{R_1^i} : V - \xi^i U = (\xi^i - 1)(a+4e)/4.$$

Here, the assumption $a \neq e$ assures that $U = 0$ and $V = 0$ are not tangent lines at the ideal points of $\mathcal{H}_1$; hence,

$$\begin{aligned} v_{P_1}(u) = v_{R_1^i}(u) = -1, &\quad v_{Q_1}(u) = 0, \\ v_{Q_1}(v) = v_{R_1^i}(v) = -1, &\quad v_{P_1}(v) = 0. \end{aligned} \tag{4.22}$$

For each place centered at an affine point and for $Q_1$ there exists $\rho \in \mathbb{K}(u,v)$ such that the valuation of $u - (\rho^\sigma - \rho)$ at that place is non-negative; in fact, it is sufficient to consider $\rho = 0$. Hence, $u = x^\sigma - x$ defines a Kummer extension $\mathbb{K}(u,v)(x) = \mathbb{K}(v,x)$ of $\mathbb{K}(u,v)$ of degree $\sigma$. Moreover, $P_1$ and $R_1^i$ $(i = 1,2,3)$ are the only totally ramified places; all other places are unramified. By Lemma 1.1.36, $\mathbb{F}_q$ is the constant field of $F_2 = \mathbb{F}_q(x,v)$. The genus is given by

$$g_2 = \sigma g_1 + \frac{\sigma-1}{2}\Big(-2 + \sum_{P \in \mathbb{P}(\mathbb{K}(u,v))} (m_P + 1)\deg P\Big) = 6\sigma + \frac{\sigma-1}{2}\,(-2+4(1+1)) = 9\sigma - 3.$$

□

Denote by $P_2$, $R_2^i$ the places of $\mathbb{K}(x,v)$ lying over $P_1$, $R_1^i$, respectively, and by $Q_2^1, \ldots, Q_2^\sigma$ the places lying over $Q_1$.

**Proposition 4.2.13.** *Let $a, b \in \mathbb{F}_q$ with $b \neq 0$, $b \neq a^5$, $a \neq e$, and $a \neq -4e$. The equation $y^\sigma - y = v$ defines an extension $F_3 = F_2(y)$ with genus $g_3 \leq 10\sigma^2 - 3\sigma - 1$ whose field of constants is $\mathbb{F}_q$.*

*Proof.* In $\mathbb{K}(x,v)$ we have $v_{P_2}(v)=0$, $v_{Q_2^i}(v)=-1$, and $v_{R_2^i}(v)=-\sigma$. The element $v-\xi^i u\in\mathbb{K}(u,v)$ satisfies $v_{R_2^i}(v-\xi^i u)=0$. Let $k_i\in\mathbb{K}$ be such that $k_i^\sigma=\xi^i$, and consider $\rho_i=k_i x$; then,

$$v-(\rho_i^\sigma-\rho_i)=v-\xi^i x^\sigma+k_i x=v-\xi^i x^\sigma+\xi^i x-\xi^i x+k_i x=v-\xi^i u+(k_i-\xi^i)x.$$

For $i=2$, $\xi^2=-1$ and $k_2=-1$; hence, $v_{R_2^2}(v-(\rho_2^\sigma-\rho_2))=0$. For $i\in\{1,3\}$, we have that $k_i\neq\xi^i$ by the assumption $4\nmid(\sigma-1)$; hence, $v_{R_2^i}((k_i-\xi^i)x)=-1$ and $v_{R_2^i}(v-(\rho_i^\sigma-\rho_i))=-1$. For the places centered at affine points, at $P_2$, and at $Q_2^i$, it is sufficient to choose $\rho=0$. Then $\mathbb{K}(x,y)|\mathbb{K}(x,v)$ is a generalized Artin-Schreier extension with $[\mathbb{K}(x,y):\mathbb{K}(x,v)]=\sigma$ and

$$g_3=\sigma g_2+\frac{\sigma-1}{2}\Big(-2+\sum_{P\in\mathbb{P}(\mathbb{K}(x,v))}(m_P+1)\deg P\Big)$$

$$\leq\sigma(9\sigma-3)+\frac{\sigma-1}{2}\left(-2+(\sigma+2)(1+1)\right)=10\sigma^2-3\sigma-1.$$

Finally, by Lemma 1.1.36, $\mathbb{F}_q$ is the constant field of $F_3=\mathbb{F}_q(x,y)$. □

In the extension $\mathbb{K}(x,y):\mathbb{K}(x,v)$ the only totally ramified places are $Q_2^1,\ldots,Q_2^\sigma$, $R_2^1$, and $R_2^3$; let $Q_3^1,\ldots,Q_3^\sigma$, $R_3^1$, and $R_3^3$ be the places lying over them. All other places are unramified; denote by $P_3^i$ and $R_3^{2,i}$ $(i=1,\ldots,\sigma)$ the places lying over $P_2$ and $R_2^2$, respectively. Now we investigate an auxiliary function field.

**Lemma 4.2.14.** *Let $a,b\in\mathbb{F}_q$, with $b\neq0$ and $b\neq a^5$. The equations*

$$\begin{cases}\eta^2=-\frac{4\mu^3+5\mu+5}{4\mu}\\ 64\mu^6\lambda^5-64a\mu^6\lambda^4+80\mu^4\lambda^5-80a\mu^4\lambda^4+76\mu^2\lambda^5\\ \qquad\qquad+180a\mu^2\lambda^4-256b\mu^2-25\lambda^5+25a\lambda^4=0\end{cases}$$

*define a function field $\mathbb{F}_q(\mu,\lambda,\eta)$ with genus at most 53 and constant field $\mathbb{F}_q$.*

*Proof.* We divide the proof in three steps.

1. We show that the equation $C(\rho,\lambda)=0$, with

   $$\begin{aligned}C(\rho,\lambda)=\;&64\rho^3\lambda^5-64a\rho^3\lambda^4+80\rho^2\lambda^5-80a\rho^2\lambda^4+76\rho\lambda^5\\&+180a\rho\lambda^4-256b\rho-25\lambda^5+25a\lambda^4,\end{aligned}$$

   defines a function field $\mathbb{F}_q(\rho,\lambda)$ with genus at most 8 and constant field $\mathbb{F}_q$.

   Let $P_\infty=(1:0:0)$ and $Q_\infty=(0:1:0)$ be the ideal points of the curve $\mathcal{C}:C(R,L)=0$. The point $P_\infty$ is singular with multiplicity 5; the tangent lines at $P_\infty$ are $L = 0$ with multiplicity 4 and $L = a$. The point $Q_\infty$ is singular with multiplicity 3; the tangent lines at $Q_\infty$ have equation $R = 1/4$, $R = -3/4 + \sqrt{-1}$, and $R = -3/4 - \sqrt{-1}$. The affine points of $\mathcal{C}$ are non-singular.

The curve $\mathcal{C}$ has no linear components. In fact, assume by contradiction that a line $\ell$ is a component of $\mathcal{C}$. If $P_\infty \in \ell$, then $\ell$ has equation $L = k$; hence, either $k = 0$ or $k = a$, which implies either $256b = 0$ or $256(a^5 - b) = 0$, a contradiction to the hypothesis. If $Q_\infty \in \ell$, then $\ell$ has equation $R = k$; hence, either $256b = 0$, or $k = 0$ and $25 = 0$, impossible.

The curve $\mathcal{C}$ has no proper components of degree higher than one. In fact, assume by contradiction that $\mathcal{C}$ splits into two proper components $\mathcal{C}_i$ and $\mathcal{C}_{8-i}$, where $\mathcal{C}_i$, $\mathcal{C}_{8.i}$ have degree $i$, $8-i$; the product of the leading terms of $\mathcal{C}_i$ and $\mathcal{C}_{8-i}$ equals $64\rho^3\lambda^5$. By comparing the coefficients of $\mathcal{C}_i \cdot \mathcal{C}_{8-i}$ and $\mathcal{C}$ for each $i \in \{2,3,4\}$ we obtain $b = 0$, a contradiction.

Therefore, $\mathcal{C}$ is absolutely irreducible. As $\mathcal{C}$ has two singular points of multiplicity 5 and 3, $\mathcal{C}$ has genus at most 8. Since $\mathbb{F}_q(\rho,\lambda)$ is the function field of $\mathcal{C}$ and $\mathbb{F}_q$ is the constant field of $\mathbb{F}_q(\rho,\lambda)$ by Lemma 1.1.36, the claim follows.

2. We show that the equation $\mu^2 = \rho$ defines a Kummer extension $\mathbb{F}_q(\mu,\lambda) = \mathbb{F}_q(\rho,\lambda)(\mu)$ with genus at most 18, whose constant field is $\mathbb{F}_q$.

   The function $\rho$ has two zeros in $\mathbb{K}(\rho,\lambda)$, namely the simple zero $A_a$ centered at $(0,a)$ and the zero $A_0$ with multiplicity 4 centered at $(0,0)$. Hence, $\rho$ is a non-square in $\mathbb{K}(\rho,\lambda)$. Also, there are at least two places and at most six places of $\mathbb{K}(\rho,\lambda)$ at which $\rho$ has odd multiplicity; namely, the place $A_a$ and between one and five places lying over the pole $P_\infty$ of $\rho$ in $\mathbb{K}(\rho)$. Then $\mathbb{F}_q(\mu\lambda)|\mathbb{F}_q(\rho,\lambda)$ is a Kummer extension with genus at most $1+2(8-1)+6/2 = 18$. By Lemma 1.1.36, $\mathbb{F}_q$ is the field of constants of $\mathbb{F}_q(\mu,\lambda)$.

3. We show that the equation $\eta^2 = -\frac{4\mu^3+5\mu+5}{4\mu}$ defines a Kummer extension $\mathbb{F}_q(\mu,\lambda,\eta) = \mathbb{F}_q(\mu,\lambda)(\eta)$ with genus at most 53 and constant field $\mathbb{F}_q$.

   Let $\overline{A}_a$ be the place of $\mathbb{K}(\mu.\lambda)$ lying over $A_a$; then $v_{\overline{A}_a}(\eta^2) = -1$. Therefore $\mathbb{K}(\mu,\lambda,\eta)|\mathbb{K}(\mu,\lambda)$ is a Kummer extension, and $\overline{A}_a$ is ramified. There are exactly five places of $\mathbb{K}(\mu,\lambda)$ lying over $P_\infty$; they ramify in $\mathbb{K}(\mu,\lambda,\eta)|\mathbb{K}(\mu,\lambda)$. Let $\mu_1,\mu_2,\mu_3$ be the distinct solutions in $\mu$ of the equation $4\mu^3+5\mu+5 = 0$. For $i = 1,2,3$, there are at most 10 places of $\mathbb{K}(\mu,\lambda,\eta)$ which are ramified in $\mathbb{K}(\mu,\lambda,\eta) : \mathbb{K}(\mu,\lambda)$ and lie over the zero of $\rho - \mu_i^2$ in $\mathbb{K}(\rho)$. All other places are unramified in $\mathbb{K}(\mu,\lambda,\eta)|\mathbb{K}(\mu,\lambda)$. Then the genus of $\mathbb{F}_q(\mu,\lambda,\eta)$ is at most $1+2(18-1)+36/2=53$. By Lemma 1.1.36, $\mathbb{F}_q$ is the field of constants of $\mathbb{F}_q(\mu,\lambda,\eta)$.

□

**Proposition 4.2.15.** *Let $a,b\in\mathbb{F}_q$, with $b\neq 0$ and $b\neq a^5$. The equations*

$$\begin{cases} b+(u+e)(v+e)(u+v+2e)\left[u^2+v^2+2e(u+v)+e^2\right]-a\big[u^4+u^3v+u^2v^2\\ +uv^3+v^4+5e(u+v)(u^2+v^2)+10e^2(u^2+uv+v^2)+9e^3(u+v)+4e^4\big]=0\\ w^3+w^2(u+v+5e)+w\left[u^2+uv+v^2+5e(u+v)+10e^2\right]\\ +(u+v)(u^2+v^2)+5e(u^2+uv+v^2)+9e^2(u+v)+7e^3=0 \end{cases} \tag{4.23}$$

*define a function field $\mathbb{F}_q(u,v,w)$ with genus at most 53 and constant field $\mathbb{F}_q$.*

*Proof.* Let $\mathcal{X}$ be the space curve with affine equations $C_1(U,V,W)=0$ and $C_2(U,V,W)=0$, where

$$C_1(U,V,W)=b+UV(U^3+U^2V+UV^2+V^3)-a(U^4+U^3V+U^2V^2+UV^3+V^4),$$
$$C_2(U,V,W)=W^3+W^2(U+V)+W(U^2+UV+V^2)+(U^3+U^2V+UV^2+V^3).$$

Denote by $\overline{u},\overline{v},\overline{w}$ the coordinate functions of $\mathcal{X}$. Consider the morphism

$$\varphi:(U,V,W,T)\mapsto(M,L,E,T)=(U/W+V/W+1/2,W,U/W-V/W,T).$$

Then $\mathcal{X}$ is $\mathbb{F}_q$-birationally equivalent to the curve $\mathcal{Y}=\varphi(\mathcal{X})$ with affine equations

$$\mathcal{Y}:\begin{cases} L^3\left(E^2+\frac{4M^3+5M+5}{4M}\right)=0\\ 64M^6L^5-64aM^6L^4+80M^4L^5-80aM^4L^4+76M^2L^5\\ +180aM^2L^4-256bM^2-25L^5+25aL^4=0 \end{cases}.$$

Since $\mathcal{Y}$ has no points $(M,L,E,T)$ with $L=0$, equivalent equations for $\mathcal{Y}$ are

$$\mathcal{Y}:\begin{cases} E^2=-\frac{4M^3+5M+5}{4M}\\ 64M^6L^5-64aM^6L^4+80M^4L^5-80aM^4L^4+76M^2L^5\\ +180aM^2L^4-256bM^2-25L^5+25aL^4=0 \end{cases}.$$

By Lemma 4.2.14, $\mathcal{X}$ is absolutely irreducible and has genus at most 53. Also, the function field $\mathbb{F}_q(\overline{u},\overline{v},\overline{w})$ of $\mathcal{X}$ has constant field $\mathbb{F}_q$. Let $\overline{u}=u+e$, $\overline{v}=v+e$, and $\overline{w}=w+e$. Then $\mathbb{F}_q(u,v,w)=\mathbb{F}_q(\overline{u},\overline{v},\overline{w})$ and $u,v,w$ satisfy the equations (4.23). This yields the thesis. □

The function field $F_4$ is the compositum of $\mathbb{F}_q(u,v,w)$ and $F_3$. The extension $F_4|F_1$ has degree $[\mathbb{F}_q(u,v,w) : F_1] \cdot [F_3 : F_1] = 3\sigma^2$, since 3 and $\sigma^2$ are coprime. Also, $\mathbb{F}_q$ is the field of constants of $F_4$.

For $i = 1, \dots, \sigma$, we have by Equations (4.23) that in the extension $F_4|F_3$ there are three distinct places $P_4^{i,j}$ $(j = 1, 2, 3)$ lying over $P_3^i$. Also, there are three distinct places $R_{4,2}^{i,j}$ and $R_4^{\ell,j}$ $(\ell, j = 1, 2, 3)$ lying over $R_3^{2,i}$ and $R_3^{\ell}$, respectively; let $R_{4,2}^{i,1}$ be the place centered at the point $(X : Y : 0 : 0)$ with $W = 0$.

**Proposition 4.2.16.** *Let $a, b \in \mathbb{F}_q$ with $b \neq 0$, $b \neq a^5$, $a \neq e$, and $a \neq -4e$. The equation $z^\sigma - z = w$ defines an extension $F_5 = F_4(z)$ with genus $g_5 \leq 100\sigma^3 - 24\sigma^2 - 6\sigma + 1$ whose field of constants is $\mathbb{F}_q$.*

*Proof.* Let $P_1$ be the place of $\mathbb{K}(u,v)$ centered at $(1 : 0 : 0)$. In the extension $\mathbb{K}(u,v,w)|\mathbb{K}(u,v)$ there are three distinct places lying over $P_1$, namely the places $\widetilde{P}_2^i$ centered at $(1, 0, \xi^i, 0)$, $i = 1, 2, 3$. Consider the place $\widetilde{P}_2^1$. Then $v_{\widetilde{P}_2^1}(u) = v_{\widetilde{P}_2^1}(w) = -1$, and $w = \xi u + \Phi$ for some $\Phi \in \mathbb{K}(u,v,w)$ with $v_{\widetilde{P}_2^1}(\Phi) \geq 0$. Since $\sigma \equiv 3 \pmod 4$, we have $\xi \notin \mathbb{F}_\sigma$; hence, there exists $k \in \mathbb{K}$ with $k^\sigma = \xi$ and $k \neq \xi$. Let $\rho = kx$; then

$$w - (\rho^\sigma - \rho) = \xi(x^\sigma - x) + \Phi - k^\sigma x^\sigma + kx = (\xi - k^\sigma)x^\sigma + (k - \xi)x + \Phi = (k - \xi)x + \Phi.$$

Choose $i$ and $j$ such that $P_4^{i,j}$ lies over $\widetilde{P}_2^1$. Then

$$v_{P_4^{i,j}}(\Phi) = e(P_4^{i,j} \mid \widetilde{P}_2^1) \cdot v_{\widetilde{P}_2^1}(\Phi) \geq 0\,, \qquad v_{P_4^{i,j}}(x) = e(P_4^{i,j} \mid P_3^i) \cdot v_{P_3^i}(x) = -1.$$

Therefore,

$$v_{P_4^{i,j}}(w - (\rho^\sigma - \rho)) = -1. \tag{4.24}$$

Now we prove that

$$\gamma\, w \neq \zeta^p - \zeta \quad \text{for all} \quad \zeta \in \mathbb{K}(x,y,w), \gamma \in \mathbb{F}_\sigma.$$

On the contrary, assume $\gamma\, w = \zeta^p - \zeta$ with $\zeta \in \mathbb{K}(x,y,w), \gamma \in \mathbb{F}_\sigma$. From (4.24),

$$-1 = v_{P_4^{i,j}}(\gamma w - (\gamma\rho^\sigma - \gamma\rho)) = v_{P_4^{i,j}}(\gamma w - (\alpha^\sigma - \alpha)),$$

with $\alpha = \gamma\rho \in \mathbb{K}(x,y,w)$. Since

$$\alpha^\sigma - \alpha = \left(\alpha^{\sigma/p} + \alpha^{\sigma/p^2} + \ldots + \alpha\right)^p - \left(\alpha^{\sigma/p} + \alpha^{\sigma/p^2} + \ldots + \alpha\right),$$

we have

$$v_{P_4^{i,j}}((\zeta - \beta)^p - (\zeta - \beta)) = v_{P_4^{i,j}}(\zeta^p - \zeta - (\beta^p - \beta)) = -1,$$

where $\beta = \alpha^{\sigma/p} + \alpha^{\sigma/p^2} + \ldots + \alpha \in \mathbb{K}(u,v,w)$. But this is clearly impossible, since the valuation of $((\zeta-\beta)^p - (\zeta-\beta))$ must be either non-negative or a multiple of $p$. Then we can apply Lemma 1.3 in [46] to conclude that $T^\sigma - T - w$ is irreducible over $\mathbb{K}(x,y,w)$, and $\mathbb{K}(x,y,z)|\mathbb{K}(x,y,w)$ is an Artin-Schreier extension of degree $\sigma$. Also, by Lemma 1.1.36, $\mathbb{F}_q$ is the constant field of $\mathbb{F}_q(x,y,z)$. Finally, we give a bound on $g_5$. By Castelnuovo's Inequality ([107, Theorem 3.11.3]),

$$g_5 \leq [F_5:F_3]\cdot g_3 + [F_5:\mathbb{F}_q(u,v,z)]\cdot g(\mathbb{F}_q(u,v,z)) + ([F_5:F_3]-1)\cdot([F_5:\mathbb{F}_q(u,v,z)]-1)\,.$$

