J. Geom. 108 (2017), 985–1011

0047-2468/17/030985-27
published online June 3, 2017
DOI 10.1007/s00022-017-0390-2

Journal of Geometry

Complete $(k, 4)$-arcs from quintic curves

Daniele Bartoli, Pietro Speziali, and Giovanni Zini

Abstract. Complete $(k, 4)$-arcs in projective Galois planes are the geometric counterpart of linear non-extendible codes of length k, dimension 3 and Singleton defect 2. A class of infinite families of complete $(k, 4)$-arcs in $\mathrm{PG}(2, q)$ is constructed, for q a power of an odd prime $p \equiv 3 \pmod 4$, $p > 3$. The order of magnitude of k is smaller than q. This property significantly distinguishes the complete $(k, 4)$-arcs of this paper from the previously known infinite families, whose size exceeds $q - 6\sqrt{q}$.

Mathematics Subject Classification. 51E21.

Keywords. $(k$, 4)-arcs, Quintic curves, Hasse-Weil bound.

1. Introduction

A (k, s)-arc in $\mathrm{PG}(2, q)$, the projective Galois plane over the finite field $\mathbb{F}_q$ with q elements, is a set of k points no $(s + 1)$ of which are collinear and such that there exist s collinear points. A general introduction to (k, s)-arcs can be found in the monograph [10, Chapt. 12], as well as in the survey paper [13, Sect. 5]. A natural problem in this context is the construction of infinite families of *complete* (k, s)-arcs, that is, arcs that are maximal with respect to set theoretical inclusion. From the standpoint of Coding Theory, complete (k, s)-arcs correspond to linear $[k, 3, k - s]_q$-codes which cannot be extended to a code with the same minimum distance.

In the case $s = 2$, the theory is well developed and quite rich of constructions; see e.g. [1–3, 9, 12, 13, 18, 19] and the references therein, as well as [10, Chapt. 8-10]. On the other hand, for most $s > 2$, the only known infinite families either consist of the set of $\mathbb{F}_q$-rational points of some irreducible curve of degree s (see [7, 14, 20] for $s = 3$, as well as [6] for $s > 3$), or arise from the theory of 2-character sets in $\mathrm{PG}(2, q)$ (see Sects. 12.2 and 12.3 in [10], as well as the more recent work [8]). For $s = 3$ smaller complete $(k, 3)$-arcs have been recently constructed in [4]; they consist of a subset of $\mathbb{F}_q$-rational points of a curve of degree 4.

In this paper 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 1.1. *Let σ 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 σ with $q\geq 580644\sigma^8$, there exists a complete $(k,4)$-arc in $\mathrm{PG}(2,q)$ of size

$$k\leq\frac{\tau(\sigma)}{\sigma}q+8.$$

A lower bound for the minimum size of a complete $(k,4)$-arc in $\mathrm{PG}(2,q)$ is $\sqrt{12(q+1)}$; see [11]. The order of magnitude of the $(k,4)$-arcs constructed in Theorem 1.1 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.

On the other hand, the size of the arcs of Theorem 1.1 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 $q^{25/27}$.

The points of the $(k,4)$-arcs constructed in this paper belong, with at most 8 exceptions, to the set of $\mathbb{F}_q$-rational points of the quintic curve $\mathcal{Q}$ with equation $Y=X^5$. It should be noted that for this reason they share at most 28 points with an irreducible quartic. The proof of their completeness is based on a classical idea going back to Segre [16] and Lombardo-Radice [15]. In order to show that the 4-secants of the $(k,4)$-arc cover a point P off the quintic curve $\mathcal{Q}$, we construct an algebraic curve $\mathcal{H}_P$ defined over $\mathbb{F}_q$ describing the collinearity of four points of the arc and P, and then prove that $\mathcal{H}_P$ has an absolutely irreducible component defined over $\mathbb{F}_q$; the Hasse–Weil bound guarantees the existence of a suitable $\mathbb{F}_q$-rational point in $\mathcal{H}_P$. Finally we deduce that P is collinear with four points in the arc. The main difficulty here is that $\mathcal{H}_P$ is not a plane curve, but a curve embedded in the 4-dimensional space; see Eq. (6). This is why the theory and the language of Function Fields have been used in order to show that $\mathcal{H}_P$ possesses an absolutely irreducible component defined over $\mathbb{F}_q$.

The paper is organized as follows. In Sect. 2 we summarize the notions and the results from the theory of Function Fields that will be used in the paper. In Sect.3 we show how it is possible to construct complete $(k,4)$-arcs from quartic curves, with $k\geq q-6\sqrt{q}+1$. In Sect. 4, we construct a $(q/\sigma,4)$-arc $\mathcal{K}_e$ lying on $\mathcal{Q}$; it is associated to an additive subgroup M with index σ in $\mathbb{F}_q$. We show in Sect. 5 that under the conditions of Theorem 1.1, the 4-secants of $\mathcal{K}_e$ covers almost all points of $\mathrm{PG}(2,q)\backslash\mathcal{Q}$. 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 Sect. 6. This allows us to show in Sect. 7 how to cover the points of $\mathcal{Q}$, for q large enough, by joining more copies of $\mathcal{K}_e$.

2. Preliminaries from Function Field theory

We recall that a *function field* over a perfect field $\mathbb{L}$ is an extension $\mathbb{F}$ of $\mathbb{L}$ such that $\mathbb{F}$ is a finite algebraic extension of $\mathbb{L}(\alpha)$, with α transcendental over $\mathbb{L}$. For basic definitions on function fields we refer to [17]. In particular, the (full) constant field of $\mathbb{F}$ is the set of elements of $\mathbb{F}$ that are algebraic over $\mathbb{L}$.

If $\mathbb{F}'$ is a finite extension of $\mathbb{F}$, then a place P' of $\mathbb{F}'$ is said to be *lying over* a place P of $\mathbb{F}$ if $P \subset P'$. This holds precisely when $P = P' \cap \mathbb{F}$. In this paper, $e(P'|P)$ will denote the ramification index of P' over P. A finite extension $\mathbb{F}'$ of a function field $\mathbb{F}$ is said to be *unramified* if $e(P'|P) = 1$ for every P' place of $\mathbb{F}'$ and every P place of $\mathbb{F}$ with P' lying over P. Throughout the paper, we will refer to the following results.

Theorem 2.1 [17, Cor. 3.7.4]. *Consider an algebraic function field $\mathbb{F}$ with constant field $\mathbb{L}$ containing a primitive n-th root of unity ($n > 1$ and n relatively prime to the characteristic of $\mathbb{L}$). Let $u \in \mathbb{F}$ be such that there is a place Q of $\mathbb{F}$ with $\gcd(v_Q(u), n) = 1$. Let $\mathbb{F}' = \mathbb{F}(y)$ with $y^n = u$. Then*

1. *$\Phi(T) = T^n - u$ is the minimal polynomial of y over $\mathbb{F}$. The extension $\mathbb{F}' : \mathbb{F}$ is Galois of degree n and the Galois group of $\mathbb{F}' : \mathbb{F}$ is cyclic;*
2. $$e(P'|P) = \frac{n}{r_P} \quad \text{where} \quad r_P := GCD(n, v_P(u)) > 0\,;$$
3. *$\mathbb{L}$ is the constant field of $\mathbb{F}'$;*
4. *let g' (resp. g) be the genus of $\mathbb{F}'$ (resp. $\mathbb{F}$), then*
$$g' = 1 + n(g-1) + \frac{1}{2}\sum_{P\in\mathbb{P}(\mathbb{F})}(n - r_P)\deg P.$$

Theorem 2.2 [17, Th. 3.7.10]. *Consider an algebraic function field $\mathbb{F}$ with constant field $\mathbb{L}$ of characteristic $p > 0$, and an additive separable polynomials $a(T) \in \mathbb{L}[T]$ of degree p^n with all its roots in $\mathbb{L}$. Let $u \in \mathbb{F}$. Suppose that for each place P of $\mathbb{F}$ there is an element $z \in \mathbb{F}$ (depending on P) such that either*

$$v_P(u - a(z)) \geq 0$$

or

$$v_P(u - a(z)) = -m \text{ with } m > 0 \text{ and } p \not| m.$$

Define $m_P := -1$ in the former case and $m_p := m$ in the latter case. Let $\mathbb{F}' = \mathbb{F}(y)$ be the extension with $a(y) = u$. If there exists at least one place Q such that $m_Q > 0$, then

1. *the extension $\mathbb{F}' : \mathbb{F}$ is Galois of degree p^n and the Galois group of $\mathbb{F}' : \mathbb{F}$ is isomorphic to the additive group $\{\alpha \in \mathbb{L} : a(\alpha) = 0\}$;*

2. $\mathbb{L}$ is the constant field of $\mathbb{F}'$;
3. each place P in F with $m_P = -1$ is unramified in $\mathbb{F}' : \mathbb{F}$;
4. each place P in F with $m_P > 0$ is totally ramified in $\mathbb{F}' : \mathbb{F}$;
5. let g' (resp. g) be the genus of $\mathbb{F}'$ (resp. $\mathbb{F}$), then

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

An extension such as $\mathbb{F}'$ in Theorem 2.1 or 2.2 is said to be a Kummer extension or a generalized Artin–Schreier extension of $\mathbb{F}$, respectively.

Denote by $\mathbb{F}_q$ the finite field with q elements and let $\mathbb{K}$ be the algebraic closure of $\mathbb{F}_q$. A curve $\mathcal{C}$ in some affine or projective space over $\mathbb{K}$ is said to be defined over $\mathbb{F}_q$ if the ideal of $\mathcal{C}$ is generated by polynomials with coefficients in $\mathbb{F}_q$. Let $\mathbb{K}(\mathcal{C})$ denote the function field of $\mathcal{C}$. The subfield $\mathbb{F}_q(\mathcal{C})$ of $\mathbb{K}(\mathcal{C})$ consists of the rational functions on $\mathcal{C}$ defined over $\mathbb{F}_q$. The extension $\mathbb{K}(\mathcal{C}) : \mathbb{F}_q(\mathcal{C})$ is a constant field extension (see [17, Sect. 3.6]). In particular, $\mathbb{F}_q$-rational places of $\mathbb{F}_q(\mathcal{C})$ can be viewed as the restrictions to $\mathbb{F}_q(\mathcal{C})$ of places of $\mathbb{K}(\mathcal{C})$ that are fixed by the Frobenius map on $\mathbb{K}(\mathcal{C})$. The center of an $\mathbb{F}_q$-rational place is an $\mathbb{F}_q$-rational point of $\mathcal{C}$; conversely, if P is a simple $\mathbb{F}_q$-rational point of $\mathcal{C}$, then the only place centered at P is $\mathbb{F}_q$-rational.

We now recall the well-known Hasse–Weil bound.

Theorem 2.3 (Hasse–Weil bound, [17, Theorem 5.2.3]). *The number N_q of $\mathbb{F}_q$-rational places of a function field $\mathbb{F}$ with constant field $\mathbb{F}_q$ and genus g satisfies*

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

In order to apply the Hasse–Weil bound, the following lemma will be useful.

Lemma 2.4. *Let $F = \mathbb{F}_q(\beta_1, \ldots, \beta_n)$ be a function field with constant field $\mathbb{F}_q$. Suppose that $f \in \mathbb{F}[T]$ is a polynomial which is irreducible over $\mathbb{K}(\beta_1, \ldots, \beta_n)$ $[T]$. Then, for a root z of f, the field $\mathbb{F}_q$ is the constant field of $\mathbb{F}_q(\beta_1, \ldots, \beta_n)(z)$.*

Proof. Let $\mathbb{F}_{q'}$ be the constant field of $\mathbb{F}_q(\beta_1, \ldots, \beta_n)(z)$. Then

$$\mathbb{F}_q(\beta_1, \ldots, \beta_n) \subseteq \mathbb{F}_{q'}(\beta_1, \ldots, \beta_n) \subseteq \mathbb{F}_{q'}(\beta_1, \ldots, \beta_n)(z) = \mathbb{F}_q(\beta_1, \ldots, \beta_n)(z).$$

Clearly f is irreducible over $\mathbb{F}_{q'}(\beta_1, \ldots, \beta_n)$; then $[\mathbb{F}_{q'}(\beta_1, \ldots, \beta_n)(z) : \mathbb{F}_{q'}(\beta_1, \ldots, \beta_n)] = \deg(f) = [\mathbb{F}_q(\beta_1, \ldots, \beta_n)(z) : \mathbb{F}_q(\beta_1, \ldots, \beta_n)]$, and hence $[\mathbb{F}_{q'}(\beta_1, \ldots, \beta_n) : \mathbb{F}_q(\beta_1, \ldots, \beta_n)] = 1$. This implies $\mathbb{F}_{q'} = \mathbb{F}_q$. □

3. $(k, 4)$-arcs from quartic curves

An absolutely irreducible quartic curve is always a $(k, 4)$-arc. By the Hasse–Weil bound the size of such arc 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.