We have $[F_5:F_3] = [F_5:F_4]\cdot[F_4:F_3] = 3\sigma$, and $g_3 \leq 10\sigma^2 - 3\sigma - 1$. Since $\{x, x^2, \ldots, x^\sigma\}$ is a basis of $\mathbb{F}_q(x,v,z)$ over $\mathbb{F}_q(u,v,z)$ and $\{y, y^2, \ldots, y^\sigma\}$ is a basis of $F_5$ over $\mathbb{F}_q(x,v,z)$, we have that $\{x^i y^j \mid i,j = 1,\ldots,\sigma\}$ is a basis of $F_5$ over $\mathbb{F}_q(u,v,z)$ and $[F_5:\mathbb{F}_q(u,v,z)] = \sigma^2$. By direct computations with Equations (4.23), the places $P_1$, $Q_1$, $R_1^i$ $(i = 1,2,3)$ of $\mathbb{K}(u,v)$ are not ramified in $\mathbb{K}(u,v,w)|\mathbb{K}(u,v)$. Hence, $v_{\widetilde{P}_2^j}(w) = v_{\widetilde{Q}_2^j}(w) = v_{\widetilde{R}_2^{i,j}}(w) = -1$ for $j = 1,2,3$, where $\widetilde{P}_2^j$, $\widetilde{Q}_2^j$, $\widetilde{R}_2^{i,j}$ are the places of $\mathbb{K}(u,v,w)$ lying over $P_1$, $Q_1$, $R_1^i$, respectively. The valuation of $w$ at any other place of $\mathbb{K}(u,v,w)$ is non-negative. Then $\mathbb{K}(u,v,z)|\mathbb{K}(u,v,w)$ is a generalized Artin-Schreier extension of degree $\sigma$, and

$$g(\mathbb{K}(u,v,z)) \leq 53\sigma + \frac{\sigma-1}{2}(-2 + 15(1+1)) = 67\sigma - 14\,.$$

Therefore $g(\mathbb{F}_q(u,v,z)) \leq 67\sigma - 14$, and

$$g_5 \leq 3\sigma(10\sigma^2 - 3\sigma - 1) + \sigma^2(67\sigma - 14) + (3\sigma-1)(\sigma^2-1) = 100\sigma^3 - 24\sigma^2 - 6\sigma + 1.$$

□

The places $R_4^{\ell,j}$ and $R_{4,2}^{i,1}$ are zeros of $w$, hence they are not ramified in the Artin-Schreier extension $F_5|F_4$, whereas $P_4^{i,j}$ is totally ramified. Denote by $P_5^{i,j}$, $R_{5,\ell}^{j,1}, \ldots, R_{5,\ell}^{j,\sigma}$, and $R_{5,2}^{i,1,1}, \ldots, R_{5,2}^{i,1,\sigma}$ the places of $F_5$ lying over $P_4^{i,j}$, $R_4^{\ell,j}$, and $R_{4,2}^{i,1}$, respectively.

**Proposition 4.2.17.** *Let $a, b \in \mathbb{F}_q$ with $b \neq 0$ and $b \neq a^5$. The equation*

$$\begin{aligned} &t^2 + t(u+v+w+5e) + u^2 + v^2 + w^2 + uv + uw + vw \\ &+e\,[3(u+v+w) + 2(uv+uw+vw)] + 10e^2 = 0 \end{aligned} \tag{4.25}$$

*defines an extension $\mathbb{F}_q(u,v,w,t) = \mathbb{F}_q(u,v,w)(t)$ with genus at most* 150 *whose field of constants is $\mathbb{F}_q$.*

*Proof.* Let $\mathbb{K}(\overline{u},\overline{v},\overline{w})$ be the function field defined by the equations $C_1(\overline{u},\overline{v},\overline{w})=0$ and $C_2(\overline{u},\overline{v},\overline{w})=0$, where

$$\begin{aligned} C_1(\overline{u},\overline{v},\overline{w}) &= b+\overline{uv}(\overline{u}^3+\overline{u}^2\overline{v}+\overline{uv}^2+\overline{v}^3)-a(\overline{u}^4+\overline{u}^3\overline{v}+\overline{u}^2\overline{v}^2+\overline{uv}^3+\overline{v}^4),\\ C_2(\overline{u},\overline{v},\overline{w}) &= \overline{w}^3+\overline{w}^2(\overline{u}+\overline{v})+\overline{w}(\overline{u}^2+\overline{uv}+\overline{v}^2)+(\overline{u}^3+\overline{u}^2\overline{v}+\overline{uv}^2+\overline{v}^3). \end{aligned}$$

As shown in the proof of Proposition 4.2.15, $\mathbb{K}(\overline{u},\overline{v},\overline{w})$ has genus at most 53 and constant field $\mathbb{F}_q$. Let

$$\overline{t}^2=-\frac{3\overline{u}^2+3\overline{v}^2+3\overline{w}^2+2\overline{uv}+2\overline{uw}+2\overline{vw}}{4}. \tag{4.26}$$

The zeros of $\overline{t}^2$ are centered at common roots of the polynomials $C_1(\overline{U},\overline{V},\overline{W})$, $C_2(\overline{U},\overline{V},\overline{W})$, and $C_3(\overline{U},\overline{V},\overline{W})=3\overline{U}^2+3\overline{V}^2+3\overline{W}^2+2\overline{UV}+2\overline{UW}+2\overline{VW}$. The resultant of $C_2$ and $C_3$ with respect to $\overline{W}$ is

$$C_4(\overline{U},\overline{V})=16\overline{U}^6+24\overline{U}^5\overline{V}+35\overline{U}^4\overline{V}^2+50\overline{U}^3\overline{V}^3+35\overline{U}^2\overline{V}^4+24\overline{UV}^5+16\overline{V}^6,$$

which is homogeneous in $\overline{U}$ and $\overline{V}$; hence, $C_5=C_4/\overline{V}^6$ is an univariate polynomial of degree 6 in the indeterminate $\widetilde{U}=\overline{U}/\overline{V}$. The discriminant of $C_5$ with respect to $\widetilde{U}$ is $-2^{19}5^{10}\neq 0$, then $C_4(\overline{U},\overline{V})$ splits into six distinct linear components $L_1,\ldots,L_6$ passing through $O=(0,0)$. For each $i=1,\ldots,6$, $C_1$ and $L_i$ have at least one common zero $Z_i$ with odd multiplicity, and $Z_i\neq O$. Let $D$ be the discriminant of $C_3$ with respect to $\overline{W}$. The resultant of $D$ and $C_4$ with respect to $\overline{V}$ is $2^{28}5^4\overline{U}^{12}$; hence, $Z_i$ is a simple zero of $C_3$. Therefore, Equation (4.26) defines a Kummer extension $\mathbb{K}(\overline{u},\overline{v},\overline{w},\overline{t})=\mathbb{K}(\overline{u},\overline{v},\overline{w})(\overline{t})$, and there are at most $6\cdot 5\cdot 3=90$ zeros of $\overline{t}^2$ with odd multiplicity. The genus of $\mathbb{K}(\overline{u},\overline{v},\overline{w},\overline{t})$ satisfies

$$g(\mathbb{K}(\overline{u},\overline{v},\overline{w},\overline{t}))\leq 1+2(53-1)+\frac{1}{2}\cdot 90=150.$$

By Lemma 1.1.36, $\mathbb{F}_q$ is the constant field of $\mathbb{F}_q(\overline{u},\overline{v},\overline{w},\overline{t})$. By the substitutions

$$\overline{u}=u+e,\quad \overline{v}=v+e,\quad \overline{w}=w+e,\quad \overline{t}=t+e+\frac{1}{2}\left((u+e)+(v+e)+(w+e)\right),$$

we have $\mathbb{F}_q(u,v,w,t)=\mathbb{F}_q(\overline{u},\overline{v},\overline{w},\overline{t})$; also, $u,v,w,t$ satisfy Equations (4.23) and (4.25). The thesis follows. □

The function field $F_6$ is the compositum of $\mathbb{F}_q(u,v,w,t)$ and $F_5$. Since 6 and $\sigma^3$ are coprime, we have $[F_6:F_1]=6\sigma^3$. Also, $\mathbb{F}_q$ is the constant field of $F_6$.

**Proposition 4.2.18.** *Suppose that $\sqrt{2e-1} \notin \mathbb{F}_\sigma$, and let $a, b \in \mathbb{F}_q$ with $b \neq 0$, $b \neq a^5$, $a \neq e$, and $a \neq -4e$. The equation $r^\sigma - r = t$ defines an extension $F_7 = F_6(r)$ with genus $g_7 \leq 381\sigma^4 - 78\sigma^3 - 12\sigma^2 + 1$ whose constant field is $\mathbb{F}_q$.*

*Proof.* Let $\widetilde{R}_2^{2,1}$ be the place of $\mathbb{K}(u,v,w)$ centered at $(1:-1:0:0)$. By Equation (4.25), $\widetilde{R}_2^{2,1}$ is not ramified in $\mathbb{K}(u,v,w,t)|\mathbb{K}(u,v,w)$; denote by $\widetilde{R}_{3,2}^{1,1}$ the place of $\mathbb{K}(u,v,w,t)$ lying over $\widetilde{R}_2^{2,1}$ and centered at $(1:-1:0:\eta:0)$, where $\eta^2 = 2e-1$. Similarly, $R_{5,2}^{i,1,j}$ is not ramified in $\mathbb{K}(x,y,z,t)|\mathbb{K}(x,y,z)$; denote by $R_{6,2,1}^{i,1,j}$ the place of $\mathbb{K}(x,y,z,t)$ lying over $R_{5,2}^{i,1,j}$ and centered at the ideal point $(X:Y:Z:\eta:0)$ with $T=\eta$. Note that the assumption $q \geq \sigma^2$ allows to choose $e$ such that $e \notin M$ and $\eta \notin \mathbb{F}_\sigma$, where $M$ is as in (4.19).

Consider the place $\widetilde{R}_{3,2}^{1,1}$. Then $v_{\widetilde{R}_{3,2}^{1,1}}(u) = v_{\widetilde{R}_{3,2}^{1,1}}(t) = -1$, and $t = \eta u + \Phi$ for some $\Phi \in \mathbb{K}(u,v,w,t)$ with $v_{\widetilde{R}_{3,2}^{1,1}}(\Phi) \geq 0$. Let $k \in \mathbb{K}$ with $k^\sigma = \eta$ and $k \neq \eta$, and choose $\rho = kx$; then

$$t-(\rho^\sigma-\rho) = \eta(x^\sigma - x) + \Phi - k^\sigma x^\sigma + kx = (\eta - k^\sigma)x^\sigma + (k-\eta)x + \Phi = (k-\eta)x + \Phi.$$

The place $R_{6,2,1}^{i,1,j}$ lies over $\widetilde{R}_{3,2}^{1,1}$ and $R_{5,2}^{i,1,j}$, and

$$v_{R_{6,2,1}^{i,1,j}}(\Phi) = e(R_{6,2,1}^{i,1,j} \mid \widetilde{R}_{3,2}^{1,1}) \cdot v_{\widetilde{R}_{3,2}^{1,1}}(\Phi) \geq 0,\ v_{R_{6,2,1}^{i,1,j}}(x) = e(R_{6,2,1}^{i,1,j} \mid R_{5,2}^{i,1,j}) \cdot v_{R_{5,2}^{i,1,j}}(x) = -1.$$

Therefore, $v_{R_{6,2,1}^{i,1,j}}(t-(\rho^\sigma - \rho)) = -1$. Arguing as in the proof of Proposition 4.2.16, it is easily proved that $\gamma t \neq \zeta^p - \zeta$ for all $\zeta \in \mathbb{K}(x,y,t)$ and $\gamma \in \mathbb{F}_\sigma$. Then we can apply Lemma 1.3 in [46] to conclude that $T^\sigma - T - t$ is irreducible over $\mathbb{K}(x,y,t)$, and $\mathbb{K}(x,y,z,r)|\mathbb{K}(x,y,z,t)$ is an Artin-Schreier extension of degree $\sigma$. Also, by Lemma 1.1.36, $\mathbb{F}_q$ is the constant field of $\mathbb{F}_q(x,y,z)$. Finally, we give a bound on $g_7$. By Castelnuovo's Inequality,

$$\begin{aligned} g_7 \leq\ & [F_7 : F_5] \cdot g_5 + [F_7 : \mathbb{F}_q(u,v,w,r)] \cdot g(\mathbb{F}_q(u,v,w,r)) \\ & + ([F_7 : F_5] - 1) \cdot ([F_7 : \mathbb{F}_q(u,v,w,r)] - 1)\ . \end{aligned}$$

We have $[F_7 : F_5] = [F_7 : F_6] \cdot [F_6 : F_5] = 2\sigma$ and $g_5 \leq 100\sigma^3 - 24\sigma^2 - 6\sigma + 1$. Since $\{x, x^2, \ldots, x^\sigma\}$ is a basis of $\mathbb{F}_q(x,v,w,r)$ over $\mathbb{F}_q(u,v,w,r)$, $\{y, y^2, \ldots, y^\sigma\}$ is a basis of $\mathbb{F}_q(x,y,w,r)$ over $\mathbb{F}_q(x,v,w,r)$, and $\{z, z^2, \ldots, z^\sigma\}$ is a basis of $F_7$ over $\mathbb{F}_q(x,y,w,r)$, we have that $\left\{x^i y^j z^\ell \mid i,j,\ell = 1, \ldots, \sigma\right\}$ a basis of $F_7$ over $\mathbb{F}_q(u,v,w,r)$; hence, $[F_7 : \mathbb{F}_q(u,v,w,r)] = \sigma^3$.

Consider a place $\widetilde{P} \in \{P_2^j, \widetilde{Q}_2^j, \widetilde{R}_2^{i,j} \mid i,j = 1,2,3\}$ of $\mathbb{K}(u,v,w)$, and a place $\overline{P}$ of $\mathbb{K}(u,v,w,t)$ lying over $\widetilde{P}$. Then $v_{\overline{P}}(t) \in \{-1,-2\}$; hence, $v_{\overline{P}}(t)$ is negative and coprime to $\sigma$. The valuation of $t$ at any other place of $\mathbb{K}(u,v,w,t)$ is non-negative.

Then $\mathbb{K}(u,v,w,r)|\mathbb{K}(u,v,w,t)$ is a generalized Artin-Schreier extension of degree $\sigma$ with at most $2\cdot 15$ ramified places, and

$$g(\mathbb{K}(u,v,w,r)) \le 150\sigma + \frac{\sigma-1}{2}(-2+30(1+1)) = 179\sigma - 29\,.$$

Therefore $g(\mathbb{F}_q(u,v,z)) \le 179\sigma - 29$, and

$$g_7 \le 2\sigma(100\sigma^3-24\sigma^2-6\sigma+1)+\sigma^3(179\sigma-29)+(2\sigma-1)(\sigma^3-1) = 381\sigma^4-78\sigma^3-12\sigma^2+1.$$

□

**Theorem 4.2.19.** *Let $\mathcal{K}_e$ be as in* (4.20), *with $e$ such that $\sqrt{2e-1} \notin \mathbb{F}_\sigma$. If $q \ge 580644\sigma^8$, then $\mathcal{K}_e$ is a 4-arc covering all points of* $\mathrm{AG}(2,q)\setminus\mathcal{Q}$ *except possibly those lying on the line $Y=0$ .*

*Proof.* Let $P=(a,b)\in \mathrm{AG}(2,q)\setminus\mathcal{Q}$ and assume that $a\neq t$, $a\neq -4e$, and $b\neq 0$. We start by counting the number $Z_1$ of poles of $x^\sigma - x$, $y^\sigma - y$, $z^\sigma - z$, and $r^\sigma - r$ in $\mathbb{K}(x,y,z,r)$. Clearly, $Z_1$ is the number of places lying over $P_1$, $Q_1$, $R_1^1$, $R_1^2$, or $R_1^3$ in $\mathbb{K}(x,y,z,r)|\mathbb{K}(u,v)$, hence over $P_5^{i,j}$, $Q_5^{i,j}$, $R_{5,\ell}^{j,i}$, or $R_{5,2}^{i,j,k}$ in $\mathbb{K}(x,y,z,r)|\mathbb{K}(x,y,z)$ $(i,k=1,\ldots,\sigma,\ \ell=1,3,\ j=1,2,3)$. Since $[\mathbb{K}(x,y,z,r):\mathbb{K}(x,y,z)]=2\sigma$, we have by the Fundamental Equality 1.1.1 that $Z_1 \le 2\sigma(3\sigma+3\sigma+6\sigma+3\sigma^2) = 6\sigma^3+24\sigma^2$.

Now we count the number $Z_2$ of zeros of $(x^\sigma-x)-(y^\sigma-y)$ in $\mathbb{K}(x,y,z,r)$. Clearly a place is a zero of $(x^\sigma-x)-(y^\sigma-y)=(x-y)^\sigma-(x-y)$ if and only if it is a zero of $x-y-\lambda$ for some $\lambda\in\mathbb{F}_\sigma$, then

$$Z_2 \le \sum_{\lambda\in\mathbb{F}_\sigma} \deg(x-y-\lambda)_0 = \sum_{\lambda\in\mathbb{F}_\sigma} \deg(x-y-\lambda)_\infty\,.$$

The poles of $x-y-\lambda$ are the places lying over $P_5^{i,j}$, $Q_5^{i,j}$, $R_{5,\ell}^{j,i}$, and $R_{5,2}^{i,j,k}$. Then

$$\deg(x-y-\lambda)_\infty = (12\sigma+3\sigma^2)\cdot[\mathbb{K}(x,y,z,r):\mathbb{K}(x,y,z)] = 6\sigma^3+24\sigma^2$$

for all $\lambda\in\mathbb{F}_\sigma$; hence, $Z_2 \le 6\sigma^4+24\sigma^3$. Also, $Z_2$ equals the number of zeros of $(x^\sigma-x)-(z^\sigma-z)$, $(x^\sigma-x)-(r^\sigma-r)$, $(y^\sigma-y)-(z^\sigma-z)$, $(y^\sigma-y)-(r^\sigma-r)$, and $(z^\sigma-z)-(r^\sigma-r)$ in $\mathbb{K}(x,y,z,r)$.

Therefore, if the number $N_q$ of $\mathbb{F}_q$-rational places of $F_7$ is greater than

$$6\sigma^3+24\sigma^2+6(6\sigma^4+24\sigma^3) = 36\sigma^4+150\sigma^3+24\sigma^2\,,$$

then there exists an $\mathbb{F}_q$-rational place $P$ of $F_7$ such that $(x(P),y(P),z(P),r(P))$ is a well-defined affine point of $\mathcal{H}$ with $x(P)^\sigma-x(P)$, $y(P)^\sigma-y(P)$, $z(P)^\sigma-z(P)$, $r(P)^\sigma-r(P)$ pairwise distinct. By Hasse-Weil bound we have

$$N_q \;\ge\; q+1-2g_7\sqrt{q} \;\ge\; q+1-2(381\sigma^4-78\sigma^3-12\sigma^2+1)\sqrt{q}\,.$$

From $q \geq 580644\sigma^8$ it follows that

$$q+1-2(381\sigma^4-78\sigma^3-12\sigma^2+1)\sqrt{q} \geq 36\sigma^4+150\sigma^3+24\sigma^2+1\,,$$

and hence, by Corollary 4.2.10, $P$ is collinear with four distinct points in $\mathcal{K}_e$.