Throughout this section, q is a power of a prime $p > 3$, and $\mathcal{C} = \{(x, x^4) \mid x \in \mathbb{F}_q\}$ is the set of the $\mathbb{F}_q$-rational affine points of the plane curve with equation $Y = X^4$.

The following proposition shows the collinearity conditions of four points of $\mathcal{C}$ and one point of $\mathrm{AG}(2, q)\backslash\mathcal{C}$.

Proposition 3.1 [4, Propositions 2 and 4]. *Four distinct points $A = (u, u^4)$, $B = (v, v^4)$, $C = (w, w^4)$, $D = (t, t^4)$ of $\mathcal{C}$ and $P = (a, b) \in \mathrm{AG}(2, q)\backslash\mathcal{C}$ are collinear if and only if*

$$\begin{cases} u + v + w + t = 0 \\ w^2 + (u + v)w + u^2 + uv + v^2 = 0 \\ a(u^2 + v^2)(u + v) - uv(u^2 + uv + v^2) - b = 0 \end{cases} . \tag{1}$$

Proposition 3.2. *Let $a, b \in \mathbb{F}_q$ with $b \neq a^4$. The equation $\ell_1(u, v) = 0$, where*

$$\ell_1(u, v) = a(u^2 + v^2)(u + v) - uv(u^2 + uv + v^2) - b, \tag{2}$$

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 ℓ_1 as in (2). If $b = 0$ then $(0, 0, 1)$ is an ordinary triple point and no lines through it 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 therefore irreducible and of genus 3.

Since E_1 is the function field $\mathbb{F}_q(\mathcal{E}_1)$ of $\mathcal{E}_1$, the thesis follows. □

Proposition 3.3. *Let $a, b \in \mathbb{F}_q$ with $b \neq a^4$. The equation*

$$w^2 + (u + v)w + u^2 + uv + v^2 = 0 \tag{3}$$

defines an extension $E_2 = E_1(w)$ with genus at most 9 whose field of constants 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 α_1, α_2 are the two distinct solutions of $3T^2 + 2T + 3 = 0$. By 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 $\overline{\mathbb{F}}_q[V]$. Then ψ^2 has at least one zero in $\overline{\mathbb{F}}_q(u, v)$ with odd multiplicity, and hence ψ^2 is not a square in $\overline{\mathbb{F}}_q(u, v)$. Therefore, by Theorem 2.1, $\overline{\mathbb{F}}_q(u, v, w) : \overline{\mathbb{F}}_q(u, v)$ is a Galois extension of degree 2; by Lemma 2.4, $\mathbb{F}_q$ is the field of constants of $E_2 = \mathbb{F}_q(u, v, w)$. Since ψ^2 has at most 8 zeros in $\overline{\mathbb{F}}_q(u, v)$ 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 3.4. *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 $\overline{\mathbb{F}}_q(u,v,w,t) = \overline{\mathbb{F}}_q(u,v,w)$. The poles lie over the four unramified places of $\overline{\mathbb{F}}_q(u,v)$ centered at the ideal points of $\mathcal{E}_1$. Since $[\overline{\mathbb{F}}_q(u,v,w,t) : \overline{\mathbb{F}}_q(u,v)] = 2$, the number of poles of $u-v$, $u-w$, $u-t$, $v-w$, $v-t$, and $w-t$ in $\overline{\mathbb{F}}_q(u,v,w,t)$ is 8. Since the zero divisor and the pole divisor of $u-v$ have the same degree [17, Th. 1.4.11], the number of zeros of $u-v$ in $\overline{\mathbb{F}}_q(u,v,w,t)$ 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 $\big(u(Q), u(Q)^4\big)$, $\big(v(Q), v(Q)^4\big)$, $\big(w(Q), w(Q)^4\big)$, $\big(t(Q), t(Q)^4\big)$ of $\mathcal{C}$. By Theorem 2.3,

$$N_q \geq q+1-2g(E_3)\sqrt{q} \geq q+1-18\sqrt{q}.$$

The hypothesis $q \geq 431$ implies $N_q > 56$.

We proved that $\mathcal{C}$ is a $(q,4)$-arc which covers all the points of $\mathrm{PG}(2,q)$, except at most the ideal line.

Consider now an ideal point $(1,a,0)$, with $a \neq 0$. This point 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

$$\begin{cases} u+v+w+t=0 \\ w^2+(u+v)w+u^2+uv+v^2=0 \\ u^3+u^2v+uv^2+v^3=a \end{cases}.$$

Arguing as above we can easily prove that for each $a \in \mathbb{F}_q^*$, $q \geq 431$, the previous conditions are satisfied and therefore the point $(1,a,0)$ is covered by $\mathcal{C}$. Also, the points $(0,1,0)$ and $(1,0,0)$ are not collinear with four distinct points of $\mathcal{C}$. This shows that there exists a complete $(k,4)$-arc in $\mathrm{PG}(2,q)$ of size $q+2$ containing $\mathcal{C}$. □

4. $(k,4)$-arcs from quintic curves

Throughout the rest of paper, p is an odd prime with $p > 5$ and $p \equiv 3 \pmod 4$, $\sigma = p^{h'}$ with h' odd, $q = p^h$ with $h > h'$, $h' \mid h$, and $\mathbb{K} = \overline{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$.

Let

$$\mathcal{Q} = \{(x, x^5) \mid x \in \mathbb{F}_q\}$$

be the set of the $\mathbb{F}_q$-rational affine points of the plane curve with equation $Y = X^5$. The following propositions show the collinearity condition of three and four points on the quartic $\mathcal{Q}$.

Proposition 4.1. *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. *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 4.1, 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. □

Next we construct a $(k,4)$-arc contained in $\mathcal{Q}$ from a coset of an additive subgroup of $\mathbb{F}_q$. Let

$$M := \{(a^\sigma - a) \mid a\in\mathbb{F}_q\}, \tag{4}$$

and

$$\mathcal{K}_e := \{(v,v^5) \mid v\in M+e\}, \tag{5}$$

with $e\notin M$.

Proposition 4.3. *No five points of $\mathcal{K}_e$ are collinear.*

Proof. By Proposition 4.2, if five distinct points $(a_i+e,(a_i+e)^5)$, $a_i\in M$, $i=1,\dots,5$, are collinear then

$$a_1+e+a_2+e+a_3+e+a_4+e+a_5+e=0, \quad \text{hence}$$
$$-5e=a_1+a_2+a_3+a_4+a_5\in M.$$

Since $p\neq 5$ and M is closed under addition by elements of $\mathbb{F}_\sigma$, then $e\in M$, a contradiction. □

5. 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 we can prove the following.

Proposition 5.1. *Four distinct points $A=(u,u^5)$, $B=(v,v^5)$, $C=(w,w^5)$, $C=(t,t^5)$ 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

$$\det\begin{pmatrix} u & u^5 & 1\\ v & v^5 & 1\\ a & b & 1\end{pmatrix}=(v-u)\left[b+uv(u^2+v^2)(u+v)\right.$$
$$\left.-a(u^4+u^3v+u^2v^2+uv^3+v^4)\right].$$

□

In particular, if the points of $\mathcal{Q}$ have the form $A=(u+e,(u+e)^5)$, $B=(v+e,(v+e)^5)$, $C=(w+e,(w+e)^5)$, $D=(t+e,(t+e)^5)$, then the conditions in Proposition 5.1 read

$$\begin{cases} w^3+w^2(u+v+5e)+w\left[u^2+uv+v^2+5e(u+v)+10e^2\right]\\ +(u+v)(u^2+v^2)+5e(u^2+uv+v^2)+9e^2(u+v)+7e^3=0\\ \\ t^2+t(u+v+w+5e)+u^2+v^2+w^2+uv+uw+vw\\ +e\left[3(u+v+w)+2(uv+uw+vw)\right]+10e^2=0\\ \\ b+(u+e)(v+e)(u+v+2e)\left[u^2+v^2+2e(u+v)+e^2\right]\\ \quad -a\left[u^4+u^3v+u^2v^2+uv^3+v^4+5e(u+v)(u^2+v^2)\right.\\ \quad \left.+10e^2(u^2+uv+v^2)+9e^3(u+v)+4e^4\right]=0 \end{cases}.$$

Therefore, the following result holds.

Corollary 5.2. *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*

$$\mathcal{H}_P : \begin{cases} (Z^\sigma - Z)^3 + (Z^\sigma - Z)^2(X^\sigma - X + Y^\sigma - Y + 5e) \\ + (Z^\sigma - Z)\left[(X^\sigma - X)^2 + (X^\sigma - X)(Y^\sigma - Y) + (Y^\sigma - Y)^2 + 5e(X^\sigma - X + Y^\sigma - Y) + 10e^2\right] \\ + (X^\sigma - X + Y^\sigma - Y)\left[(X^\sigma - X)^2 + (Y^\sigma - Y)^2\right] \\ + 5e\left[(X^\sigma - X)^2 + (X^\sigma - X)(Y^\sigma - Y) + (Y^\sigma - Y)^2\right] + 9e^2(X^\sigma - X + Y^\sigma - Y) + 7e^3 = 0 \\ \\ (R^\sigma - R)^2 + (R^\sigma - R)(X^\sigma - X + Y^\sigma - Y + Z^\sigma - Z + 5e) + (X^\sigma - X)^2 + (Y^\sigma - Y)^2 \\ +(Z^\sigma - Z)^2 + (X^\sigma - X)(Y^\sigma - Y) + (X^\sigma - X)(Z^\sigma - Z) + (Y^\sigma - Y)(Z^\sigma - Z) \\ + e\big[3(X^\sigma - X + Y^\sigma - Y + Z^\sigma - Z) \\ + 2((X^\sigma - X)(Y^\sigma - Y) + (X^\sigma - X)(Z^\sigma - Z) + (Y^\sigma - Y)(Z^\sigma - Z))\big] + 10e^2 = 0 \\ \\ b + (X^\sigma - X + e)(Y^\sigma - Y + e)(X^\sigma - X + Y^\sigma - Y + 2e) \\ \quad \cdot\left[(X^\sigma - X)^2 + (Y^\sigma - Y)^2 + 2e(X^\sigma - X + Y^\sigma - Y) + e^2\right] \\ - a\Big[(X^\sigma - X)^4 + (X^\sigma - X)^3(Y^\sigma - Y) + (X^\sigma - X)^2(Y^\sigma - Y)^2 + (X^\sigma - X)(Y^\sigma - Y)^3 \\ + (Y^\sigma - Y)^4 + 5e(X^\sigma - X + Y^\sigma - Y)\left[(X^\sigma - X)^2 + (Y^\sigma - Y)^2\right] \\ + 10e^2((X^\sigma - X)^2 + (X^\sigma - X)(Y^\sigma - Y) + (Y^\sigma - Y)^2) + 9e^3(X^\sigma - X + Y^\sigma - Y) + 4e^4\Big] = 0 \end{cases} . \tag{6}$$