Assume now that $P=(e,b)$ or $P=(-4e,b)$ with $b \neq 0$. Let $e' \in M+e$ with $e' \neq e$, and consider the curve $\mathcal{H}'_P$ obtained by replacing $e$ with $e'$ in Equation (4.21). Arguing as above $\mathcal{K}_{e'}$ covers the point $P$. Clearly $\mathcal{K}_{e'} = \mathcal{K}_e$, and the assertion follows. □

### 4.2.4 Constructions of 5-independent subsets

We want to construct complete $(k,4)$-arcs from union of cosets $\mathcal{K}_t$; to this end, we will use the notion of a 5-independent subset of an elementary abelian $p$-group, which is analogous to the notion of 4-independent subsets used in Section 4.1.

**Definition 4.2.20.** *Let $G$ be a finite abelian group and let $\mathcal{E}$ be a subset of $G$. If*

$$y_1+y_2+y_3+y_4+y_5 \neq 0 \quad \text{for all} \quad y_1,y_2,y_3,y_4,y_5 \in \mathcal{E},$$

*then $\mathcal{E}$ is said to be a* 5-independent subset *of $G$. An element $g \in G$ is* covered *by $\mathcal{E}$ if either $g \in \mathcal{E}$ or*

$$\text{there exist } \ y_1,y_2,y_3,y_4 \in \mathcal{E} \text{ such that } \ y_1+y_2+y_3+y_4+g=0.$$

In the remaining part of the section we construct 5-independent subsets of the abelian group $\mathbb{Z}_p^{h'}$, for $h'$ an odd integer and $p \geq 7$. We distinguish the cases $h'=1$ and $h' \geq 3$. For a subset $S$ of a group $G$, $s^\wedge S$ denotes the $s$-fold sumset $\{y_1+\ldots+y_s \mid y_1,\ldots,y_s \in S\}$ and $[a,b]$ denotes the set of elements in $\mathbb{Z}_p$ represented by integers $x$ with $a \leq x \leq b$.

**Proposition 4.2.21.** *Let $p \geq 25+i$ be an integer, with $p \equiv i \bmod 5$, $i=1,2,3,4$. Then*

$$\mathcal{E} = \{-1,1,3\} \cup \left[5, \frac{p-i}{5}\right]$$

*is a 5-independent subset of $\mathbb{Z}_p$ covering*

$$\mathbb{Z}_p \setminus \left\{ \frac{p-i}{5}+j \;\middle|\; 1 \leq j \leq i-1 \right\}.$$

*Proof.* The sum of five elements of $\mathcal{E}^* = \{1,3\} \cup \left[5, \frac{p-i}{5}\right]$ is contained in $\{5,7\} \cup [9, p-i]$ and therefore is different from 0. An easy check shows that if one or more of the five elements is $-1$, then it is not possible to obtain 0. Then

$$\begin{aligned} 4^\wedge\mathcal{E} &= \{-4\} \cup (-3+\mathcal{E}^*) \cup (-2+2^\wedge\mathcal{E}^*) \cup (-1+3^\wedge\mathcal{E}^*) \cup 4^\wedge\mathcal{E}^* \\ &= \{-4\} \cup \{-2,0\} \cup \left[2, \tfrac{p-i-15}{5}\right] \cup \{0,2\} \cup \left[4, \tfrac{2p-2i-10}{5}\right] \\ &\qquad \cup \{2,4\} \cup \left[6, \tfrac{3p-3i-5}{5}\right] \cup \{4,6\} \cup \left[8, \tfrac{4p-4i}{5}\right] \\ &= \{-4,-2,0\} \cup \left[2, \tfrac{4p-4i}{5}\right] \end{aligned}$$

for $p > 25+i$, and $4^\wedge\mathcal{T} = \{-4,-2,0,2\} \cup \left[4, \frac{4p-4i}{5}\right]$ for $p = 25+i$. Hence, the set of covered elements not in $\mathcal{E}$ is $-4^\wedge\mathcal{E} = \{0,2,4\} \cup \left[\frac{p+4i}{5}, p-2\right]$, and the non-covered elements are $\left\{\frac{p-i}{5} + j \;\middle|\; 1 \le j \le i-1\right\}$. □

We now consider the case $G = \mathbb{Z}_p^{h'}$ for $h' \ge 3$. We write $G$ as $G = A \times B \times C$, with $A = \mathbb{Z}_p$, $B = C = \mathbb{Z}_p^{\frac{h'-1}{2}}$. Let

$$\mathcal{E} = \mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3, \tag{4.27}$$

where $\mathcal{E}_1 = \{(a,1,1) \mid a \in A \setminus \{-4\}\}$, $\mathcal{E}_2 = \{(1,b,1) \mid b \in B \setminus \{-4\}\}$, and $\mathcal{E}_3 = \{(1,1,c) \mid c \in C \setminus \{-4\}\}$. Here, 1 and $-4$ are viewed as elements of the additive group of the finite field $\mathbb{F}_{p^{\frac{h'-1}{2}}}$, which is isomorphic to $A$, $B$, and $C$.

**Proposition 4.2.22.** *Let $h' \ge 3$, $p > 5$, and $\mathcal{E}$ be as in (4.27). Then $\mathcal{E}$ is a 5-independent subset of $\mathbb{Z}_p^{h'}$ of size $2p^{\frac{h'-1}{2}} + p - 5$ not covering 3 elements of $\mathbb{Z}_p^{h'}$.*

*Proof.* Consider five elements $e_1, e_2, e_3, e_4, e_5 \in \mathcal{E}$. If $e_1, e_2, e_3, e_4, e_5$ belong either to the same $\mathcal{E}_i$ or to exactly two distinct $\mathcal{E}_i$'s, then they all share 1 in one of the coordinates, and therefore $e_1 + e_2 + e_3 + e_4 + e_5 \neq (0,0,0)$ holds.

Assume then that $e_1, e_2, e_3, e_4, e_5$ belong to all the three $\mathcal{E}_i$'s. This means that there exists a $\mathcal{E}_i$ containing exactly one element $e_j$. Since $a, b, c$ are different from $-4$, their sum cannot be equal to $(0,0,0)$. This proves that $\mathcal{E}$ is a 5-independent subset of $\mathbb{Z}_p^{h'}$. Now, let $e = (x,y,z) \in \mathbb{Z}_p^{h'} \setminus \mathcal{E}$ with $y, z \neq 1$. Then there exist $\alpha, \beta \in A$ both different from $-4$ such that $\alpha + \beta + 2 + x = 0$. Therefore

$$(x,y,z) + (\alpha,1,1) + (\beta,1,1) + (1,-y-3,1) + (1,1,-z-3) = (0,0,0),$$

and hence $e$ is covered by $\mathcal{E}$. The same holds for $e = (x,y,z) \in \mathbb{Z}_p^{h'} \setminus \mathcal{E}$ with $x, y \neq 1$ or $x, z \neq 1$. The only noncovered elements are $(-4,1,1), (1,-4,1), (1,1,-4)$. □

### 4.2.5 Construction of $(k,4)$-arcs from union of cosets of $M$

We fix three (not necessarily distinct) subsets $\mathcal{K}_{e_1}$, $\mathcal{K}_{e_2}$, and $\mathcal{K}_{e_3}$, defined as in (4.20), and a point $P=(t,t^5)$ in $\mathcal{Q}\setminus(\mathcal{K}_{e_1}\cup\mathcal{K}_{e_2}\cup\mathcal{K}_{e_3})$. Clearly $P$ belongs to some subset $\mathcal{K}_{e_P}$ for some $e_P\in\mathbb{F}_q$.

Let $A_1=(x^\sigma-x+e_1,(x^\sigma-x+e_1)^5)\in\mathcal{K}_{e_1}$, $A_2=(y^\sigma-y+e_2,(y^\sigma-y+e_2)^5)\in\mathcal{K}_{e_2}$, and $A_3=(z^\sigma-z+e_3,(z^\sigma-z+e_3)^5)\in\mathcal{K}_{e_3}$. By Proposition 4.2.6, the four points $P$, $A_1$, $A_2$, and $A_3$ are collinear if and only if

$$\begin{cases} t^3+t^2\left(x^\sigma-x+e_1+y^\sigma-y+e_2\right)+t\big((x^\sigma-x+e_1)^2+(x^\sigma-x+e_1)(y^\sigma-y+e_2)\\ +(y^\sigma-y+e_2)^2\big)+(x^\sigma-x+e_1+y^\sigma-y+e_2)\left((x^\sigma-x+e_1)^2+(y^\sigma-y+e_2)^2\right)=0,\\ \\ (z^\sigma-z+e_3)^2+(z^\sigma-z+e_3)\left(x^\sigma-x+e_1+y^\sigma-y+e_2+t\right)+(x^\sigma-x+e_1)^2\\ +(y^\sigma-y+e_2)^2+t^2+(x^\sigma-x+e_1)(y^\sigma-y+e_2)+(x^\sigma-x+e_1)t+(y^\sigma-y+e_2)t=0. \end{cases} \tag{4.28}$$

Consider the following sequence of function fields:

$$\begin{tikzcd}
L_5=L_4(z): \arrow[d, dash, "\sigma"] & z^\sigma-z=w \\
L_4=L_3(w): \arrow[d, dash, "2"] & \begin{array}{l}(w+e_3)^2+(w+e_3)\left(x^\sigma-x+e_1+y^\sigma-y+e_2+t\right)\\ +(x^\sigma-x+e_1)^2+(y^\sigma-y+e_2)^2+t^2\\ +(x^\sigma-x+e_1)(y^\sigma-y+e_2)+(x^\sigma-x+e_1)t+(y^\sigma-y+e_2)t=0\end{array} \\
L_3=L_2(y): \arrow[d, dash, "\sigma"] & y^\sigma-y=v \\
L_2=L_1(x): \arrow[d, dash, "\sigma"] & x^\sigma-x=u \\
L_1=\mathbb{F}_q(u,v): & \begin{array}{l}t^3+t^2\left(u+e_1+v+e_2\right)+t\big((u+e_1)^2+(u+e_1)(v+e_2)\\ +(v+e_2)^2\big)+(u+e_1+v+e_2)\left((u+e_1)^2+(v+e_2)^2\right)=0\end{array}
\end{tikzcd}$$

We now show that each extension $L_i|L_{i-1}$ is well-defined and that the constant field of each $L_i$ is $\mathbb{F}_q$. We also estimate the genus of $L_i$. Finally, by using the Hasse-Weil bound, we show that if $q$ is large enough, then $L_5$ has a large number of $\mathbb{F}_q$-rational places, so that Equations (4.28) have a suitable solution.

**Proposition 4.2.23.** *The equation* $f_1(u,v)=0$, *where*

$$\begin{aligned} f_1(u,v)=t^3+t^2\left(u+e_1+v+e_2\right)+t\left((u+e_1)^2+(u+e_1)(v+e_2)+(v+e_2)^2\right)\\ +\left(u+e_1+v+e_2\right)\left((u+e_1)^2+(v+e_2)^2\right), \end{aligned} \tag{4.29}$$

*defines a function field* $L_1=\mathbb{F}_q(u,v)$ *with genus* $1$ *whose field of constants is* $\mathbb{F}_q$.

*Proof.* Let $\Gamma_1$ be the plane curve with equation $f_1(U,V) = 0$, whose function field over $\mathbb{F}_q$ is $L_1$. The curve $\Gamma_1$ has three distinct ideal points; hence, they are simple points. Since

$$\partial_U f_1(U,V) = 3(U+e_1)^2 + 2(U+e_1)(V+e_2) + (V+e_2)^2 + 2t(U+e_1) + t(V+e_2) + t^2\,,$$
$$\partial_V f_1(U,V) = (U+e_1)^2 + 2(U+e_1)(V+e_2) + 3(V+e_2)^2 + t(U+e_1) + 2t(V+e_2) + t^2\,,$$

we have by direct computation that $\Gamma_1$ has no singular affine points; here we use that $t \neq 0$, $p > 5$, and $\sigma \equiv 3 \pmod 4$. Therefore, $\Gamma_1$ is non-singular. Then $\Gamma_1$ is absolutely irreducible with genus 1 and constant field $\mathbb{F}_q$ by Lemma 1.1.36. □

Let $\xi$ be a primitive 4-th root of unity. For $i = 1, 2, 3$, denote by $P_1^i$ the point of $\mathbb{K}(u,v)$ centered at the ideal point $(1 : \xi^i : 0)$ of $\Gamma_1$.

**Proposition 4.2.24.** *The equation $x^\sigma - x = u$ defines an extension $L_2 = L_1(x)$ with genus $g_2 = 3\sigma - 2$ whose field of constants is $\mathbb{F}_q$.*

*Proof.* The rational function $u$ has valuation $-1$ at $P_1^i$ $(i = 1, 2, 3)$, and non-negative valuation at the places centered at the affine points of $\Gamma_1$. Then $\mathbb{K}(x,v)|\mathbb{K}(u,v)$ is a generalized Artin-Schreier extension with $[\mathbb{K}(x,v) : \mathbb{K}(u,v)] = \sigma$. Moreover, $P_1^1$, $P_1^2$, and $P_1^3$ are the only totally ramified places, and

$$g_2 = \sigma \cdot 1 + \frac{\sigma - 1}{2}(-2 + 3(1+1)) = 3\sigma - 2\,.$$

By Lemma 1.1.36, $\mathbb{F}_q$ is the constant field of $L_2 = \mathbb{F}_q(x,v)$. □

For $i = 1, 2, 3$, denote by $P_2^i$ the unique place of $\mathbb{K}(x,v)$ lying over $P_1^i$.

**Proposition 4.2.25.** *The equation $y^\sigma - y = u$ defines an extension $L_3 = L_2(y)$ with genus $g_3 = 3\sigma^2 - 2$ whose field of constants is $\mathbb{F}_q$.*

*Proof.* For $i \in \{1,2,3\}$, we have $v_{P_2^i}(v - \xi^i u) \geq 0$. Let $k_i \in \mathbb{K}$ be such that $k_i^\sigma = \xi^i$, and consider $\rho_i = k_i x$; then,

$$v - (\rho_i^\sigma - \rho_i) = v - \xi^i x^\sigma + k_i x = v - \xi^i x^\sigma + \xi^i x - \xi^i x + k_i x = v - \xi^i u + (k_i - \xi^i)x.$$

For $i = 2$, we have $\xi^2 = -1 = k_2$; hence, $v_{P_2^2}(v - (\rho_i^\sigma - \rho_i)) \geq 0$. For $i \in \{1,3\}$, we have $k_i \neq \xi^i$ since $4 \nmid (\sigma - 1)$; hence, $v_{P_2^i}((k_i - \xi^i)x) = -1$ and $v_{P_2^i}(v - (\rho_i^\sigma - \rho_i)) = -1$. For the places centered at affine points, it is sufficient to choose $\rho = 0$. Then $\mathbb{K}(x,y)|\mathbb{K}(x,v)$ is a generalized Artin-Schreier extension with $[\mathbb{K}(x,y) : \mathbb{K}(x,v)] = \sigma$. Moreover, $P_2^1$ and $P_2^3$ are the only totally ramified places, and

$$g_3 = \sigma(3\sigma - 2) + \frac{\sigma - 1}{2}(-2 + 2(1+1)) = 3\sigma^2 - \sigma - 1.$$

Finally, by Lemma 1.1.36, $\mathbb{F}_q$ is the constant field of $L_3 = \mathbb{F}_q(x,y)$. □

For $i \in \{1,3\}$, denote by $P_3^i$ the unique place of $\mathbb{K}(x,y)$ lying over $P_2^i$. Also, denote by $P_3^{2,1}, \ldots, P_3^{2,\sigma}$ the places lying over $P_2^2$.

**Proposition 4.2.26.** *The equation*

$$\begin{array}{l}(w+e_3)^2+(w+e_3)\,(u+e_1+v+e_2+t)+(u+e_1)^2\\ +(v+e_2)^2+t^2+(u+e_1)(v+e_2)+(u+e_1)t+(v+e_2)t=0\end{array} \tag{4.30}$$

*defines an extension $\mathbb{F}_q(u,v,w)$ of $\mathbb{F}_q(u,v)$ with genus at most 4 whose field of constants is $\mathbb{F}_q$.*

*Proof.* After the substitution $\theta = w+e_3+(u+e_1+v+e_2+t)/2$, we have

$$\begin{array}{l}\theta^2=\Theta(u,v)=\\ -\frac{1}{4}\big[3(u+e_1)^2+3(v+e_2)^2+3t^2+2(u+e_1)(v+e_2)+2(u+e_1)t+2(v+e_2)t\big].\end{array}$$

The poles of $w$ and $\theta$ in $\mathbb{K}(u,v)$ are $P_1^1$, $P_1^2$, and $P_1^3$; $\theta^2$ has valuation 2 at each of them. Hence, the number of zeros of $\theta^2$ in $\mathbb{K}(u,v)$ is at most 6. Let $D_1(U,V)$ be the discriminant of $\Theta(U,V)$ with respect to $U$, and let $R \in \mathbb{K}$ be the resultant of $D_1(U,V)$ and $f_1(U,V)$ with respect to $V$, where $f_1(u,v)$ is defined in (4.29). By direct computation, $R \neq 0$. Since $f_1(U,V)$ has odd degree, this implies that $\theta$ has a zero in $\mathbb{K}(u,v)$ with odd multiplicity. Then $\mathbb{K}(u,v,\theta)|\mathbb{K}(u,v)$ is a Kummer extension with $[\mathbb{K}(u,v,\theta):\mathbb{K}(u,v)]=2$. Moreover, the unique totally ramified places are the zeros of $\theta^2$ in $\mathbb{K}(u,v)$ with odd multiplicity, and

$$g(\mathbb{F}_q(u,v,w)) = g(\mathbb{F}_q(u,v,\theta)) \leq 1+2(1-1)+\frac{1}{2}\cdot 6 = 4.$$

Finally, by Lemma 1.1.36, $\mathbb{F}_q$ is the constant field of $\mathbb{F}_q(u,v,w)$. □

The function field $L_4$ is the compositum of $\mathbb{F}_q(u,v,w)$ and $L_3$. The extension $L_4|L_1$ has degree $[\mathbb{F}_q(u,v,w):L_1]\cdot[L_3:L_1]=2\sigma^2$, since 2 and $\sigma^2$ are coprime. Also, $\mathbb{F}_q$ is the field of constants of $L_4$.

For $i=1,2,3$ and $j=1,2$, denote by $\widetilde{Q}_i^j$ the place of $\mathbb{K}(u,v,w)$ lying over $P_i$, and by $Q_i^j$ the place of $L_4$ lying over $\widetilde{Q}_i^j$. The places $\widetilde{Q}_2^1$, $\widetilde{Q}_2^2$ are centered at the ideal points $(1:-1:\xi:0)$, $(1:-1:-\xi:0)$.