Consider the following sequence of function fields:

$$F_7 = F_6(r) : r^\sigma - r = t$$

$$\Big| \ \sigma$$

$$F_6 = F_5(t) : \begin{array}{l} t^2 + t(x^\sigma - x + y^\sigma - y + z^\sigma - z + 5e) + (x^\sigma - x)^2 + (y^\sigma - y)^2 \\ +(z^\sigma - z)^2 \\ +(x^\sigma - x)(y^\sigma - y) + (x^\sigma - x)(z^\sigma - z) + (y^\sigma - y)(z^\sigma - z) \\ + e\big[3(x^\sigma - x + y^\sigma - y + z^\sigma - z) \\ \quad + 2((x^\sigma - x)(y^\sigma - y) + (x^\sigma - x)(z^\sigma - z) + (y^\sigma - y)(z^\sigma - z))\big] \\ +10e^2 = 0 \end{array}$$

$$\Big| \ 2$$

$$F_5 = F_4(z) : z^\sigma - z = w$$

$$\Big| \ \sigma$$

$$F_4 = F_3(w) : \begin{array}{l} w^3 + w^2(x^\sigma - x + y^\sigma - y + 5e) \\ + w\left[(x^\sigma - x)^2 + (x^\sigma - x)(y^\sigma - y) + (y^\sigma - y)^2 + 5e(x^\sigma - x + y^\sigma - y) \right. \\ \left. +10e^2\right] \\ + (x^\sigma - x + y^\sigma - y)((x^\sigma - x)^2 + (y^\sigma - y)^2) \\ + 5e((x^\sigma - x)^2 + (x^\sigma - x)(y^\sigma - y) + (y^\sigma - y)^2) + 9e^2(x^\sigma - x + y^\sigma - y) \\ +7e^3 = 0 \end{array}$$

$$\Big| \ 3$$

$$F_3 = F_2(y) : y^\sigma - y = v$$

$$\Big| \ \sigma$$

$$F_2 = F_1(x) : x^\sigma - x = u$$

$$\Big| \ \sigma$$

$$F_1 = \mathbb{F}_q(u, v) : \begin{array}{l} b + (u + e)(v + e)(u + v + 2e)\left[u^2 + v^2 + 2e(u + v) + e^2\right] \\ - a\big[u^4 + u^3 v + u^2 v^2 + u v^3 + v^4 + 5e(u + v)(u^2 + v^2) \\ \quad + 10e^2(u^2 + uv + v^2) + 9e^3(u + v) + 4e^4\big] = 0 \end{array}$$

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 σ, then F_7 has a large number of $\mathbb{F}_q$-rational places. By the equations defining F_7, 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 6 whose field of constants is $\mathbb{F}_q$. Equivalently, the plane 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 5.3. *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 $R_1^i=(1,\xi^i,0)$, $i=1,2,3$, with ξ a primitive 4-th root of unity; being distinct, they are simple points. We have

$$\partial_U G_1(U,V) = (V-(a-e))$$
$$\left(4(U+e)^3+3(U+e)^2(V+e)+2(U+e)(V+e)^2+(V+e)^3\right),$$
$$\partial_V G_1(U,V) = (U-(a-e))$$
$$\left((U+e)^3+2(U+e)^2(V+e)+3(U+e)(V+e)^2+4(V+e)^3\right).$$

Since $b\neq a^5$, no points $(U,V)\in\mathcal{H}_1$ have either $U=a-e$ or $V=a-e$. Also, the resultant of $\partial_U G_1(U,V)/\left(V-(a-e)\right)$ and $\partial_V G_1(U,V)/\left(U-(a-e)\right)$ 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 $(U,V)=(-e,-e)$, which is not a point of $\mathcal{H}_1$ as $b\neq 0$. Therefore, $\mathcal{H}_1$ is non-singular; hence, $\mathcal{H}_1$ is absolutely irreducible and has genus 6. □

Proposition 5.4. *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 5.3, $\mathcal{H}_1$ is a non-singular curve such that $F_1=\mathbb{F}_q(\mathcal{H}_1)$. 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,

$$\begin{aligned} v_{P_1}(u) = v_{R_1^i}(u) = -1, \quad v_{Q_1}(u)=0,\\ v_{Q_1}(v) = v_{R_1^i}(v) = -1, \quad v_{P_1}(v)=0. \end{aligned} \tag{7}$$

Consider the function field $\mathbb{K}(u,v)(x)=\mathbb{K}(v,x)$ defined by $u=x^\sigma-x$. Also, 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, we can apply Theorem 2.2, so that $\mathbb{K}(x,v):\mathbb{K}(u,v)$ is a Galois extension and $[\mathbb{K}(x,v):\mathbb{K}(u,v)]=\sigma$. Moreover P_1 and R_1^i, $i=1,2,3$, are the only totally ramified places; all other places are unramified. By Lemma 2.4, $\mathbb{F}_q$ is the constant field of $F_2 = \mathbb{F}_q(x,v)$. The genus is given by

$$\begin{aligned} g_2 &= \sigma g_1 + \frac{\sigma-1}{2}\left(-2 + \sum_{P\in\mathbb{P}(\mathbb{K}(u,v))}(m_P+1)\deg P\right) \\ &= 6\sigma + \frac{\sigma-1}{2}(-2+4(1+1)) = 9\sigma - 3. \end{aligned}$$

□

Denote by P_2, R_2^i the places of $\mathbb{K}(x,v)$ lying over P_1, R_1^i, respectively. Also, let $Q_2^1,\ldots,Q_2^\sigma$ be the places lying over Q_1.

Proposition 5.5. *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

$$v_{P_2}(v) = 0, \quad v_{Q_2^i}(v) = -1, \quad v_{R_2^i}(v) = -\sigma.$$

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,

$$\begin{aligned} v - (\rho_i^\sigma - \rho_i) = v - \xi^i x^\sigma + k_i x = v - \xi^i x^\sigma \\ +\xi^i x - \xi^i x + k_i x = v - \xi^i u + (k_i - \xi^i)x. \end{aligned}$$

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, by Theorem 2.2, $\mathbb{K}(x,y):\mathbb{K}(x,v)$ is a Galois extension with $[\mathbb{K}(x,y):\mathbb{K}(x,v)] = \sigma$ and

$$\begin{aligned} g_3 &= \sigma g_2 + \frac{\sigma-1}{2}\left(-2 + \sum_{P\in\mathbb{P}(\mathbb{K}(x,v))}(m_P+1)\deg P\right) \\ &\leq \sigma(9\sigma-3) + \frac{\sigma-1}{2}(-2+(\sigma+2)(1+1)) = 10\sigma^2 - 3\sigma - 1. \end{aligned}$$

Finally, by Lemma 2.4, $\mathbb{F}_q$ is the constant field of $F_3 = \mathbb{F}_q(x,y)$. □

In the extension $\mathbb{K}(x,y) : \mathbb{K}(x,v)$ the unique 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 5.6. *Let $a,b\in\mathbb{F}_q$, with $b\neq 0$ and $b\neq a^5$. The equations*

$$\begin{cases} \eta^2 = -\frac{4\mu^3+5\mu+5}{4\mu} \\ 64\mu^6\lambda^5 - 64a\mu^6\lambda^4 + 80\mu^4\lambda^5 - 80a\mu^4\lambda^4 \\ \quad +76\mu^2\lambda^5 + 180a\mu^2\lambda^4 - 256b\mu^2 - 25\lambda^5 + 25a\lambda^4 = 0 \end{cases}$$

define a function field $\mathbb{F}_q(\mu, \lambda, \eta)$ *with genus at most* 53*, whose field of constants is* $\mathbb{F}_q$*.*

Proof. We divide the proof in three steps.

1. We show that the equation $C(\rho, \lambda) = 0$, with
$$C(\rho, \lambda) = 64\rho^3\lambda^5 - 64a\rho^3\lambda^4 + 80\rho^2\lambda^5 \\ -80a\rho^2\lambda^4 + 76\rho\lambda^5 + 180a\rho\lambda^4 - 256b\rho - 25\lambda^5 + 25a\lambda^4,$$
defines a function field $\mathbb{F}_q(\rho, \lambda)$ of genus at most 8, whose field of constants is $\mathbb{F}_q$.
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_∞ is singular with multiplicity 5; the tangent lines at P_∞ are $L = 0$ with multiplicity 4 and $L = a$. The point Q_∞ is singular with multiplicity 3; the tangent lines at Q_∞ 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 the line ℓ is a component of $\mathcal{C}$. If $P_\infty \in \ell$, then ℓ has equation $L = k$; hence, either $k = 0$ or $k = a$, which implies either $256b = 0$ or $256(a^5 - b) = 0$, against the assumptions. If $Q_\infty \in \ell$, then ℓ 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, $8 - i$; also, 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 get $b = 0$, a contradiction.
Therefore, $\mathcal{C}$ is absolutely irreducible. As $\mathcal{C}$ has two singular points of multiplicity 5 and 3, the genus of $\mathcal{C}$ is at most 8. The thesis follows, since $\mathbb{F}_q(\rho, \lambda)$ is the function field of $\mathcal{C}$, and $\mathbb{F}_q$ is the field of constants of $\mathbb{F}_q(\rho, \lambda)$ by Lemma 2.4.
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 field of constants is $\mathbb{F}_q$.
The function ρ 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, ρ is not a 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 ρ has odd multiplicity; namely, the place A_a and between one and five places lying over the pole P_∞ of ρ in $\mathbb{K}(\rho)$. Then, by Theorem 2.1, the genus of $\mathbb{F}_q(\mu, \lambda)$ is at most $1 + 2(8 - 1) + 6/2 = 18$. By Lemma 2.4, $\mathbb{F}_q$ 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, whose field of constants is $\mathbb{F}_q$.
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

in $\mathbb{K}(\mu, \lambda, \eta) : \mathbb{K}(\mu, \lambda)$. There are exactly five places of $\mathbb{K}(\mu, \lambda)$ lying over P_∞; they are ramified in $\mathbb{K}(\mu, \lambda, \eta) : \mathbb{K}(\mu, \lambda)$. Let μ_1, μ_2, μ_3 be the three distinct solutions in μ 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, by Theorem 2.1, the genus of $\mathbb{F}_q(\mu, \lambda, \eta)$ is at most $1 + 2(18 - 1) + 36/2 = 53$. By Lemma 2.4, $\mathbb{F}_q$ is the field of constants of $\mathbb{F}_q(\mu, \lambda, \eta)$.

□

Proposition 5.7. *Let $a, b \in \mathbb{F}_q$, with $b \neq 0$ and $b \neq a^5$. The equations*

$$\begin{cases} b + (u+e)(v+e)(u+v+2e)\left[u^2+v^2+2e(u+v)+e^2\right] \\ -a\left[u^4+u^3v+u^2v^2+uv^3+v^4+5e(u+v)(u^2+v^2)\right. \\ \left.+10e^2(u^2+uv+v^2)+9e^3(u+v)+4e^4\right] = 0 \\ \\ w^3+w^2(u+v+5e)+w\left[u^2+uv+v^2+5e(u+v)+10e^2\right] \\ +(u+v)(u^2+v^2)+5e(u^2+uv+v^2)+9e^2(u+v)+7e^3 = 0 \end{cases} \tag{8}$$

define a function field $\mathbb{F}_q(u, v, w)$ with genus at most 53, whose field of constants is $\mathbb{F}_q$.

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

$$\begin{aligned} C_1(U,V,W) &= b + UV\left(U^3+U^2V+UV^2+V^3\right) \\ &\quad -a\left(U^4+U^3V+U^2V^2+UV^3+V^4\right), \\ C_2(U,V,W) &= W^3+W^2(U+V)+W\left(U^2+UV+V^2\right) \\ &\quad +\left(U^3+U^2V+UV^2+V^3\right). \end{aligned}$$

Denote by $\overline{u}, \overline{v}, \overline{w}$ the coordinate functions of $\mathcal{X}$. Now 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

$$\mathcal{Y} : \begin{cases} L^3\left(E^2 + \frac{4M^3+5M+5}{4M}\right) = 0 \\ 64M^6L^5 - 64aM^6L^4 + 80M^4L^5 - 80aM^4L^4 \\ \quad +76M^2L^5 + 180aM^2L^4 - 256bM^2 - 25L^5 + 25aL^4 = 0 \end{cases}.$$

Since $\mathcal{Y}$ has no points (M, L, E, T) with $L = 0$, equivalent equations for $\mathcal{Y}$ are

$$\mathcal{Y} : \begin{cases} E^2 = -\frac{4M^3+5M+5}{4M} \\ 64M^6L^5 - 64aM^6L^4 + 80M^4L^5 - 80aM^4L^4 \\ \quad +76M^2L^5 + 180aM^2L^4 - 256bM^2 - 25L^5 + 25aL^4 = 0 \end{cases}.$$

By Lemma 5.6, $\mathcal{X}$ 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 Eq. (8). 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 σ^2 are coprime. Also, $\mathbb{F}_q$ is the field of constants of F_4.

For $i = 1, \dots, \sigma$, we have by the Eq. (8) 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^{ℓ}, respectively; let $R_{4,2}^{i,1}$ be the place centered at the point $(X,Y,0,0)$ with $W = 0$.