**Proposition 4.2.27.** *The equation $z^\sigma - z = w$ defines an extension $L_5 = L_4(z)$ with genus $g_5 \leq 21\sigma^3-9\sigma^2-6\sigma+1$ whose field of constants is $\mathbb{F}_q$.*

*Proof.* We have $v_{\widetilde{Q}_2^1}(u) = v_{\widetilde{Q}_2^1}(w) = -1$, and $w=\xi u+\Phi$ for some $\Phi \in \mathbb{K}(u,v,w)$ with $v_{\widetilde{Q}_2^1}(\Phi)\geq 0$. Since $\sigma \equiv 3 \pmod 4$, we have $\xi \notin \mathbb{F}_\sigma$; hence, there exists $k \in \mathbb{K}$ with $k^\sigma = \xi$ and $k \neq \xi$. Let $\rho = kx$; then $w-(\rho^\sigma-\rho)=(k-\xi)x+\Phi$. Since

$v_{Q_2^1}(\Phi) = e(Q_2^1|\widetilde{Q}_2^1) \cdot v_{\widetilde{Q}_2^1}(\Phi) \geq 0$ and $v_{Q_2^1}(x) = e(Q_2^1|P_2) \cdot v_{P_2}(x) = -1$, we have $v_{Q_2^1}(w - (\rho^\sigma - \rho)) = -1$. Arguing as in the proof of Proposition 4.2.16, it is easily proved that $\gamma t \neq \zeta^p - \zeta$ for all $\zeta \in \mathbb{K}(x,y,t)$ and $\gamma \in \mathbb{F}_\sigma$. Then we can apply Lemma 1.3 in [46] to conclude that $T^\sigma - T - w$ is irreducible over $\mathbb{K}(x,y,t)$, and $\mathbb{K}(x,y,z)|\mathbb{K}(x,y,w)$ is an Artin-Schreier extension of degree $\sigma$. Also, by Lemma 1.1.36, $\mathbb{F}_q$ is the constant field of $\mathbb{F}_q(x,y,z)$. Finally, we give a bound on $g_5$. By Castelnuovo's Inequality,

$$g_5 \leq [L_5 : L_3]\cdot g_3 + [L_5 : \mathbb{F}_q(u,v,z)]\cdot g(\mathbb{F}_q(u,v,z)) + ([L_5 : L_3]-1)\cdot([L_5 : \mathbb{F}_q(u,v,z)]-1)\,.$$

We have $[L_5 : L_3] = [L_5 : L_4] \cdot [L_4 : L_3] = 3\sigma$ and $g_3 = 3\sigma^2 - \sigma - 1$. Since $\{x, x^2, \ldots, x^\sigma\}$ is a basis of $\mathbb{F}_q(x,v,z)$ over $\mathbb{F}_q(u,v,z)$ and $\{y, y^2, \ldots, y^\sigma\}$ is a basis of $L_5$ over $\mathbb{F}_q(x,v,z)$, we have that $\{x^i y^j \mid i,j = 1,\ldots,\sigma\}$ is a basis of $L_5$ over $\mathbb{F}_q(u,v,z)$; hence, $[L_5 : \mathbb{F}_q(u,v,z)] = \sigma^2$.

For $i = 1,2,3$, the place $P_i$ does not ramify in $\mathbb{K}(u,v,w)|\mathbb{K}(u,v)$; hence, by (4.30), $w$ has valuation $-1$ at the places $\widetilde{Q}_i^j$ over $P_i$, whereas $w$ has non-negative valuation at any other place of $\mathbb{K}(u,v,w)$. Then $\mathbb{K}(u,v,z)|\mathbb{K}(u,v,w)$ is a generalized Artin-Schreier extension with $[\mathbb{K}(u,v,z) : \mathbb{K}(u,v,w)] = \sigma$ and

$$g(\mathbb{K}(u,v,z)) = \sigma \cdot 4 + \frac{\sigma - 1}{2}(-2 + 6(1+1)) = 9\sigma - 5.$$

Therefore,

$$g_5 \leq 3\sigma(3\sigma^2 - \sigma - 1) + \sigma^2(9\sigma - 5) + (3\sigma - 1)(\sigma^2 - 1) = 21\sigma^3 - 9\sigma^2 - 6\sigma + 1.$$

□

**Proposition 4.2.28.** *Assume that $q \geq 1764\sigma^6$. Then $P$ is collinear with three distinct points $A_1 \in \mathcal{K}_{e_1}$, $A_2 \in \mathcal{K}_{e_2}$, and $A_3 \in \mathcal{K}_{e_3}$.*

*Proof.* We are going to show that there exist $x_0, y_0, z_0 \in \mathbb{F}_q$ such that (4.28) holds for $x = x_0$, $y = y_0$, $z = z_0$, and $x_0^\sigma - x_0$, $y_0^\sigma - y_0$, $z_0^\sigma - z_0$ are pairwise distinct. We start by counting the number $Z_1$ of poles of $x^\sigma - x$, $y^\sigma - y$, and $z^\sigma - z$ in $\mathbb{K}(x,y,z)$. This is the number of places of $\mathbb{K}(x,y,z)$ lying over $P_3^1$, $P_3^3$, $P_3^{2,1}, \ldots, P_3^{2,\sigma}$; hence, $Z_1 \leq [\mathbb{K}(x,y,z) : \mathbb{K}(x,y)] \cdot (\sigma + 2) = 2\sigma^2 + 4\sigma$. Next we estimate the number $Z_2$ of zeros of $(x^\sigma - x) - (y^\sigma - y) = (x-y)^\sigma - (x-y)$ in $L_5$, hence the number of zeros of $x - y - \lambda$ for some $\lambda \in \mathbb{F}_\sigma$. We have

$$Z_2 \leq \textstyle\sum_{\lambda \in \mathbb{F}_\sigma} \deg(x - y - \lambda)_0 = \sum_{\lambda \in \mathbb{F}_\sigma} \deg(x - y - \lambda)_\infty = |\{P_1^1, P_1^2, P_1^3\}|\cdot[L_5 : L_1] = 6\sigma^3.$$

By the same argument, also $(x^\sigma - x) - (z^\sigma - z)$ and $(y^\sigma - y) - (z^\sigma - z)$ have at most $6\sigma^3$ zeros in $L_5$. Therefore, if the number $N_q$ of $\mathbb{F}_q$-rational places of $L_5$ is greater than $18\sigma^3+2\sigma^2+4\sigma$, then there exists an $\mathbb{F}_q$-rational place $A$ of $L_5$ such that the point $(x_0,y_0,z_0)=(x(A),y(A),z(A))$ is well defined and $x_0^\sigma-x_0$, $y_0^\sigma-y_0$, $z_0^\sigma-z_0$ are pairwise distinct. By Hasse-Weil bound,

$$N_q \geq q+1-2g_5\sqrt{q} \geq q+1-2(21\sigma^3-9\sigma^2-6\sigma+1)\sqrt{q}.$$

The hypothesis $q\geq 1764\sigma^6$ implies $N_q\geq 18\sigma^3+2\sigma^2+4\sigma+1$. □

**Proposition 4.2.29.** *Assume that $q\geq 1764\sigma^6$. Then $P$ is collinear with four distinct points $A_1\in\mathcal{K}_{e_1}$, $A_2\in\mathcal{K}_{e_2}$, $A_3\in\mathcal{K}_{e_3}$, and $A_4\in\mathcal{K}_{e_4}$.*

*Proof.* By Proposition 4.2.28, $P$ is collinear with three distinct points $A_1\in\mathcal{K}_{e_1}$, $A_2\in\mathcal{K}_{e_2}$, and $A_3\in\mathcal{K}_{e_3}$. The line through $A_1$, $A_2$, $A_3$, and $P$ can be a tangent line to the curve $\mathcal{Q}$. Note that there are at most five tangent lines through $P$ to $\mathcal{Q}$; in fact, imposing that $P$ lies on the tangent to $\mathcal{Q}$ at $(X,X^5)$ gives an equation in $X$ of degree 5. Therefore, we need at least six distinct triples $\{A_1,A_2,A_3\}$ such that $A_1$, $A_2$, $A_3$ are collinear with $P$. Arguing as in the proof of Proposition 4.2.28, it is sufficient to require that the number of $\mathbb{F}_q$-rational places of $L_5$ is greater than $5\cdot 18\sigma^3+2\sigma^2+4\sigma=90\sigma^3+2\sigma^2+4\sigma$. This is implied by the Hasse-Weil bound. □

Henceforth, $\mathcal{E}$ denotes a 5-independent subset of $\mathbb{F}_q/M$, for $M$ as in (4.19). Let

$$\mathcal{K}_\mathcal{E}=\bigcup_{M+e\,\in\,\mathcal{E}}\mathcal{K}_e\,. \tag{4.31}$$

**Proposition 4.2.30.** *The set $\mathcal{K}_\mathcal{E}$ is a $(k,4)$-arc.*

*Proof.* By Proposition 4.2.7, the sum of the first coordinate of 5 collinear points on $\mathcal{Q}$ is equal to 0. This is impossible if the points belong to $\mathcal{K}_\mathcal{E}$, since $\mathcal{E}$ is a 5-independent subset of $\mathbb{F}_q/M$. □

**Proposition 4.2.31.** *Assume that $q\geq 1764\sigma^6$. Let $Cov(\mathcal{E})$ be the set of all the elements of $\mathbb{F}_q/M$ covered by $\mathcal{E}$ as 5-independent subset. Then the points in*

$$\bigcup_{M+e\in Cov(\mathcal{E})}\mathcal{K}_e$$

*are covered by $\mathcal{K}_\mathcal{E}$.*

*Proof.* Let $P\in\mathcal{K}_{e_P}$ with $M+e_P\in Cov(\mathcal{E})$. Then there exist $M+e_1,M+e_2,M+e_3,M+e_4$ in $\mathcal{E}$ such that $e_P+e_1+e_2+e_3+e_4\in M$. Also, by Proposition 4.2.29, there exists four distinct points $P_1\in\mathcal{K}_{e_1}$, $P_2\in\mathcal{K}_{e_2}$, $P_3\in\mathcal{K}_{e_3}$, and $P_4\in\mathcal{Q}$ which are collinear with $P$. Let $e_4'$ be such that $P_4\in\mathcal{K}_{e_4'}$. By Proposition 4.2.7, $e_P+e_1+e_2+e_3+e_4'\in M$. Then $M+e_4=M+e_4'$, that is, $\mathcal{K}_{e_4}=\mathcal{K}_{e_4'}$. Hence, $P_1,P_2,P_3,P_4\in\mathcal{K}_\mathcal{E}$ and the assertion is proved. □

**Theorem 4.2.32.** *Let $\mathcal{E}$ be a 5-independent subset of $\mathbb{F}_q/M$ of size $n$, not covering at most $m$ elements of $\mathbb{F}_q/M$, and let $\mathcal{K}_\mathcal{E}$ be as in* (4.31)*. Assume $q \geq 580644\sigma^8$. Then there exists a complete $(k, 4)$-arc $\mathcal{K}$ with $\mathcal{K}_\mathcal{E} \subset \mathcal{K} \subset \mathcal{Q}$ of size at most*

$$(n+m)\frac{q}{\sigma} + 8.$$

*Proof.* Fix a coset $M + e$ in $\mathcal{E}$. By Theorem 4.2.19, all the points of $\mathrm{PG}(2, q) \setminus \mathcal{Q}$ are covered by a $\mathcal{K}_e$ plus at most eight points covering the lines $Y = 0$ and $T = 0$. By Proposition 4.2.31, there are at most $m\frac{q}{\sigma}$ affine points of $\mathcal{Q}$ not covered by $\mathcal{K}_\mathcal{E}$. This shows that there exists a complete $(k, 4)$-arc $\mathcal{K}$ containing $\mathcal{K}_\mathcal{E}$ of size at most

$$|\mathcal{K}_\mathcal{E}| + m\frac{q}{\sigma} + 8 = (n+m)\frac{q}{\sigma} + 8.$$

□

We are finally in a position to prove Theorem 4.2.1. Identify the additive groups $\mathbb{Z}_p^{h'}$ and $\mathbb{F}_q/M$. From Propositions 4.2.21 and 4.2.22 the following values of $n$ and $m$ occur in Theorem 4.2.32:

- For $\sigma = p$, $p \geq 29$, $p \equiv i \in \{1, 2, 3, 4\} \pmod 5$,

$$n = \frac{p-5-i}{5} \quad \text{and} \quad m = i - 1;$$

- for $\sigma \geq p^3$,

$$n = 2p^{\frac{h'-1}{2}} + p - 5 \quad \text{and} \quad m = 3.$$

## 4.3 Complete permutation polynomials from exceptional polynomials

Let $q$ be a prime power. A *permutation polynomial* (or PP) of $\mathbb{F}_q$ is a polynomial $f(x) \in \mathbb{F}_q[x]$ which is a bijection of $\mathbb{F}_q$ onto itself. A polynomial $f(x) \in \mathbb{F}_q[x]$ is a *complete permutation polynomial* (or CPP), if both $f(x)$ and $f(x) + x$ are permutation polynomials of $\mathbb{F}_q$. A polynomial $f(x) \in \mathbb{F}_q[x]$ is said to be an *exceptional polynomial* over $\mathbb{F}_q$ if $f(x)$ is a permutation polynomial of $F_{q^m}$ for infinitely many $m$. Both permutation polynomials and complete permutation polynomials have been extensively studied also because of their applications to cryptography and combinatorics; see for instance [23, 71, 95, 93, 102, 120] and the references therein.

In particular, CPPs over fields of characteristic 2 give rise to bent-negabent boolean functions, which are a useful tool in cryptography; see [106].

Some families of CPPs are obtained in [23, 71, 93, 97, 114, 120]. Nevertheless, CPPs seem to be very rare objects, even if we restrict to the monomial case. It is easily seen that a monomial $ax^d$ is a CPP of $\mathbb{F}_q$ if and only if $(d, q-1) = 1$ and $x^d + \frac{x}{a}$ is a PP of $\mathbb{F}_q$. This motivates the investigation of permutation binomials of type $x^d + bx$ for $d = (q-1)/m + 1$ with $m$ a divisor of $q-1$.

In [12, 11, 13, 120, 121] PPs of type $f_b(x) = x^{\frac{q^n-1}{q-1}+1} + bx$ over $\mathbb{F}_{q^n}$ are thoroughly investigated for $n = 2$, $n = 3$, and $n = 4$. For $n = 6$, sufficient conditions for $f_b$ to be a PP of $\mathbb{F}_{q^6}$ are provided in [120, 121] in the special cases of characteristic $p \in \{2, 3, 5\}$. The case $p = n + 1$ is dealt with in [84].

In this section we discuss monomial CPPs of $\mathbb{F}_{q^n}$ of degree $d = \frac{q^n-1}{q-1}$ for general $n$, in connection with exceptional polynomials. The starting point of our investigation is the observation that $b^{-1}x^d \in \mathbb{F}_{q^n}[x]$ is a CPP of $\mathbb{F}_{q^n}$ if and only if $b, b^q, \ldots, b^{q^{n-1}}$ are the roots of

$$v_g(x) = \frac{g(-x) - g(0)}{-x} \in \mathbb{F}_q[x]$$

for some permutation polynomial $g(x)$ of $\mathbb{F}_q$ of degree $n + 1$ such that the first-degree term is not zero. If for a root $b$ of $v_g(x)$ the monomial $b^{-1}x^d$ is a CPP of $\mathbb{F}_{q^n}$, then $g(x)$ will be called a *good* PP of $\mathbb{F}_q$; in this case, all roots of $v_g(x)$ have the same property. Clearly, a PP $g(x)$ of $\mathbb{F}_q$ is good if and only if the roots of $v_g(x)$ in the algebraic closure $\mathbb{K}$ of $\mathbb{F}_q$ form a unique orbit under the action of the Frobenius map $x \mapsto x^q$.

Our aim is to classify good permutation polynomials over $\mathbb{F}_q$. Here we achieve this goal for all $n$, $n^4 < q$, with the exception of the cases $n + 1 = p^r$, with $r > 1$, and $n + 1 = p^r(p^r - 1)/2$, with $p \in \{2, 3\}$. For $n + 1 = p^r$ we provide several examples. Proposition 4.3.8 shows that, if $q = p^k$ and $n + 1$ is a prime different from $p$ satisfying $\gcd(n, k) = \gcd(n + 1, p^2 - 1) = 1$, then there exists a CPP od degree $d = \frac{q^n-1}{q-1} + 1$ over $\mathbb{F}_{q^n}$. This solves a conjecture by Wu, Li, Helleseth, and Zhang, see [121, Conjecture 4.18 and Proposition 4.19].

Note that since every permutation polynomial with degree less than $q^{1/4}$ is exceptional (see [94, Theorem 8.4.19]), condition $n^4 < q$ allows us to consider only exceptional polynomials. A key tool is the classification of indecomposable exceptional polynomials of degree different from $p^r$, $r > 1$; see [94, Section 8.4].

If $g(x)$ is a good PP over $\mathbb{F}_q$ then it is easily seen that $c \cdot g(c'x) + e$ is a good PP over $\mathbb{F}_q$ for each $c, c', e \in \mathbb{F}_q$ with $cc' \neq 0$. In this paper two PPs $g(x)$ and $h(x)$ over $\mathbb{F}_q$ will be called *CPP-equivalent* if there exist $c, c', e \in \mathbb{F}_q$ with $cc' \neq 0$ such that $h(x) = c \cdot g(c'x) + e$. Note that for $g(x)$ a PP over $\mathbb{F}_q$ and $k \in \mathbb{F}_q$, the permutation polynomials $g(x + k)$ and $g(x)$ are equivalent in the usual sense but not CPP-equivalent; in fact, it's possible that one of them is good but the other is not. When $g'(x)$ ranges over the CPP-equivalence class of $g(x)$, the roots of $v_{g'}(x)$ range over the roots of $v_g(x)$ and their multiples by non-zero elements in $\mathbb{F}_q$. We will consider only one polynomial in a CPP-equivalence class. In particular, we assume that $g(x)$ is monic and that $g(0) = 0$. Since exceptional polynomials only exist for degrees coprime with $q-1$, when $n$ is odd we assume that $p = 2$.

Our first result is that if $g$ is decomposable, that is $g$ is a composition of two exceptional polynomials with degree grater than one, then $g$ is not good.

If $g(x) \in \mathbb{F}_q[x]$ is a monic indecomposable exceptional polynomial of degree $n+1$ with $g(0) = 0$, then, up to CPP-equivalence, one of the following holds [94, Section 8.4].

A) $n+1$ is a prime different from $p$ not dividing $q-1$, and

A1) $g(x) = (x+e)^{n+1} - e^{n+1}$, with $e \in \mathbb{F}_q$, or

A2) $g(x) = D_{n+1}(x+e, a) - D_{n+1}(e, a)$, where $a, e \in \mathbb{F}_q$, $a \neq 0$, $n+1 \nmid q^2 - 1$, and $D_{n+1}(x, a)$ denotes a Dickson polynomial of degree $n+1$.

B) $n+1 = p$ and $g(x) = (x+e)((x+e)^{\frac{p-1}{r}} - a)^r - e(e^{\frac{p-1}{r}} - a)^r$, with $r \mid p-1$, $a, e \in \mathbb{F}_q$, and $a^{r(q-1)/(p-1)} \neq 1$.

C) $n+1 = s(s-1)/2$, where $p \in \{2, 3\}$, $q = p^m$, $r > 1$, $s = p^r > 3$, and $(r, 2m) = 1$.

D) $n+1 = p^r$ with $r > 1$.

For the case $n+1 = p^r$, $r > 1$, Guralnick and Zieve conjectured in [62] that there are no examples of indecomposable exceptional polynomials other than those described in [94, Propositions 8.4.15, 8.4.16, 8.4.17].

The section is organized as follows. We classify good exceptional polynomials of type A) and B) in Sections 4.3.2 and 4.3.5; see Theorems 4.3.5 and 4.3.9. We describe some good exceptional polynomials of type C) and D) in Sections 4.3.6 and 4.3.7; see Propositions 4.3.10, 4.3.11, 4.3.12 and 4.3.13. Finally, we determine all the exceptional polynomials of degree 8 and 9 (see Propositions 4.3.14 and 4.3.18); in this way we provide a proof of the above mentioned Guralnick-Zieve conjecture for the special cases $n = 8, 9$. As a byproduct, we obtain all the CPPs with $n+1 = 8$ and $n+1 = 9$; see Corollaries 4.3.17 and 4.3.22 in Section 4.3.8.

### 4.3.1 Preliminaries

Throughout Section 4.3, $\zeta_s$ denotes a $s$-th primitive root of unity, $s \geq 1$, and $\varphi$ denotes the Frobenius map $x \mapsto x^q$. For $b \in \mathbb{F}_{q^n}$, let $A_i(b) \in \mathbb{F}_q$ denote the evaluation of the $i$-th elementary symmetric polynomial in $b, b^q, \ldots, b^{q^{n-1}}$, that is,

$$A_i(b) = \sum_{0 \le j_1 < j_2 < \ldots < j_i \le n-1} b^{q^{j_1}+q^{j_2}+\ldots+q^{j_i}}.$$

Let $A_0(b) = 1$. Recall that $b, b^q, \ldots, b^{q^{n-1}}$ are the roots of the polynomial

$$(-1)^n A_n(b) + (-1)^{n-1} A_{n-1}(b) T + \ldots + (-1)^{n-i} A_{n-i}(b) T^i + \ldots + T^n.$$

By [119, Lemma 5] we have the following result.

**Proposition 4.3.1.** *Assume that $n^4 < q$. The monomial $b^{-1}x^{\frac{q^n-1}{q-1}+1}$ is a CPP of $\mathbb{F}_{q^n}$ if and only if $\gcd(n+1, q-1) = 1$ and $\sum_{i=0}^{n} A_{n-i}(b) x^{i+1}$ is an exceptional polynomial over $\mathbb{F}_q$.*

Let $g(x) = \sum_{i=0}^{n+1} \lambda_{n+1-i} x^i$ be an exceptional polynomial over $\mathbb{F}_q$, and assume that $\lambda_n \neq 0$ and $\lambda_0 = 1$. Consider the polynomial

$$h_g(x) = \frac{g(x) - g(0)}{x} = \frac{\sum_{i=1}^{n+1} \lambda_{n+1-i} x^i}{x} = \sum_{i=0}^{n} \lambda_{n-i} x^i.$$

Then $v_g(x) := h_g(-x) = \sum_{i=0}^{n} (-1)^i \lambda_{n-i} x^i$. If $n$ is even, $h_g(-x)$ can be written as $\sum_{i=0}^{n} (-1)^{n-i} \lambda_{n-i} x^i$. If $n$ is odd, then $p = 2$ and the same relation holds.

This means that, for any root $b$ of $v_g(x)$, the monomial $b^{-1}x^{\frac{q^n-1}{q-1}+1}$ is a CPP over $\mathbb{F}_{q^n}$ if and only if the roots of $v_g(x)$, or equivalently $h_g(-x)$, form a unique orbit under the $\varphi_q$. This motivates the following definition.

**Definition 4.3.2.** *An exceptional polynomial $g(x) \in \mathbb{F}_q[x]$ with $g(0) = 0$ and $g'(0) \neq 0$ is said to be* good *if the roots of $\frac{g(-x)}{-x}$ form a unique orbit under $\varphi_q$.*

Therefore, the following has been proved.

**Proposition 4.3.3.** *Assume that $n^4 < q$. Then the elements $b \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$ such that $b^{-1}x^{\frac{q^n-1}{q-1}+1}$ is a CPP over $\mathbb{F}_{q^n}$ are the roots of polynomials $\frac{g(-x)}{-x}$, for $g$ ranging over good exceptional polynomials of degree $n+1$ over $\mathbb{F}_q$, with $g(0) = 0$ and $g'(0) \neq 0$.*

Note that $h_g(x)$ can be viewed as the bivariate polynomial $\frac{g(x)-g(y)}{x-y}$ evaluated at $y = 0$. So, assume that we know the factorization of $\frac{g(x)-g(y)}{x-y}$ into absolutely irreducible factors defined over the algebraic closure of $\mathbb{F}_q$, say $\frac{g(x)-g(y)}{x-y} = \prod_{k=1}^{s} \ell_k(x,y)$. Then

$$h_g(x) = \prod_{k=1}^{s} \ell_k(x, 0).$$

Obviously, this can be extremely useful to establish whether an exceptional polynomial $g$ is good or not. Recall that an exceptional polynomial $g(t)$ is *decomposable* if there exist exceptional polynomials $g_1$, $g_2$ with degree greater than 1 such that $g(x) = g_1(g_2(x))$.

**Proposition 4.3.4.** *If $g(x)$ is a good exceptional polynomial, then $g(x)$ is not decomposable.*

*Proof.* Suppose that $g(x)$ is decomposable and write $g(x) = g_1(g_2(x))$, with polynomials $g_1, g_2$ such that $\deg(g_1), \deg(g_2) > 1$. Then

$$v_g(x) = \frac{g_1(g_2(-x)) - g_1(g_2(0))}{-x} = \frac{g_2(-x) - g_2(0)}{-x}\lambda(g_2(-x)),$$

with

$$\lambda(g_2(-x)) = \prod_{i=1}^{\deg(g_1)-1} (g_2(-x) - \beta_i)$$

for some $\beta_i \in \mathbb{K}$. Since $\frac{g_2(-x)-g_2(0)}{-x}$ is a factor of positive degree defined over $\mathbb{F}_q$, the only possibility for the roots of $v_g(x)$ to form a unique orbit under $\varphi_q$ is that $v_g(x)$ is a power of $\frac{g_2(-x)-g_2(0)}{-x}$. Note that 0 cannot be a root of $v_g(x)$, since for $b = 0$ the monomial $bx^{\frac{q^n-1}{q-1}+1}$ is not a CPP. On the other hand, any root of a factor $g_2(-x) - \beta_i$ must be a root of $g_2(-x) - g_2(0)$, that is $\beta_i = g_2(0)$. Therefore,

$$v_g(x) = \left(\frac{g_2(-x) - g_2(0)}{-x}\right)^{\deg(g_1)} (-x)^{\deg(g_1)-1},$$

which is impossible since $\deg(g_1) > 1$. □

### 4.3.2 CPPs from exceptional polynomials of type A)

Throughout this section we assume that $n + 1 \geq 3$ is a prime different from $p$. We denote by $T_{q^{n/2}}$ the absolute trace map $\mathbb{F}_{q^{n/2}} \to \mathbb{F}_2$, $x \mapsto x + x^2 + x^4 + \cdots + x^{(q^{n/2})/2}$. We are going to prove the following result.

**Theorem 4.3.5.** *Assume that $n^4 < q$. For $i \in \{1, \ldots, n/2\}$ let*

$$\alpha_i = \zeta_{n+1}^i + \zeta_{n+1}^{-i} \text{ and } \beta_i = \zeta_{n+1}^i - \zeta_{n+1}^{-i}.$$

*Then the monomial $b^{-1}x^{\frac{q^n-1}{q-1}+1}$ is a CPP of $\mathbb{F}_{q^n}$ precisely in the following cases:*

- *If $p \neq 2$:*

*i) the order of $q$ modulo $n+1$ is $n$ and, up to multiplication by a non-zero element in $\mathbb{F}_q$, $b$ is as follows:*

*(a) $b = \zeta_{n+1}^i - 1$, for some $i \in \{1, \dots, n\}$;*

*(b) for $n/2$ even, $b = e(\alpha_i - 2) \pm \sqrt{\beta_i^2(e^2 - 4a)}$ for some $i \in \{1, \dots n/2\}$, $a \in \mathbb{F}_q^*$, and $e \in \mathbb{F}_q$;*

*(c) for $n/2$ odd, $b = e(\alpha_i - 2) \pm \sqrt{\beta_i^2(e^2 - 4a)}$ for some $i \in \{1, \dots n/2\}$, $a \in \mathbb{F}_q^*$, and $e \in \mathbb{F}_q$ s.t. $e^2 - 4a$ is a square in $\mathbb{F}_q$.*

*ii) the order of $q$ modulo $n+1$ is $n/2$, $n$ is not divisible by 4, and, up to multiplication by a non-zero element in $\mathbb{F}_q$, $b = e(\alpha_i - 2) \pm \sqrt{\beta_i^2(e^2 - 4a)}$ for some $i \in \{1, \dots n/2\}$, $a \in \mathbb{F}_q^*$, and $e \in \mathbb{F}_q$ s.t. $e^2 - 4a$ is 0 or a non-square in $\mathbb{F}_q$.*

- *If $p = 2$:*

*i) the order of $q$ modulo $n+1$ is $n$ and, up to multiplication by a non-zero element in $\mathbb{F}_q$, $b = \zeta_{n+1}^i$ for some $i \in \{1, \dots, n\}$;*

*ii) the order of $q$ modulo $n+1$ is $n$ or $n/2$, and*

$$b = z_i := \varepsilon\delta_i^2 + (\varepsilon+\varepsilon^2)\delta_i^4 + \cdots + (\varepsilon+\varepsilon^2+\cdots+\varepsilon^{q^n/4})\delta_i^{q^n/2} \quad or \quad b = z_i + 1,$$

*where $\varepsilon \in \mathbb{F}_{q^n}$ satisfies $T_{q^{n/2}}(\varepsilon) = 1$ and, for some $i \in \{1, \dots, n\}$, $\delta_i = \frac{1}{\alpha_i} + \frac{a}{e^2}$ and $T_{q^{n/2}}(\delta_i) = 1$.*

By Propositions 4.3.1 and 4.3.4, the determination of CPPs of type $b^{-1}x^{\frac{q^n-1}{q-1}+1}$ over $\mathbb{F}_{q^n}$ relies on the classification of indecomposable exceptional polynomials, which is given in [94, Section 8.4]. In particular, by [94, Theorem 8.4.11], Theorem 4.3.5 is implied by the results of Sections 4.3.3 and 4.3.4.

### 4.3.3 CPPs from exceptional polynomials of type A1)

Throughout this subsection we also assume that $n+1$ does not divide $q-1$. Note that for each $e \neq 0$ the polynomial $g(x) = (x+e)^{n+1} - e^{n+1}$ has a non-zero term of degree one. Also, the $n$ distinct roots of $h_g(-x) = \frac{(-x+e)^{n+1} - e^{n+1}}{-x}$ are

$$-e(\zeta_{n+1}^i - 1), \quad i = 1, \dots, n.$$

**Proposition 4.3.6.** *Assume that $e \in \mathbb{F}_q^*$. The polynomial $(x+e)^{n+1} - e^{n+1}$ is a good exceptional polynomial over $\mathbb{F}_q$ if and only if $q$ has order $n$ modulo $n+1$.*

*Proof.* The roots of $h_g(-x)$ form a unique orbit under $\varphi_q$ if and only if $\zeta_{n+1}$ does not belong to any proper subfield of $\mathbb{F}_{q^n}$. This is equivalent to the order of $q$ modulo $n+1$ being equal to $n$. □

**Corollary 4.3.7.** *Assume that $q$ has order $n$ modulo $n+1$. Then for $b = e(\zeta_{n+1}^i - 1)$ the monomial $b^{-1}x^{\frac{q^n-1}{q-1}+1}$ is a CPP of $\mathbb{F}_{q^n}$, for each $e \in \mathbb{F}_q^*$ and $i \in \{1, \dots, n\}$.*

### 4.3.4 CPPs from exceptional polynomials of type A2)

Throughout this subsection we further assume that $n+1$ does not divide $q^2-1$. We begin by considering Dickson polynomials $D_{n+1}(x,a) \in \mathbb{F}_q[x]$. Recall that

$$D_{n+1}(x,a) = \sum_{k=0}^{n/2} \frac{n+1}{n+1-k}\binom{n+1-k}{k}(-a)^k x^{n+1-2k}\,.$$

Note that $D_{n+1}(x,a)$ has a non-zero term of degree 1, for each $a \neq 0$. In [14, Th. 7 and 8] Bhargava and Zieve provide the factorization of $\frac{D_{n+1}(x+e,a)-D_{n+1}(y+e,a)}{x-y}$, $e \in \mathbb{F}_q$.

**Proposition 4.3.8.** *The polynomial $g(x) = D_{n+1}(x+e,a) - D_{n+1}(e,a)$, with $a, e \in \mathbb{F}_q$, $a \neq 0$ and $D'_{n+1}(e,a) \neq 0$, is a good exceptional polynomial over $\mathbb{F}_q$ if and only if one of the following cases occurs:*

*i) $p \neq 2$, $n/2$ is even and $q$ has order $n$ modulo $n+1$;*

*ii) $p \neq 2$, $n/2$ is odd and either $e^2-4a$ is a non-square in $\mathbb{F}_q$ and $q$ has order $n/2$ modulo $n+1$, or $e^2-4a$ is a square in $\mathbb{F}_q$ and $q$ has order $n$ modulo $n+1$;*

*iii) $p = 2$, the order of $q$ modulo $n+1$ is $n$ or $n/2$, and $T_{q^{n/2}}(\delta_1) = 1$, where $\delta_i = \frac{1}{\alpha_i} + \frac{a}{e^2}$.*

*In Cases i) and ii), the roots of $h_g(-x)$ are $b = -\frac{1}{2}\cdot\left(e(\alpha_i - 2) \pm \sqrt{\beta_i^2(e^2-4a)}\right)$. In Case iii), let $\varepsilon \in \mathbb{F}_{q^n}$ with $T_{q^{n/2}}(\varepsilon) = 1$. Then the roots of $h_g(-x)$ are*

$$b = \varepsilon\delta_i^2 + (\varepsilon+\varepsilon^2)\delta_i^4 + \cdots + (\varepsilon+\varepsilon^2+\cdots+\varepsilon^{q^n/4})\delta_i^{q^n/2} \quad \textit{and} \quad b+1.$$

*Proof.* By [14, Theorem 7] we have

$$D_{n+1}(x+e,a) - D_{n+1}(y+e,a) = (x-y)\prod_{i=1}^{n/2}\left((x+e)^2 - \alpha_i(x+e)(y+e) + (y+e)^2 + \beta_i^2 a\right),$$

where $\alpha_i = \zeta_{n+1}^i + \zeta_{n+1}^{-i}$ and $\beta_i = \zeta_{n+1}^i - \zeta_{n+1}^{-i}$. Then

$$h_g(-x) = \frac{D_{n+1}(-x+e,a) - D_{n+1}(e,a)}{-x} = \prod_{i=1}^{n/2} \left((-x+e)^2 - \alpha_i e(-x+e) + e^2 + \beta_i^2 a\right),$$

that is, since $\alpha_i^2 = \beta_i^2 + 4$,

$$h_g(-x) = \prod_{i=1}^{n/2} \left(x^2 + xe(\alpha_i - 2) + (\alpha_i - 2)((\alpha_i + 2)a - e^2)\right).$$

Note that the values $e(\alpha_i - 2)$ are pairwise distinct for $i = 1, \ldots, n$; hence, the sets of roots of two distinct quadratic factors of $h_g(-x)$ are disjoint.

Assume $p \neq 2$. Since $\alpha_i^2 = \beta_i^2 + 4$, the roots of $h_g(-x)$ are

$$-\frac{1}{2} \cdot \left(e(\alpha_i - 2) \pm \sqrt{\beta_i^2(e^2 - 4a)}\right).$$

Since $(\beta_i^2(e^2-4a))^{q^j} = \left(\beta_{iq^j \pmod{n+1}}\right)^2 (e^2 - 4a)$, if the roots of $h_g(-x)$ form a unique orbit under $\varphi_q$ then the order $ord_{n+1}(q)$ of $q$ in $\mathbb{Z}_{n+1}^*$ must be either $n$ or $n/2$. Thus, we check when $\beta_i^2(e^2-4a)$ is a non-square in $\mathbb{F}_{q^{n/2}}$, so that the $(n/2)$-th power of $\varphi_q$ permutes the roots of $h_g(-x)$. Note that if $ord_{n+1}(q) = n/2$, then $\beta_i^{q^{n/2}} = \beta_i$ and therefore $\beta_i^2$ is a square in $\mathbb{F}_{q^{n/2}}$; if on the contrary $ord_{n+1}(q) = n$, then $\beta_i^{q^{n/2}} = -\beta_i$ and $\beta_i^2$ is a non-square in $\mathbb{F}_{q^{n/2}}$. Also, $n/2$ even implies that $(e^2 - 4a)$ is always a square in $\mathbb{F}_{q^{n/2}}$, whereas if $n/2$ is odd then $(e^2 - 4a)$ is a square in $\mathbb{F}_{q^{n/2}}$ if and only if it is a square in $\mathbb{F}_q$.

If $e^2 - 4a = 0$, then $h_g(-x)$ is a square and its roots form a unique orbit under Frobenius. This completes the proof for $p \neq 2$.

For $p = 2$, similar computations using the solutions of quadratic equations in characteristic 2 provide the claim. □

### 4.3.5 CPPs from exceptional polynomials of type B)

Throughout this section we assume that $n+1 = p$. For $p = 2$, it is straightforward that there exist no exceptional polynomials of type B); hence, we assume that $p \neq 2$. We denote by $\mathbb{N}_{\mathbb{F}_q/\mathbb{F}_p}$ the norm map $\mathbb{F}_q \to \mathbb{F}_p$, $x \mapsto x^{1+p+p^2+\cdots+q/p}$.

**Theorem 4.3.9.** *Assume that $n^4 < q$. The monomial $b^{-1}x^{\frac{q^n-1}{q-1}+1}$ is a CPP of $\mathbb{F}_{q^n}$ if and only if, for some divisor $r$ of $n$, one of the following cases occurs:*

*i) $b$ is an element of $\left\{-\zeta_r^i \alpha \mid i \in \{0, \ldots, r-1\},\ \alpha^r = \zeta_{q-1}^j,\ \gcd(r,j) = 1\right\}$, or* *ii) b is an element of*

$$\Big\{(v_0-\lambda u_0)^r - e \mid \quad \lambda\in\mathbb{F}_p^*,\ e,u_0^{p-1}\in\mathbb{F}_q^*,\ u_0^{\frac{q-1}{r}}\neq 1,$$
$$v_0^r = e,\ ord\left(\mathbb{N}_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{u_0^{p-1}}{e^{(p-1)/r}}\right)\right)=p-1\Big\}.$$

*Proof.* Up to CCP-equivalence, the only indecomposable exceptional polynomials of degree $p$ over $\mathbb{F}_q$ are the polynomials $g(x)=(x+e)\left((x+e)^r-a\right)^k$, where $r$ is a divisor of $n$ and $k=n/r$, with $a,e\in\mathbb{F}_q$, $a^{\frac{q-1}{r}}\neq 1$; see [94, Theorem 8.4.14]. Hence, $h_g(-x)=\frac{1}{-x}\Big((-x+e)\left((-x+e)^r-a\right)^k - e\left(e^r-a\right)^k\Big)$. We distinguish a number of cases.