Proposition 5.8. *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

$$\begin{aligned} w - (\rho^\sigma - \rho) &= \xi(x^\sigma - x) + \Phi - k^\sigma x^\sigma + kx \\ &= (\xi - k^\sigma)x^\sigma + (k - \xi)x + \Phi = (k - \xi)x + \Phi. \end{aligned}$$

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,

$$v_{P_4^{i,j}}(w - (\rho^\sigma - \rho)) = -1. \tag{9}$$

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 (9),

$$-1 = v_{P_4^{i,j}}(\gamma w - (\gamma\rho^\sigma - \gamma\rho)) = v_{P_4^{i,j}}(\gamma w - (\alpha^\sigma - \alpha)),$$

with $\alpha = \gamma\rho \in \mathbb{K}(x,y,w)$. Since

$$\alpha^\sigma - \alpha = \left(\alpha^{\sigma/p} + \alpha^{\sigma/p^2} + \cdots + \alpha\right)^p - \left(\alpha^{\sigma/p} + \alpha^{\sigma/p^2} + \cdots + \alpha\right),$$

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 $\beta = \alpha^{\sigma/p} + \alpha^{\sigma/p^2} + \cdots + \alpha \in \mathbb{K}(u,v,w)$. 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 [5] 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 σ. Also, by Lemma 2.4, $\mathbb{F}_q$ is the constant field of $\mathbb{F}_q(x,y,z)$.

Finally, we give a bound on g_5. By Castelnuovo's Inequality (see Theorem 3.11.3 in [17]),

$$g_5 \leq [F_5 : F_3] \cdot g_3 + [F_5 : \mathbb{F}_q(u,v,z)] \cdot g(\mathbb{F}_q(u,v,z)) + ([F_5 : F_3] - 1) \cdot ([F_5 : \mathbb{F}_q(u,v,z)] - 1)\,.$$

We have

$$[F_5 : F_3] = [F_5 : F_4] \cdot [F_4 : F_3] = 3\sigma\,, \qquad g_3 \leq 10\sigma^2 - 3\sigma - 1.$$

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 the Eq. (8), 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,

$$v_{\widetilde{P}_2^j}(w) = v_{\widetilde{Q}_2^j}(w) = v_{\widetilde{R}_2^{i,j}}(w) = -1\,, \quad \text{for } j = 1,2,3\,,$$

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, by Theorem 2.2, $\mathbb{K}(u,v,z) : \mathbb{K}(u,v,w)$ is a generalized Artin–Schreier extension of degree σ, and

$$\begin{aligned} g(\mathbb{K}(u,v,z)) &= \sigma\, g(\mathbb{K}(u,v,w)) + \frac{\sigma-1}{2}\left(-2 + \sum_{P \in \mathbb{P}(\mathbb{K}(u,v,w))} (m_P + 1) \deg P\right) \\ &\leq 53\sigma + \frac{\sigma - 1}{2}(-2 + 15(1+1)) = 67\sigma - 14. \end{aligned}$$

Therefore $g(\mathbb{F}_q(u,v,z)) \leq 67\sigma - 14$, and

$$\begin{aligned} g_5 &\leq 3\sigma(10\sigma^2 - 3\sigma - 1) + \sigma^2(67\sigma - 14) \\ &\quad + (3\sigma - 1)(\sigma^2 - 1) = 100\sigma^3 - 24\sigma^2 - 6\sigma + 1. \end{aligned}$$

□

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 $F_5 : F_4$ (see [17, Prop. 3.7.8]), 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 5.9. *Let $a, b \in \mathbb{F}_q$ with $b \neq 0$ and $b \neq a^5$. The equation*

$$\begin{aligned} &t^2 + t(u + v + w + 5e) + u^2 + v^2 + w^2 + uv + uw + vw \\ &\quad + e\,[3(u + v + w) + 2(uv + uw + vw)] + 10e^2 = 0 \end{aligned} \tag{10}$$

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 $C_1(\overline{u},\overline{v},\overline{w}) = 0$ and $C_2(\overline{u},\overline{v},\overline{w}) = 0$, where

$$C_1(\overline{u},\overline{v},\overline{w}) = b + \overline{uv}(\overline{u}^3 + \overline{u}^2\overline{v} + \overline{uv}^2 + \overline{v}^3) - a(\overline{u}^4 + \overline{u}^3\overline{v} + \overline{u}^2\overline{v}^2 + \overline{uv}^3 + \overline{v}^4),$$
$$C_2(\overline{u},\overline{v},\overline{w}) = \overline{w}^3 + \overline{w}^2(\overline{u} + \overline{v}) + \overline{w}(\overline{u}^2 + \overline{uv} + \overline{v}^2) + (\overline{u}^3 + \overline{u}^2\overline{v} + \overline{uv}^2 + \overline{v}^3).$$

As shown in the proof of Proposition 5.7, $\mathbb{K}(\overline{u},\overline{v},\overline{w})$ has genus at most 53 and constant field $\mathbb{F}_q$. Let

$$\overline{t}^2 = -\frac{3\overline{u}^2 + 3\overline{v}^2 + 3\overline{w}^2 + 2\overline{uv} + 2\overline{uw} + 2\overline{vw}}{4}. \qquad (11)$$

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, the Eq. (11) 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. By Theorem 2.1,

$$g(\mathbb{K}(\overline{u},\overline{v},\overline{w},\overline{t})) \leq 1 + 2(53-1) + \frac{1}{2}\cdot 90 = 150.$$

Also, by Lemma 2.4, $\mathbb{F}_q$ is the constant field of $\mathbb{F}_q(\overline{u},\overline{v},\overline{w},\overline{t})$. By the substitution

$$\overline{u} = u+e,\ \ \overline{v} = v+e,\quad \overline{w} = w+e,\ \ \overline{t} = t+e+\frac{1}{2}\left((u+e)+(v+e)+(w+e)\right),$$

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 Eqs. (8) and (10). The thesis follows. □

The function field F_6 is the compositum of $\mathbb{F}_q(u,v,w,t)$ and F_5. The extension $F_6 : F_1$ has degree $6\sigma^3$, since 6 and σ^3 are coprime. Also, $\mathbb{F}_q$ is the field of constants of F_6.