- $a=0$. In this case the polynomial $g(x)=(x+e)^p$ is not good.
- $e=0$ and $a\neq 0$. We have that $h_g(-x)=((-x)^r-a)^k$ has $r$ distinct roots with multiplicity $k$, namely $-\zeta_r^i\alpha$, where $\alpha^r=a$ and $i=0,\dots,k-1$. They form a single orbit under $\varphi_q$ if and only if $x^r-a$ is irreducible over $\mathbb{F}_q$. By [82, Theorem 3.75], this is equivalent to require that $a=\zeta_{q-1}^j$ with $\gcd(r,j)=1$.
- $e\neq 0$ and $a\neq 0$. Fix $u_0$, $v_0$ such that $u_0^{p-1}=a$ and $v_0^r=e$. It is straightforward to check that the set of roots of $h_g(-x)$ contains $R=\left\{(v_0-\lambda u_0)^r-e \mid \lambda\in\mathbb{F}_p^*\right\}$. Note that $e^k\neq a$, since $a^{\frac{q-1}{k}}\neq 1=\left(e^k\right)^{\frac{q-1}{k}}$. We show that $R$ actually consists of the $p-1$ distinct roots of $h_g(-x)$. Assume on the contrary that $(v_0-\lambda u_0)^r-e=(v_0-\lambda' u_0)^r-e$ for some $\lambda\neq\lambda'$. Then $v_0-\lambda u_0=\mu(v_0-\lambda' u_0)$ for some $\mu$ with $\mu^r=1$, and hence $v_0(1-\mu)=u_0(\lambda-\mu\lambda')$. Since $r$ divides $p-1$, both $\mu$ and $\mu-1$ lies in $\mathbb{F}_p$. As $\lambda\neq\lambda'$ we have $\mu\neq 1$ and hence $1=(v_0/u_0)^{p-1}=e^{\frac{p-1}{r}}/a=e^k/a$, a contradiction.

  In the following we prove that the elements of $R$ are in the same orbit under $\varphi_q$ if and only if
  $$ord\left(\mathbb{N}_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{a}{e^{(p-1)/r}}\right)\right)=p-1.$$

  Let $i\in\{1,\dots,p-1\}$ be the smallest positive integer such that $((v_0-\lambda u_0)^r-e)^{q^i}=(v_0-\lambda u_0)^r-e$, so that the elements of $R$ are in the same orbit under $\varphi_q$ if and only if $i=p-1$. Since $u_0^{q^i}=u_0a^{(q^i-1)/(p-1)}$ and $v_0^{q^i}=v_0e^{(q^i-1)/r}$, the condition $(v_0-\lambda u_0)^{rq^i}=(v_0-\lambda u_0)^r$ holds if and only if
  $$(v_0e^{(q^i-1)/r}-\lambda u_0a^{(q^i-1)/(p-1)})^r=(v_0-\lambda u_0)^r\,,$$

which is equivalent to

$$\left(v_0 - \lambda u_0 \frac{a^{(q^i-1)/(p-1)}}{e^{(q^i-1)/r}}\right)^r = (v_0 - \lambda u_0)^r \,,$$

that is,

$$v_0 - \lambda u_0 \frac{a^{(q^i-1)/(p-1)}}{e^{(q^i-1)/r}} = \xi(v_0 - \lambda u_0)\,,$$

with $\xi^r = 1$. Suppose $\xi \neq 1$; then

$$v_0/u_0 = \lambda \frac{\frac{a^{(q^i-1)/(p-1)}}{e^{(q^i-1)/r}} - \xi}{1-\xi} \in \mathbb{F}_p^*\,,$$

and hence $(v_0/u_0)^{p-1} = 1$; this implies $a = e^{(p-1)/r} = e^k$, impossible. This means $\xi = 1$, that is

$$\frac{a^{(q^i-1)/(p-1)}}{e^{(q^i-1)/r}} = 1\,. \tag{4.32}$$

Since

$$\frac{q^i-1}{p-1} \equiv \frac{i(q-1)}{p-1} \pmod{q-1} \quad \text{and} \quad \frac{q^i-1}{r} \equiv \frac{i(q-1)}{r} \pmod{q-1}\,,$$

Equation (4.32) is equivalent to

$$\frac{a^{i(q-1)/(p-1)}}{e^{i(q-1)/r}} = 1\,,$$

that is,

$$\left(\mathbb{N}_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{a}{e^{(p-1)/r}}\right)\right)^i = 1\,.$$

Thus, $i = p-1$ if and only if $ord\left(\mathbb{N}_{\mathbb{F}_q/\mathbb{F}_p}\left(\frac{a}{e^{(p-1)/r}}\right)\right) = p-1$.

□

### 4.3.6 CPPs from exceptional polynomials of type C)

In this section we deal with one of the three classes of exceptional polynomials of type C), namely the third class in [94, Theorem 8.4.12], with $e = 1$.

**Proposition 4.3.10.** *Let $p = 3$, $s = p^r > 3$, $\gcd(r, 2m) = 1$. The exceptional polynomial*

$$f_e(x) = (x+e)((x+e)^2 - a)^{(s+1)/4}\left(\frac{((x+e)^2-a)^{(s-1)/2} + a^{(s-1)/2}}{(x+e)^2}\right)^{(s+1)/2},$$

*where $a$ is a non-square in $\mathbb{F}_q^*$, is not good over $\mathbb{F}_q$.*

*Proof.* Following [123, Prop. 2], consider $\tau(y) = (Ey + F)/(\overline{F}y + \overline{E})$, with $E, F, \overline{E}, \overline{F} \in \mathbb{F}_{q^2}$ and $E\overline{E} - F\overline{F} = 1$. The points $(x, y)$ of the curve with equation $\frac{f_0(x)-f_0(y)}{x-y}$ are exactly the points such that $x = \tau(y)$, where the choice of $(E, F)$ is unique up to replacing $(E, F)$ by $(-E, -F)$ and one of the following cases occurs:

- $F\overline{F} = -1/2$ ;
- $\left(EF\overline{EF}\right)^{(q-1)/2} = -1$ and $F\overline{F} \neq -1/2$ ;
- $\left(EF\overline{EF}\right)^{(q-1)/2} = 1$ .

For $e \in \mathbb{F}_q$, a zero of $h_{f_e}(-x) = \frac{f_e(-x)-f_e(0)}{-x}$ corresponds to the point $(-x+e, e)$ of the curve defined by $\frac{f_0(x)-f_0(y)}{x-y} = 0$, that is $x = y - \tau(y)$ for some $\tau$ as described above. Since $E, F, \overline{E}, \overline{F} \in \mathbb{F}_{q^2}$, we have $(\tau(y))^{q^2} = \tau(y)$ and $x^{q^2} = x$. Therefore, the roots of $h_{f_e}(-x)$ are not in a unique orbit under $\varphi_q$. □

## 4.3.7 CPPs from exceptional polynomials of type D)

Throughout this section we assume that $n + 1 = p^r$ with $r > 1$. No complete classification of indecomposable exceptional polynomials of type D) is known. The following propositions deal with the cases related to linearized polynomials.

**Proposition 4.3.11.** *Let $j, k \geq 1$ and $H(x) \in \mathbb{F}_q[x]$ such that $L(x) = x^j H(x^k)$ is a linearized polynomial of degree $n + 1$. For $e \in \mathbb{F}_q$ we have that $S_e(x) = (x + e)^j H^k(x + e) - e^j H^k(e)$ is a good exceptional polynomial over $\mathbb{F}_q$ if and only if the elements $e - (e_0 - \ell)^k$ belong to a unique orbit under $\varphi_q$, where $e_0$ is a fixed $k$-th root of $e$ and $\ell$ ranges over the roots of $L(x) \setminus \{0\}$.*

*Proof.* Following [25, Theorem 2.1] we give the factorization of the curve defined by $S_0(x^k) - S_0(y^k) = 0$. Let $N := \deg(H) = \frac{(n+1)-j}{k}$ and write

$$H(t) = \prod_{h=1}^{N} (t - \gamma_h),$$

where $\gamma_h \in \mathbb{K}$. Then the roots of $H(t)$ and $L(x) = x^j H(x^k)$ are $\mathcal{H} = \{\gamma_h : h = 1, \dots, N\}$ and $\mathcal{L} = \{\zeta_k^i \gamma_h : i = 0, \dots, k-1,\ h = 1, \dots, N\} \cup \{0\}$, respectively.

Since $S_0(x^k) = (L(x))^k$, we have

$$S_0(x^k) - S_0(y^k) = (L(x))^k - (L(y))^k = \prod_{i=0}^{k-1} \left(L(x) - \zeta_k^i L(y)\right) = \prod_{i=0}^{k-1} L(x - \zeta_k^i y)$$

$$= \left(x^k - y^k\right)^j \prod_{\alpha=0}^{d-1} \prod_{\beta=0}^{d-1} \prod_{h=1}^{N} \left(y - \zeta_k^{\alpha} x - \zeta_k^{\beta} \gamma_h\right).$$

Consider the curve $\mathcal{C}_S$ defined by $S_0(x) - S_0(y) = 0$. Clearly, the points $(x, y)$ of $\mathcal{C}_S$ satisfy $\overline{y} = \zeta_k^{\alpha} \overline{x} + \zeta_k^{\beta} \gamma_h$, where $h \in \{1, \dots, N\}$, $\alpha, \beta \in \{0, \dots, k-1\}$, $\overline{x}^k = x$, $\overline{y}^k = y$. Now consider the polynomial $h_{S_e}(-x) = \frac{S_e(-x) - S_e(0)}{-x}$. The zeros of $h_{S_e}(-x)$ correspond to the points $(-x + e, e)$ of $\mathcal{C}_S$, $x \neq 0$. Fix $e_0$ such that $e_0^k = e$; then the zeros of $h(-x)$ are $\left\{e - (e_0 - \ell)^k \mid \ell \in \mathcal{L} \setminus \{0\}\right\}$. □

In general, it is not easy to establish when the elements $e - (e_0 - \ell)^k$ belong to the same orbit under $\varphi_q$. The following propositions provide two families of good exceptional polynomials arising from linearized polynomials.

**Proposition 4.3.12.** *Let $q = p^m$ and $L(x) = x^{p^r} - \zeta_{q-1} x \in \mathbb{F}_q[x]$. If $r$ divides $m$, then $L(x)$ is good exceptional over $\mathbb{F}_q$.*

*Proof.* Let $N = p^r - 1$, and let $\eta \in \mathbb{F}_{q^N}$ be a root of $h_L(-x) = x^N - \zeta_{q-1}$. Then the roots of $h_L(-x)$ are $\{\lambda\eta \mid \lambda \in \mathbb{F}_{p^r}^*\}$. The hypothesis $r \mid m$ is equivalent to require that $N$ divides $(q-1)$, and this implies that $N(q-1) \mid q^N - 1$. Hence we can choose $\eta = \omega^{\frac{q^N-1}{N(q-1)}}$, where $\omega$ is a primitive element of $\mathbb{F}_{q^N}$. The thesis is proved by showing that $\eta$ is not an element of any proper subfield of $\mathbb{F}_{q^N}$. Suppose that $\eta \in \mathbb{F}_{q^k}$ with $k \mid N$. Then $\omega^{\frac{q^N-1}{N(q-1)}(q^k-1)} = 1$, that is $N \mid \frac{q^k-1}{q-1}$; since $q \equiv 1 \pmod{N}$, this is equivalent to $N \mid k$, and hence to $N = k$. □

**Proposition 4.3.13.** *If $d = \gcd(m, p^r - 1)$ is a divisor of $r$, then there exists a linearized polynomial $L(x) \in \mathbb{F}_q[x]$ of degree $p^r$ which is good exceptional over $\mathbb{F}_q$.*

*Proof.* Let $d = \gcd(m, p^r - 1)$ and $\ell(x) \in \mathbb{F}_q[x]$ be a primitive polynomial of degree $r/d$ over $\mathbb{F}_{p^d}$, so that $\ell(x)$ is irreducible over $\mathbb{F}_{p^d}$ and has order $p^r - 1$. Let $L(x) \in \mathbb{F}_q[x]$ be the linearized $p^d$-associate of $\ell(x)$. Then, by [82, Theorem 3.63], the polynomial $L(x)/x$ is irreducible over $\mathbb{F}_{p^d}$. Let $\alpha$ be a non-zero root of $L(x)$. Then the field extension $\mathbb{F}_{p^d}(\alpha)|\mathbb{F}_{p^d}$ has degree $p^r - 1$, while the extension $\mathbb{F}_q|\mathbb{F}_{p^d}$ has degree $m/d$. The field $\mathbb{F}_q(\alpha)$ is the compositum of $\mathbb{F}_q$ and $\mathbb{F}_{p^d}(\alpha)$; since $\gcd(m/d, p^r - 1) = 1$, we have that $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = p^r - 1$. Then $L(x)/x = h_L(-x)$ is irreducible over $\mathbb{F}_q$, and the thesis follows. □

### 4.3.8 The cases $n+1=8$ and $n+1=9$

The aim of this section is to study the cases $n+1=8$ (with $p=2$) and $n+1=9$ (with $p=3$), via the algebraic curve

$$\mathcal{C}_f : \quad \frac{f(x)-f(y)}{x-y}=0 \tag{4.33}$$

of degree $n$ over $\mathbb{F}_q$ associated to a PP $f(x)$ of $\mathbb{F}_q$ of degree $n+1$. If $f(x)$ is a PP of $\mathbb{F}_q$ and $q$ is large enough with respect to $n$, then $\mathcal{C}_f$ splits into components not defined over $\mathbb{F}_q$ (see [7]). Conversely, if $\mathcal{C}_f$ has no absolutely irreducible component defined over $\mathbb{F}_q$, then $f(x)$ is exceptional over $\mathbb{F}_q$; see [26] and [94, Chapter 8.4].

$n+1=8$, $p=2$

**Proposition 4.3.14.** *Let $q=2^m$, $n+1=8$. The polynomial $f(x)=x^8+\sum_{i=1}^{7} A_i x^{7-i} \in \mathbb{F}_q[x]$ is exceptional over $\mathbb{F}_q$ if and only if $A_1=A_2=A_3=A_5=0$ and the polynomial $g(x)=x^7+A_4x^3+A_6x+A_7$ has no roots in $\mathbb{F}_q^*$. Also $f(x)$ is good exceptional if and only if $g(x)$ is irreducible over $\mathbb{F}_q$.*

*Proof.* The equation of the curve $\mathcal{C}_f$ reads

$$\begin{aligned}&(x+y)^7+A_1(x^6+x^5y+x^4y^2+x^3y^3+x^2y^4+xy^5+y^6)\\&+A_2(x^5+x^4y+x^3y^2+x^2y^3+xy^4+y^5)+A_3(x^4+x^3y+x^2y^2+xy^3+y^4)\\&+A_4(x+y)^3+A_5(x^2+xy+y^2)+A_6(x+y)+A_7=0.\end{aligned}$$

Applying $\varphi_q$ to the factors of $\mathcal{C}_f$ we conclude that, if the curve $\mathcal{C}_f$ does not have absolutely irreducible components defined over $\mathbb{F}_q$, then the curve contains either two conics and three lines or seven lines. The unique ideal point of $\mathcal{C}_f$ is $(1:1:0)$. A line $\ell$ that is a component of the curve $\mathcal{C}_f$ has equation $\ell : y=x+\alpha$ and

$$\begin{cases} A_1=0\\ A_2\alpha+A_3=0\\ A_2\alpha^3+A_5=0\\ A_3\alpha^2+A_5=0\\ \alpha^7+A_2\alpha^5+A_3\alpha^4+A_4\alpha^3+A_5\alpha^2+A_6\alpha+A_7=0.\end{cases}$$

If the line $\ell$ is not defined over $\mathbb{F}_q$ then $\alpha \in \overline{\mathbb{F}}_q \setminus \mathbb{F}_q$; this yields $A_2=A_3=A_5=0$, and the last equality becomes $\alpha^7+A_4\alpha^3+A_6\alpha+A_7=0$. It is easily seen that if $A_2=A_3=A_5=0$ then the curve $\mathcal{C}_f$ contains the seven lines $y+x+\alpha_i=0$, $i=1,\ldots,7$, where $\alpha_i^7+A_4\alpha_i^3+A_6\alpha_i+A_7=0$, and therefore $\mathcal{C}_f$ cannot split in two conics and three lines.

Thus, the only open case occurs when $\mathcal{C}_f$ splits in seven lines either not defined over $\mathbb{F}_q$ or equal to $x-y=0$. Thus $f(x)$ is exceptional if and only if $T^7+A_4T^3+A_6T+A_7$ has no roots in $\mathbb{F}_q$ and it is good exceptional if and only if $T^7+A_4T^3+A_6T+A_7$ is irreducible over $\mathbb{F}_q$. □

**Corollary 4.3.15.** *Let $q=2^m$, $n+1=8$ and suppose 3 divides $m$. The polynomial $x^8+A_7x$ is the only good exceptional polynomial over $\mathbb{F}_q$.*

*Proof.* Since 3 divides $m$ we have that $\zeta_7\in\mathbb{F}_q$. From Cyclic extensions theory, $T^7+A_4T^3+A_6T+A_7$ is irreducible over $\mathbb{F}_q$ if and only if $A_4=A_6=0$. The thesis follows from Proposition 4.3.14. □

**Remark 4.3.16.** *The exceptional polynomials of Proposition 4.3.14 are linearized, and hence described in [94, Prop. 8.4.15]. Also, Proposition 4.3.14 confirms the conjecture [94, Remark 8.4.18] for the special case $n+1=8$.*

**Corollary 4.3.17.** *Assume that $q=2^r>7^4$. The monomial $b^{-1}x^{\frac{q^8-1}{q-1}+1}$ is a CPP of $\mathbb{F}_{q^8}$ if and only if $b$ is, up to a scalar multiple in $\mathbb{F}_q^*$, a root of some $F(x)=x^7+\alpha x^3+\beta x+\gamma\in\mathbb{F}_q[x]$, irreducible over $\mathbb{F}_q$.*

$n+1=9$, $p=3$

**Proposition 4.3.18.** *Let $q=3^h$. The polynomial*

$$F(x)=x^9+A_1x^8+A_2x^7+A_3x^6+A_4x^5+A_5x^4+A_6x^3+A_7x^2+A_8x$$

*is exceptional over $\mathbb{F}_q$ if and only if one of the following cases occurs.*

*i)*

$$F(x)=x^9+A_3x^6+A_6x^3 \tag{4.34}$$

*and $T^6+A_3T^3+A_6\in\mathbb{F}_q[T]$ has no roots in $\mathbb{F}_q^*$;*

*ii)*

$$F(x)=x^9+A_6x^3+A_8x \tag{4.35}$$

*and $T^8+A_6T^2+A_8\in\mathbb{F}_q[T]$ has no roots in $\mathbb{F}_q^*$;*

*iii)*

$$\begin{aligned}F(x)=x^9+A_3x^6+A_4x^5+A_5x^4+\left(A_3^2+A_3\frac{A_5^3}{A_4^3}+\frac{A_5^2}{A_4}\right)x^3\\ +\left(2A_3A_4+2\frac{A_5^3}{A_4^2}\right)x^2+\left(2A_3A_5+A_4^2+2\frac{A_5^4}{A_4^3}\right)x,\end{aligned} \tag{4.36}$$

*where $A_4\neq 0$ and $T^4+2A_3T+2A_4\in\mathbb{F}_q[T]$ has no roots in $\mathbb{F}_q$;*

*iv)*

$$F(x) = x^9 + A_2x^7 + A_3x^6 + A_5x^4 + \left(A_2^3 + \frac{A_3A_5}{A_2}\right)x^3 + \left(2A_2A_5 + 2\frac{A_3^3}{A_2}\right)x^2 + \left(A_2^4 + A_3A_5 + \frac{A_5^2}{A_2} + \frac{A_3^4}{A_2^2}\right)x, \tag{4.37}$$

*where* $2A_2$ *is not a square in* $\mathbb{F}_q$*.*

*Proof.* • Suppose that the curve $\mathcal{C}_F$ defined in (4.33) contains a line $\ell$ with equation $\ell : y = x+\alpha$, where $\alpha = 0$ or $\alpha \notin \mathbb{F}_q$. Then, by direct computation,

$$\begin{cases} A_1 = A_2 = A_4 = 0 \\ 2\alpha^2A_3 + A_5 = 0 \\ \alpha^2A_5 + 2A_7 = 0 \\ \alpha^8A_0 + \alpha^5A_3 + \alpha^3A_5 + \alpha^2A_6 + \alpha A_7 + A_8 = 0 \end{cases}.$$

– Assume $\alpha = 0$. Then $A_5 = A_7 = A_8 = 0$. The curve becomes

$$(x-y)^2((x-y)^6 + A_3(x-y)^3 + A_6) = 0.$$

We require that the polynomial $T^6 + A_3T^3 + A_6$ has no roots in $\mathbb{F}_q^*$.

– Assume $\alpha \neq 0$. If $A_5 = 0$ then $A_3 = A_7 = 0$ and $\alpha^8 + A_6\alpha^2 + A_8 = 0$; hence, $\mathcal{C}_F$ splits in 8 lines. They are not defined over $\mathbb{F}_q$ or equal to $x - y = 0$ if and only if $T^8 + A_6T^2 + A_8 = 0$ has no roots in $\mathbb{F}_q^*$.

If $A_3 = 0$ then $A_5 = A_7 = 0$ and $\alpha^8 + A_6\alpha^2 + A_8 = 0$, as above.

Suppose now $A_3, A_5 \neq 0$. Then $A_5 = A_3\alpha^2$, $A_7 = A_5^2/A_3$, and $A_8 = 2A_5A_6/A_3 + 2A_5^4/A_3^4$. Since $\alpha^2 = A_5/A_3$, we have that $A_5/A_3$ is not a square in $\mathbb{F}_q$, otherwise the lines $y = x + \xi_1$ and $y = x + \xi_2$, where $\xi_i^2 = A_5/A_3$, are $\mathbb{F}_q$-rational lines and the polynomial $F(x)$ is not exceptional. Let $a_3, a_5 \in \mathbb{F}_{q^2}$ be such that $a_3^2 = A_3$ and $a_5^2 = A_5$. In this case,

$$\begin{aligned} \mathcal{C}_F : \quad & (a_3x - a_3y + a_5)(a_3x - a_3y - a_5)\big(a_3^6(x-y)^6 + a_3^4a_5^2(x-y)^4 \\ & +a_3^8(x+y)^3 + a_3^2a_5^4(x-y)^2 - a_3^6a_5^2(x+y) + a_3^6A_6 + a_5^6\big) = 0. \end{aligned}$$

Since the sextic is defined over $\mathbb{F}_q$, it must split either in three conics or in two cubics. In the first case it is easily seen that all of them must be fixed by $\psi$.

If a conic of equation $(x-y)^2+\alpha(x+y)+\beta = 0$ is contained in the sextic then in particular $A_3^2 = \alpha^3$ from which we get $a_3^{32}a_5^{12} = 0$, impossible.

Suppose now that the sextic splits in two cubics. If they are fixed by $\psi$ then they have equations

$$(x-y)^3+\alpha_1x^2+\alpha_2xy+\alpha_1y^2+\beta_1x+\beta_1y+\gamma_1=0,$$
$$(x-y)^3+\alpha_3x^2+\alpha_4xy+\alpha_3y^2+\beta_2x+\beta_2y+\gamma_2=0.$$

Then $\alpha_4=\alpha_3=-\alpha_1$, $\alpha_2=\alpha_1$. If $\alpha_1=0$ then $a_3^2=\gamma_1+\gamma_2$ and $a_3^2=-\gamma_1-\gamma_2$, which imply $a_3=0$, impossible. If $\alpha_1\neq 0$ then $\beta_1=\beta_2$ and again $a_3^2=\gamma_1+\gamma_2$ and $a_3^2=-\gamma_1-\gamma_2$, which imply $a_3=0$, impossible. If they are switched by $\psi$ then they have equations

$$(x-y)^3+\alpha_1x^2+\alpha_2xy+\alpha_3y^2+\beta_1x+\beta_2y+\gamma_1=0,$$
$$\lambda((y-x)^3+\alpha_3x^2+\alpha_2xy+\alpha_1y^2+\beta_2x+\beta_1y+\gamma_1)=0.$$

Then $\lambda=-a_3^6$, $\alpha_3=\alpha_1$. If $\alpha_2=-\alpha_1$, then $a_3^2\alpha_1^2+a_3^2\beta_1-a_3^2\beta_2-a_5^2=0$ and $\alpha_1=0$, which implies $a_3=0$, impossible. If $\alpha_2=\alpha_1$, then $\alpha_1(\beta_1+\beta_2)=0$. In both cases $a_3=0$, impossible.

- Suppose that $\mathcal{C}_f$ splits in four absolutely irreducible conics. There are three distinct possibilities, depending on the number of components fixed by $\psi$.

  1. All the conics are fixed by $\psi$. In this case the four conics are defined by

     $$\mathcal{C}_i:(x-y)^2+\alpha_i(x+y)+\beta_i=0, \tag{4.38}$$

     for $i=1,2,3,4$. This gives immediately $A_1=A_2=0$. The condition $A_4=0$ implies $A_5=A_7=0$ and $A_3A_8=0$, that is, the polynomial is either of type (4.34) or (4.35). Now assume $A_4\neq 0$. Then, by direct computation, $A_6=A_3^2+A_3A_5^3/A_4^3+A_5^2/A_4$, $A_7=2A_3A_4+2A_5^3/A_4^2$, $A_8=2A_3A_5+A_4^2+2A_5^4/A_4^3$; also, the $\alpha_i$'s are roots of $\ell_1(x)=x^4+2A_3x+2A_4$, and $\beta_i=\alpha_i^2+A_5/A_4\alpha_i$. On the other hand, if all these conditions are satisfied, then the curve splits in the four conics defined in (4.38). Finally, the four conics are not defined over $\mathbb{F}_q$ if and only if the polynomial $T^4+2A_3T+2A_4$ has no roots in $\mathbb{F}_q$.

  2. Two conics are fixed by $\psi$ and two are switched. We can assume

     $$\mathcal{C}_1:(x-y)^2+\alpha_1(x+y)+\beta_1=0,\quad \mathcal{C}_2:(x-y)^2+\alpha_2(x+y)+\beta_2=0,$$

     $$\mathcal{C}_3:(x-y)^2+\alpha_3x+\alpha_4y+\beta_3=0,\quad \mathcal{C}_4:(x-y)^2+\alpha_4x+\alpha_3y+\beta_3=0.$$

     By direct computation, $A_1=A_2=A_4=A_5=A_7=0$ and $A_3A_8=0$, and hence $F(x)$ is of type (4.34) or (4.35).

3. No conic is fixed by $\psi$. We can assume

   $$\mathcal{C}_1 : (x-y)^2+\alpha_1 x+\alpha_2 y+\beta_1 = 0, \quad \mathcal{C}_2 : (x-y)^2+\alpha_2 x+\alpha_1 y+\beta_1 = 0,$$

   $$\mathcal{C}_3 : (x-y)^2+\alpha_3 x+\alpha_4 y+\beta_2 = 0, \quad \mathcal{C}_4 : (x-y)^2+\alpha_4 x+\alpha_3 y+\beta_2 = 0.$$

   Also in this case we get $A_1 = A_2 = A_4 = A_5 = A_7 = 0$ and $A_3A_8 = 0$, and hence $F(x)$ is of type (4.34) or (4.35).

- Suppose that $\mathcal{C}_f$ splits in two absolutely irreducible quartics $\mathcal{Q}_1$ and $\mathcal{Q}_2$. The automorphism $\psi$ either switches or fixes the two components.

  In the former case, $\mathcal{Q}_1$ and $\mathcal{Q}_2$ have the form

  $$\mathcal{Q}_1 : (x-y)^4+\alpha_1x^3+\alpha_2x^2y+\alpha_3xy^2+\alpha_4y^3+\beta_1x^2+\beta_2xy+\beta_3y^2+\gamma_1x+\gamma_2y+\delta = 0,$$

  $$\mathcal{Q}_2 : (x-y)^4+\alpha_4x^3+\alpha_3x^2y+\alpha_2xy^2+\alpha_1y^3+\beta_3x^2+\beta_2xy+\beta_1y^2+\gamma_2x+\gamma_1y+\delta = 0.$$

  We obtain $A_1 = A_2 = A_3 = A_4 = A_5 = A_7 = 0$; hence, we have case (4.35).

  In the latter case, $\mathcal{Q}_1$ and $\mathcal{Q}_2$ have the form

  $$\mathcal{Q}_1 : (x-y)^4+\alpha_1x^3+\alpha_2x^2y+\alpha_2xy^2+\alpha_1y^3+\beta_1x^2+\beta_2xy+\beta_1y^2+\gamma_1(x+y)+\delta_1 = 0,$$

  $$\mathcal{Q}_2 : (x-y)^4+\alpha_3x^3+\alpha_4x^2y+\alpha_4xy^2+\alpha_3y^3+\beta_3x^2+\beta_4xy+\beta_3y^2+\gamma_2(x+y)+\delta_2 = 0.$$

  Since $A_1 = 0$, we obtain $A_2A_4 = 0$.

  - Assume $A_2 = 0$ and $A_4 \neq 0$. Then $A_6 = A_3^2 + A_3A_5^3/A_4^3 + A_5^2/A_4$, $A_7 = 2A_3A_4 + 2A_5^3/A_4^2$, $A_8 = 2A_3A_5 + A_4^2 + A_5^4/A_4^3$, and case (4.36) holds.
  - Assume $A_2 \neq 0$ and $A_4 = 0$. Then $A_6 = A_2^3 + A_3A_5/A_2$, $A_7 = 2A_2A_5 + 2A_3^3/A_2$, $A_8 = A_2^4 + A_3A_5 + A_5^2/A_2 + A_3^4/A_2^2$. Also, $\alpha_1^2 = 2A_2$, $\alpha_2 = \alpha_3 = -\alpha_4 = -\alpha_1$, $\beta_1 = -\beta_3 = 2A_3/\alpha_1$, $\beta_2 = -A_3/\alpha_1 - \alpha_1^2$, $\beta_4 = A_3/\alpha_1 - \alpha_1^2$, $\gamma_1 = A_3 + \alpha_1^3$, $\gamma_2 = A_3 - \alpha_1^3$, $\delta_1 = A_3\alpha_1 + A_3^2/A_2 + 2A_5\alpha_1/A_2 + 2\alpha_1^6/A_2$, $\delta_2 = -A_3\alpha_1 + A_3^2/A_2 + A_5\alpha_1/A_2 + 2\alpha_1^6/A_2$. Note that $\alpha_i, \beta_i, \gamma_i, \delta_i$ are not defined over $\mathbb{F}_q$ if and only if $2A_2$ is not a square in $\mathbb{F}_q$. The quartics $\mathcal{Q}_1$ and $\mathcal{Q}_2$ read

    $$(x-y)^4+\alpha_1x^3+2\alpha_1x^2y+2\alpha_1xy^2+\alpha_1y^3+2A_3/\alpha_1x^2+2(A_3/\alpha_1+\alpha_1^2)xy$$

    $$+2A_3/\alpha_1y^2+(A_3+\alpha_1^3)(x+y)+A_3\alpha_1+A_3^2/A_2+2A_5\alpha_1/A_2+2\alpha_1^6/A_2 = 0,$$

    $$(x-y)^4+2\alpha_1x^3+\alpha_1x^2y+\alpha_1xy^2+2\alpha_1y^3+A_3/\alpha_1x^2+(A_3/\alpha_1+2\alpha_1^2)xy$$

    $$+A_3/\alpha_1y^2+(A_3+2\alpha_1^3)(x+y)+2A_3\alpha_1+A_3^2/A_2+A_5\alpha_1/A_2+2\alpha_1^6/A_2 = 0;$$

    hence, $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are switched by $\varphi_q$.

- Finally, $A_2 = A_4 = 0$ implies $A_5 = A_7 = 0$ and $A_3A_8 = 0$. As above, this yields types (4.34) or (4.35).

□

**Remark 4.3.19.** *By direct computation, the exceptional polynomials of Proposition* 4.3.18 *are equivalent to exceptional polynomials described in* [94, Prop. 8.4.15].

*In fact, if $F(x)$ satisfies Case i) or ii), then $F(x)$ is a linearized polynomial.*

*If $F(x)$ satisfies Case iii), then $F(x) = L_1 \circ S \circ L_2(x)$, where $L_1(x)$ and $L_2(x)$ are linear, and $S(x) \in \mathbb{F}_q[x]$ has the form $x(a_2x^4 + a_1x + a_0)^2$.*

*If $F(x)$ satisfies Case iv), then $F(x) = L_1 \circ S \circ L_2(x)$, where $L_1(x)$ and $L_2(x)$ are linear, and $S(x) \in \mathbb{F}_q[x]$ has the form $S(x) = x(a_2x^4 + a_1x + a_0)^2$ when $A_2^2A_5 + A_3^3 \neq 0$, or $S(x) = x(a_2x^2 + a_0)^4$ when $A_2^2A_5 + A_3^3 = 0$.*

*This confirms the conjecture* [94, Remark 8.4.18] *for the special case $n+1 = 9$.*

**Proposition 4.3.20.** *Let $q = 3^h$. The polynomial*

$$F(x) = x^9 + A_1x^8 + A_2x^7 + A_3x^6 + A_4x^5 + A_5x^4 + A_6x^3 + A_7x^2 + A_8x$$

*is good exceptional over $\mathbb{F}_q$ if and only if one of the following cases occurs.*

*i)*

$$F(x) = x^9 + A_6x^3 + A_8x$$

*and $x^8 + A_6x^2 + A_8$ is irreducible over $\mathbb{F}_q$;*

*ii)*

$$F(x) = x^9 + A_3x^6 + A_4x^5 + A_5x^4 + \left(A_3^2 + A_3\frac{A_5^3}{A_4^3} + \frac{A_5^2}{A_4}\right)x^3 + \left(2A_3A_4 + 2\frac{A_5^3}{A_4^2}\right)x^2 + \left(2A_3A_5 + A_4^2 + 2\frac{A_5^4}{A_4^3}\right)x,$$

*where $A_4 \neq 0$ and $x^8 + 2A_3x^2 + 2A_4 \in \mathbb{F}_q[x]$ has no roots in $\mathbb{F}_{q^4}$;*

*iii)*

$$F(x) = x^9 + A_2x^7 + A_3x^6 + A_5x^4 + \left(A_2^3 + \frac{A_3A_5}{A_2}\right)x^3 + \left(2A_2A_5 + 2\frac{A_3^3}{A_2}\right)x^2 + \left(A_2^4 + A_3A_5 + \frac{A_5^2}{A_2} + \frac{A_3^4}{A_2^2}\right)x,$$

*where*

*(a) $2A_2$ is not a square in $\mathbb{F}_q$,*

*(b)* $h(-x) = (x^4 + 2\alpha x^3 + 2A_3/\alpha x^2 + 2(A_3 + 2\alpha A_2)x + A_3\alpha + A_3^2/A_2 + 2A_5\alpha/A_2 + A_2^2)(x^4 + \alpha x^3 + A_3/\alpha x^2 + 2(A_3 + \alpha A_2)x + 2A_3\alpha + A_3^2/A_2 + A_5\alpha/A_2 + A_2^2)$*, where* $\alpha^2 = 2A_2$*, is irreducible over* $\mathbb{F}_q$*.*

*Proof.* We use the classification obtained in Proposition 4.3.18.

- Let $F(x)$ be as in Case *i*) of Proposition 4.3.18. Then $A_8 = 0$; hence, $F(x)$ is not good.

- Let $F(x)$ be as in Case *ii*) of Proposition 4.3.18. Then $h_F(-x) = x^8 + A_6x^2 + A_8$; since $h_F(-x)$ cannot be a square in $\mathbb{F}_q[x]$, we have that $F(x)$ is good if and only if $h_F(-x)$ is irreducible over $\mathbb{F}_q$.

- Let $F(x)$ be as in Case *iii*) of Proposition 4.3.18. The factors of $h_F(-x)$ are $x^2 - \alpha_i x + \beta_i$, $i = 1, \ldots, 4$, where the $\alpha_i$'s are roots of $\ell_1(x) = x^4 + 2A_3x + 2A_4$ and $\beta_i = \alpha_i^2 + A_5/A_4\alpha_i$; hence, $\ell_1(x)$ must be irreducible over $\mathbb{F}_q$ in order for $F(x)$ to be good. Also, the roots of $h(-x)$ are $-\alpha_i \pm \sqrt{-A_5/A_4\alpha_i}$. Since $-A_5/A_4$ is an element of $\mathbb{F}_q$ and hence a square in $\mathbb{F}_{q^4}$, the roots of $h(-x)$ are in the same orbit under $\varphi_q$ if and only if $\alpha_i$ is not a square in $\mathbb{F}_{q^4}$, that is the polynomial $x^8 + 2A_3x^2 + 2A_4 \in \mathbb{F}_q[x]$ has no roots in $\mathbb{F}_{q^4}$.

- Let $F(x)$ be as in Case *iv*) of Proposition 4.3.18. Then $h_F(-x)$ reads

$$(x^4 + 2\alpha x^3 + 2A_3/\alpha x^2 + 2(A_3 + 2\alpha A_2)x + A_3\alpha + A_3^2/A_2 + 2A_5\alpha/A_2 + A_2^2)\cdot$$
$$\cdot(x^4 + \alpha x^3 + A_3/\alpha x^2 + 2(A_3 + \alpha A_2)x + 2A_3\alpha + A_3^2/A_2 + A_5\alpha/A_2 + A_2^2),$$

where $\alpha^2 = 2A_2$. Hence, the roots of $h_F(-x)$ are in a unique orbit under $\varphi_q$ if and only if $h_F(-x)$ is irreducible over $\mathbb{F}_q$.

□

**Remark 4.3.21.** *We give two families of good exceptional polynomials arising from Proposition* 4.3.20*. Let* $q = 3^h$ *with* $h$ *even, and* $d$ *be an odd number; by* [82, Theorem 3.75]*, the polynomial* $x^8 + 2\zeta_{q-1}^d \in \mathbb{F}_q[x]$ *is irreducible over* $\mathbb{F}_q$*. Therefore, by Case i) in Proposition* 4.3.20*, the polynomial* $F(x) = x^9 + 2\zeta_{q-1}^d x$ *is good exceptional over* $\mathbb{F}_q$*. Also, by Case ii) in Proposition* 4.3.20*, the polynomial*

$$F(x) = x^9 + \zeta_{q-1}^d x^5 + ax^4 + \frac{a^2}{\zeta_{q-1}^d}x^3 + 2\frac{a^3}{\zeta_{q-1}^{2d}}x^2 + \left(\zeta_{q-1}^{2d} + 2\frac{a^4}{\zeta_{q-1}^{3d}}\right)x$$

*is good exceptional over* $\mathbb{F}_q$*, for any* $a \in \mathbb{F}_q$*.*

**Corollary 4.3.22.** *Assume that $q = 3^r > 8^4$. The monomial $b^{-1}x^{\frac{q^8-1}{q-1}+1}$ is a CPP of $\mathbb{F}_{q^8}$ if and only if $b$ is, up to a scalar multiple in $\mathbb{F}_q^*$, a root of some $(F(-x+e)-F(e))/(-x) \in \mathbb{F}_q[x]$, where $e \in \mathbb{F}_q$ and $F(x) \in \mathbb{F}_q[x]$ satisfies Case i), ii), or iii) in Proposition* 4.3.20.

# Bibliography

[1] M. Abdón, L. Bezerra, and L. Quoos, Further examples of maximal curves, *J. Pure Appl. Algebra* **213**(6) (2009), 1192–1196.

[2] M. Abdón and L. Quoos, On the genera of subfields of the Hermitian function field, *Finite Fields Appl.* **10** (2004), 271–284.

[3] N. Anbar, A. Bassa, and P. Beelen, A characterization of Galois subfields of the generalized Giulietti-Korchmáros function field. ArXiv: 1610.00567

[4] U. Bartocci and B. Segre, Ovali ed altre curve nei piani di Galois di caratteristica 2, *Acta Arith.* **XVIII** (1971), 423–449.

[5] D. Bartoli, M. Giulietti, L. Quoos, and G. Zini, Complete permutation polynomials from exceptional polynomials, *J. Number Theory* **176** (2017), 46–66.

[6] D. Bartoli, M. Giulietti, and G. Zini, Complete $(k, 3)$-arcs from quartic curves, *Des. Codes Cryptogr.* **79**(3) (2016), 487–505.

[7] D. Bartoli, M. Giulietti, and G. Zini, On monomial complete permutation polynomials, *Finite Fields Appl.* **41**(3) (2016), 132–158.

[8] D. Bartoli, M. Montanucci, and G. Zini, Multi Point AG Codes on the GK Maximal Curve, *Des. Codes Cryptogr.*, to appear. DOI 10.1007/s10623-017-0333-9.

[9] D. Bartoli, L. Quoos, and G. Zini, Algebraic Geometric Codes on many points from Kummer extensions. Submitted. ArXiv: 1606.04143

[10] D. Bartoli, P. Speziali, and G. Zini, Complete $(k, 4)$-arcs from quintic curves. Submitted.

[11] L.A. Bassaligo and V.A. Zinoviev, On complete permutation polynomials, in: *Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory*, Proceedings, Svetlogorsk (Kaliningrad region), Russia, September 7–13 (2014), 57–62.

[12] L.A. Bassaligo and V.A. Zinoviev, On one class of permutation polynomials over finite fields of characteristic two, preprint.

[13] L.A. Bassaligo and V.A. Zinoviev, Permutation and complete permutation polynomials, *Finite Fields Appl.* **33** (2015), 198–211.

[14] M. Bhargava and M.E. Zieve, Factoring polynomials and applications to coding theory, *Finite Fields Appl.* **5** (1999), 103–111.

[15] N.L. Biggs and A.T. White, *Permmutation Groups and Combinatorial Structures*, Cambridge University Press, Cambridge (1979).

[16] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language. *J. Symbolic Comput.* **24**(3-4) (1997), 235–265.

[17] W. Burnside, *Theory of Groups of Finite Order*, Cambridge University Press, Cambridge (1897).

[18] E. Çakçak and F. Özbudak, Subfields of the function field of the Deligne-Lusztig curve of Ree type, *Acta Arith.* **115** (2004), 133–180.

[19] E. Çakçak and F. Özbudak, Number of rational places of subfields of the function field of the Deligne-Lusztig curve of Ree type, *Acta Arith.* **120** (2005), 79–106.

[20] P.J. Cameron, *Permutation Groups*, Cambridge University Press (1999).

[21] C. Carvalho and F. Torres, On Goppa codes and Weierstrass gaps at several points, *Des. Codes Cryptogr.* **35** (2005), 211–225.

[22] A.S. Castellanos and G.C. Tizziotti, Two-Point AG Codes on the GK Maximal Curves, *IEEE Trans. Inf. Theory* **62**(2) (2016), 681–686.

[23] P. Charpin and G.M. Kyureghyan, Cubic monomial bent functions: a subclass of $\mathcal{M}^*$, *SIAM J. Discrete Math.* **22**(2) (2008), 650–665.

[24] A.S. Castellanos, A.M. Masuda, and L. Quoos, One- and two-point codes over Kummer extensions, *IEEE Trans. Inform. Theory* **62**(9) (2016), 4867–4872.

[25] S.D. Cohen, Exceptional polynomials and the reducibility of substitution polynomials, *L'Ensiegnement Mathématique* **36** (1990), 53–65.

[26] S.D. Cohen, The distribution of polynomials over finite fields, *Acta Arith.* **17** (1970), 255–271.

[27] A. Cossidente, G. Korchmáros, and F. Torres, On curves covered by the Hermitian curve. *J. Algebra* **216** (1999), 56–76.

[28] A. Cossidente, G. Korchmáros, and F. Torres, Curves of large genus covered by the Hermitian curve, *Comm. Algebra* **28** (2000), 4707–4728.

[29] P. Deligne and G. Lusztig, Representations of reductive groups over finite fields, *Ann. of Math.* **103** (1976), 103–161.

[30] P. Dembowski, *Finite Geometries*, Springer, Berlin (1968).

[31] L.E. Dickson, *Linear groups with an exposition of the Galois field theory*, Teubner, Leipzig (1902).

[32] S. Dodunekov and I. Landjev, Near-MDS codes, *J. Geom.* **54** (1995), 30–43.

[33] S. Dodunekov and I. Landjev, Near-MDS codes over some small fields, *Discrete Math.* **213** (2000), 55–65.

[34] I. Duursma and K.-H. Mak, On maximal curves which are not Galois subcovers of the Hermitian curve, *Bull. Braz. Math. Soc. (N.S.)* **43**(3) (2012), 453–465.

[35] M. Enguehard, Charactérisation des groupes de Ree, *Astérisque* **142–143** (1986), 49–139.

[36] S. Fanali, On Linear Codes from Maximal Curves, *Lecture Notes in Computer Science* **5921** (2009), 91–111.

[37] S. Fanali and M. Giulietti, One-point AG codes on the GK maximal curves, *IEEE Trans. Inform. Theory* **56**(1) (2010), 202–210.

[38] S. Fanali and M. Giulietti, Quotient curves of the GK curve, *Adv. Geom.* **12** (2012), 239–268.

[39] R. Fuhrmann and F. Torres, On Weierstrass points and optimal curves, *Rend. Circ. Mat. Palermo*, Suppl. 51 (Recent Progress in Geometry, Ballico E, Korchmáros G, (Eds.)) (1998), 25–46.

[40] W. Fulton, *Algebraic Curves. An Introduction to Algebraic Geometry*, 3rd edn. Benjamin, New York (2008).

[41] A. Garcia, Curves over finite fields attaining the Hasse-Weil upper bound. In: *European Congress of Mathematics, vol. II (Barcellona)*, Progr. Math. 202, Birkhäuser, Basel (2001), 199–205.

[42] A. Garcia, On curves with many rational points over finite fields. In: *Finite Fields with Applications to Coding Theory, Cryptography and Related Areas*, Springer, Berlin (2002), 152–163.

[43] A. Garcia, C. Güneri, and H. Stichtenoth, A generalization of the Giulietti-Korchmáros maximal curve, *Adv. Geom.* **10**(3) (2010), 427–434.

[44] A. Garcia and H. Stichtenoth, Algebraic function fields over finite fields with many rational places, *IEEE Trans. Inform. Theory* **41** (1995), 1548–1563.

[45] A. Garcia and H. Stichtenoth, A maximal curve which is not a Galois subcover of the Hermitian curve, *Bull. Braz. Math. Soc. (N.S.)* **37**(1) (2006), 139–152.

[46] A. Garcia and H. Stichtenoth, Elementary Abelian $p$-extensions of algebraic function fields, *Manuscr. Math.* **72** (1991), 67–79.

[47] A. Garcia, H. Stichtenoth, and C.P. Xing, On subfields of the Hermitian function field, *Compositio Math.* **120** (2000), 137–170.

[48] M. Giulietti, On plane arcs contained in cubic curves, *Finite Fields Appl.* **8** (2002), 69–90.

[49] M. Giulietti, J.W.P. Hirschfeld, G. Korchmáros, and F. Torres, A family of curves covered by the Hermitian curve, *Sémin. Congr.* **21** (2010), 63–78.

[50] M. Giulietti and G. Korchmáros, A new family of maximal curves over a finite field, *Math. Ann.* **343** (2009), 229–245.

[51] M. Giulietti and G. Korchmáros, Automorphism groups of algebraic curves with $p$-rank zero, *J. London Math. Soc.* **81**(2) (2010), 277–296.

[52] M. Giulietti and G. Korchmáros, On automorphism groups of certain Goppa codes, *Des. Codes Cryptogr.* **48** (2008), 177–190.

[53] M. Giulietti, M., G. Korchmáros, and F. Torres, Quotient curves of the Suzuki curve, *Acta Arith.* **122**(3) (2006), 245–274.

[54] M. Giulietti, M. Montanucci, and G. Zini, On maximal curves that are not quotients of the Hermitian curve, *Finite Fields Appl.* **41** (2016), 72–88.

[55] M. Giulietti, M. Montanucci, L. Quoos, and G. Zini, On some Galois covers of the Suzuki and Ree curves. ArXiv: 1609.09343.

[56] M. Giulietti, L. Quoos, and G. Zini, Maximal curves from subcovers of the GK-curve, *J. Pure Appl. Algebra* **220**(10) (2016), 3372–3383.

[57] V.D. Goppa, *Codes on algebraic curves*, Dokl. Akad. NAUK, SSSR **259** (1981), 1289–1290.

[58] V.D. Goppa, *Algebraic-geometric codes*, Izv. Akad. NAUK, SSSR **46** (1982), 75–91.

[59] R.L. Graham, D.E. Knuth, and O. Patashnik, *Concrete Mathematics*, Addison-Wesley Publishing Company (1989).

[60] C. Güneri, M. Özdemir, and H. Stichtenoth, The automorphism group of the generalized Giulietti-Korchmáros function field, *Adv. Geom.* **13**(2) (2013), 369–380.

[61] R. Guralnick, B. Malmskog, and R. Pries, The automorphism of a family of maximal curves, *J. Algebra* **361** (2012), 92–106.

[62] R.M. Guralnick and M.E. Zieve, Polynomials with PSL(2) monodromy, *Annals of Math.* **172** (2010), 1321–1365.

[63] M. Hall, *The Theory of Groups*, Macmillan, New York (1959).

[64] P. Hall, A note on soluble groups, *J. Lond. Math. Soc.* **3** (1928), 98–105.

[65] R.W. Hartley, Determination of the ternary collineation groups whose coefficients lie in the $GF(2^n)$, *Ann. of Math. Second Series* **27**(2) (1925), 140–158.

[66] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, 2nd edn. Oxford University Press, Oxford (1998).

[67] J.W.P. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic curves over a finite field*, Princeton Univ. Press (2008).

[68] The characterization of elliptic curves over finite fields, *J. Austral. Math. Soc.* **45** (1988), 275–286.

[69] A.R. Hoffer, On unitary collineation groups, *J. Algebra* **22** (1972), 211–218.

[70] M. Homma, The Weierstrass semigroup of a pair of points on a curve, *Arch. Math.* **67**(4) (1996), 337–348.

[71] Permutation polynomials over finite fields - a survey of recent advances, *FInite Fields Appl.* **32** (2015), 82–119.

[72] D.R. Hughes and F.C. Piper, *Projective Planes*, Graduate Texts in Mathematics **6**, Springer, Berlin (1973).

[73] N.E. Hurt, *Many Rational Points: Coding Theory and Algebraic Geometry*, Mathematics and Its Applications **564**, Springer, Berlin (2003).

[74] D. Joyner and A. Ksir, Automorphism groups of some AG codes, *IEEE Trans. Inf. Theory* **52**(7) (2006), 3325–3329.

[75] W.N. Kantor, M.E. O'Nan, and G.M. Seitz, 2-transitive groups in which the stabilizer of two points is cyclic, *J. Algebra* **21** (1972), 17–50.

[76] S.J. Kim, On the index of the Weierstrass semigroup of a pair of points on a curve, *Arch. Math.* **62**(1) (1994), 73–82.

[77] G. Korchmáros and P. Speziali, Hermitian Codes with automorphism group isomorphic to $PGL(2, q)$, *Finite Fields Appl.*, to appear.

[78] G. Korchmáros and F. Torres, Embedding of a Maximal Curve in a Hermitian Variety, *Compositio Math.* **128** (2001), 95–113.

[79] G. Lachaud, Sommes dEisenstein et nombre de points de certaines courbes algbriques sur les corps finis, *C.R. Acad. Sci. Paris* **305** (1987), 729-732.

[80] S. Lang, *Algebra*, Addison-Wesley Publishing Company (1970).

[81] V.M. Levchuk and Y.N. Nuzhin, The structure of Ree groups, *Algebra Logic* **24** (1985), 16–26.

[82] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, Cambridge (1986).

[83] L. Lombardo-Radice, Sul problema dei $k$-archi completi in $S_{2,q}$ ($q = p^t$, $p$ primo dispari), *Boll. Unione Mat. Ital.* **3**(11) (1956), 178–181.

[84] J. Ma, T. Zhang, T. Feng, and G. Ge, New results on permutation polynomials over finite fields. ArXiv: 1506.05525

[85] I.D. Macdonald, *The Theory of Groups*, Oxford University Press, Oxford (1968).

[86] G.L. Matthews, The Weierstrass semigroup of an $m$-tuple of collinear points on a Hermitian curve, in: *Finite fields and applications*, Lecture Notes in Comput. Sci., vol. 2948, Springer, Berlin (2004), 12–24.

[87] G.L. Matthews, Codes from the Suzuki function field, *IEEE Trans. Inf. Theory* **50**(12) (2004) 3298–3302.

[88] G.L. Matthews, Weierstrass Pairs and Minimum Distance of Goppa Codes, *Des. Codes Cryptogr.* **22** (2001), 107–121.

[89] MinT, *Tables of optimal parameters for linear codes*, Univ. Salzburg, Salzburg, Austria, 2009 [Online]. Available: http://mint.sbg.ac.at.

[90] H.H. Mitchell, Determination of the ordinary and modular ternary linear groups, *Trans. Amer. Math. Soc.* **12**(2) (1911), 207–242.

[91] V.S. Monakhov, Normal subgroups of biprimary groups, *Mat. Zametki* **18**(6) (1975), 877–886.

[92] M. Montanucci and G. Zini, Some Ree and Suzuki curves are not quotients of the Hermitian curve. Submitted. ArXiv: 1511.05353

[93] G.L. Mullen and Q. Wang, Permutation polynomials: one variable, in: G.L. Mullen and D. Panario (Eds.), *Handbook of Finite Fields*, Chapman and Hall/CRC (2013).

[94] G.L. Mullen and D. Panario, *Handbook of finite fields*, Chapman and Hall (2013).

[95] A. Muratovic-Ribic and E. Pasalic, A note on complete polynomials over finite fields and their applications in cryptography, *Finite Fields Appl.* **25** (2014), 306–315.

[96] P.M. Neumann, G.A. Stoy, and E.C. Thompson, *Groups and Geometry*, Oxford University Press, Oxford (1994).

[97] H. Niederreiter and K.H. Robinson, Complete mappings of finite fields, *J. Aust. Math. Soc. Ser. A* **33** (1982), 197–212.

[98] O. Pretzel, *Codes and Algebraic Curves*, Oxford Lecture Series in Mathematics and its Applications **8**, The Clarendon Press, Oxford University Press, New York (1998).

[99] R. Ree, A family of simple groups associated with the simple Lie algebra of type $(G_2)$, *Amer. J. Math.* **83** (1961), 432–462.

[100] H.E. Rose, *A Course on Finite Groups*, Springer Science and Business Media, London (2009).

[101] H.-G. Rück and H. Stichtenoth, A characterization of the Hermitian function fields over finite fields, *J. Reine Angew. Math.* **457** (1994), 185–188.

[102] S. Sarkar, S. Bhattacharya, and A. Cesmelioglu, On some permutation binomials of the form $x^{(2^h-1)/k+1} + ax$ over $\mathbb{F}_{2^k}$: existence and count, in: *International Workshop on the Arithmetic of Finite Fields WAIFI 2012*, in: Lect. Notes Comput. Sci., vol. 7369, Springer (2012), 236–246.

[103] B. Segre, Ovali e curve $\sigma$ nei piani di Galois di caratteristica due, *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat.* **32**(8) (1962), 785–790.

[104] S. Singh and Q. Zameeruddin, *Modern Algebra*, 8th edn. Vikas Publishing House, New Delhi (2006).

[105] D. Skabelund, New maximal curves as Ray Class Fields over Deligne-Lusztig curves. ArXiv: 1605.05428v2

[106] P. Stanica, S. Gangopadhyay, A. Chaturvedi, A.K. Gangopadhyay, and S. Maitra, Investigation on bent and negabent functions via the nega-Hadamard transform, *IEEE Trans. Inf. Theory* **58**(6) (2012), 4064–4072.

[107] H. Stichtenoth, *Algebraic function fields and codes*, 2nd edn. Graduate Texts in Mathematics, vol. 254, Springer, Berlin (2009).

[108] M. Suzuki, A new type of simple groups of finite order, *Proc. Nat. Acad. Sci. U.S.A.* **46** (1960), 868–870.

[109] M. Suzuki, On a class of doubly transitive groups, *Ann. of Math.* **75** (1962), 105–145.

[110] S. Tafazolian, A. Teheran-Herrera, and F. Torres, Further examples of maximal curves which cannot be covered by the Hermitian curve, *J. Pure Appl. Algebra* **220**(3) (2016), 1122–1132.

[111] J. Tits, Ovoides et groupes de Suzuki, *Arch. Math.* **13** (1962), 187–198.

[112] J. Tits, Les groupes simples de Suzuki et de Ree, *Séminaire Bourbaki* **6**, Soc. Math. France, Paris (1995), 65–82.

[113] M.A. Tsfasman and S.G. Vladut, *Algebraic-Geometric Codes*, Kluwer, Amsterdam (1991).

[114] Z. Tu, X. Zeng, and L. Hu, Several classes of complete permutation polynomials, *Finite Fields Appl.* **25** (2014), 182–193.

[115] G. van der Geer, Curves over finite fields and codes. In: *European Congress of Mathematics, vol. II (Barcellona)*, Progr. Math. 202, Birkhäuser, Basel (2001), 225–238.

[116] G. van der Geer, Coding theory and algebraic curves over finite fields: a survey and questions. In *Applications of Algebraic Geometry to Coding Theory, Physics and Computation*, NATO Sci. Ser. II Math. Phys. Chem. 36, Kluwer, Dordrecht (2001), 139–159.

[117] J.H. van Lint, *Introduction to Coding Theory*, Graduate Texts in Mathematics, vol. 86, Springer, Berlin (1982).

[118] O. Veblen and J.W. Young, *Projective Geometry*, The Atheneum Press, Boston (1910).

[119] G. Wu, N. Li, T. Helleseth, and Y. Zhang, More classes of Complete Permutation Polynomials over $\mathbb{F}_q$. ArXiv: 1312.4716

[120] G. Wu, N. Li, T. Helleseth, and Y. Zhang, Some classes of monomial complete permutation polynomials over finite fields of characteristic two, *Finite Fields Appl.* **28** (2014), 148–165.

[121] G. Wu, N. Li, T. Helleseth, and Y. Zhang, Some classes of complete permutation polynomials over $\mathbb{F}_q$, *Sci. China Math.* **58**(10) (2015), 2081–2094.

[122] H. Zassenhaus, Über endliche Fastkörper, *Abh. Math. Semin. Univ. Hamb.* **11** (1936), 132–145.

[123] M. Zieve, Bivariate factorizations via Galois theory, with application to exceptional polynomials, *J. Algebra* **210** (1998), 670–689.