Proposition 5.10. *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 field of constants 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 Eq. (10), $\widetilde{R}_2^{2,1}$ 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 $e \notin M$ (with M as in (4)) and $\eta \notin \mathbb{F}_\sigma$.

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 $\mathbb{K}(u,v,w,t)$ 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 let $\rho = kx$; then

$$\begin{aligned} t-(\rho^\sigma-\rho) &= \eta(x^\sigma - x) + \Phi - k^\sigma x^\sigma \\ &\quad + kx = (\eta - k^\sigma)x^\sigma + (k-\eta)x + \Phi = (k-\eta)x + \Phi. \end{aligned}$$

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

$$\begin{aligned} v_{R_{6,2,1}^{i,1,j}}(\Phi) &= e(R_{6,2,1}^{i,1,j} \mid \widetilde{R}_{3,2}^{1,1}) \cdot v_{\widetilde{R}_{3,2}^{1,1}}(\Phi) \geq 0, \\ v_{R_{6,2,1}^{i,1,j}}(x) &= e(R_{6,2,1}^{i,1,j} \mid R_{5,2}^{i,1,j}) \cdot v_{R_{5,2}^{i,1,j}}(x) = -1. \end{aligned}$$

Therefore,

$$v_{R_{6,2,1}^{i,1,j}}(t-(\rho^\sigma-\rho)) = -1.$$

Arguing as in the proof of Proposition 5.8, 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 [5] 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 σ. Also, by Lemma 2.4, $\mathbb{F}_q$ is the constant field of $\mathbb{F}_q(x,y,z)$. Finally, we give a bound on g_7. By Castelnuovo's Inequality (see Theorem 3.11.3 in [17]),

$$\begin{aligned} g_7 \;\leq\; & [F_7 : F_5] \cdot g_5 + [F_7 : \mathbb{F}_q(u,v,w,r)] \cdot g(\mathbb{F}_q(u,v,w,r)) \\ & + ([F_7:F_5]-1) \cdot ([F_7 : \mathbb{F}_q(u,v,w,r)] - 1)\,. \end{aligned}$$

We have

$$[F_7 : F_5] = [F_7 : F_6] \cdot [F_6 : F_5] = 2\sigma\,, \qquad g_5 \leq 100\sigma^3 - 24\sigma^2 - 6\sigma + 1.$$

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 a basis of F_7 over $\mathbb{F}_q(u,v,w,r)$ is $\{x^i y^j z^\ell \mid i,j,\ell = 1,\ldots,\sigma\}$; 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 with σ. The valuation of t at any other place of $\mathbb{K}(u,v,w,t)$ is non-negative. Then, by Theorem 2.2, $\mathbb{K}(u,v,w,r) : \mathbb{K}(u,v,w,t)$ is a generalized Artin–Schreier extension of degree σ, with at most $2 \cdot 15$ ramified places, and

$$
\begin{aligned}
g(\mathbb{K}(u,v,w,r)) &= \sigma\, g(\mathbb{K}(u,v,w,t)) \\
&\qquad + \frac{\sigma-1}{2}\left(-2 + \sum_{P\in\mathbb{P}(\mathbb{K}(u,v,w,t))} (m_P+1)\deg P\right) \\
&\le 150\sigma + \frac{\sigma-1}{2}(-2+30(1+1)) = 179\sigma - 29.
\end{aligned}
$$

Therefore $g(\mathbb{F}_q(u,v,z)) \le 179\sigma - 29$, and

$$
\begin{aligned}
g_7 &\le 2\sigma(100\sigma^3 - 24\sigma^2 - 6\sigma + 1) + \sigma^3(179\sigma - 29) + (2\sigma-1)(\sigma^3-1) \\
&= 381\sigma^4 - 78\sigma^3 - 12\sigma^2 + 1.
\end{aligned}
$$

□

Theorem 5.11. *Let $\mathcal{K}_e$ as in (5), 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 $\mathrm{AG}(2,q)\backslash\mathcal{Q}$ except possibly those lying on the line $Y=0$.*

Proof. Let $P=(a,b) \in \mathrm{AG}(2,q)\backslash\mathcal{Q}$ and assume that $a \ne t$, $a \ne -4e$, and $b \ne 0$. 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 [17, Thm. 3.1.11] that

$$
Z_1 \le 2\sigma(3\sigma + 3\sigma + 6\sigma + 3\sigma^2) = 6\sigma^3 + 24\sigma^2.
$$

Now 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

$$
\begin{aligned}
Z_2 &\le \sum_{\lambda\in\mathbb{F}_\sigma} \deg(x-y-\lambda)_0 \\
&= \sum_{\lambda\in\mathbb{F}_\sigma} \deg(x-y-\lambda)_\infty.
\end{aligned}
$$

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, by [17, Thm. 3.1.11],

$$
\begin{aligned}
\deg(x-y-\lambda)_\infty &= (12\sigma + 3\sigma^2)\cdot[\mathbb{K}(x,y,z,r) : \mathbb{K}(x,y,z)] \\
&= 6\sigma^3 + 24\sigma^2 \quad \text{for all} \quad \lambda \in \mathbb{F}_\sigma\,;
\end{aligned}
$$

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 theorem 2.3 we have

$$N_q \;\geq\; q + 1 - 2g_7\sqrt{q} \;\geq\; q + 1 - 2(381\sigma^4 - 78\sigma^3 - 12\sigma^2 + 1)\sqrt{q}.$$

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 5.2, the point 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 Eq. (6). Arguing as above $\mathcal{K}_{e'}$ covers the point P. Clearly $\mathcal{K}_{e'} = \mathcal{K}_e$, and the assertion follows. □

6. Constructions of 5-independent subsets

We now 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.

Definition 6.1. *Let G be a finite abelian group and let $\mathcal{E}$ be a subset of G. If*

$$y_1 + y_2 + y_3 + y_4 + y_5 \neq 0 \qquad \text{for all} \qquad y_1, y_2, y_3, y_4, y_5 \in \mathcal{E},$$

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, let $s^\wedge S$ denote the s-fold sumset of S, that is,

$$s^\wedge S = \{y_1 + \ldots + y_s \mid y_1, \ldots, y_s \in S\}.$$

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 6.2. *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

$$\mathbb{Z}_p \backslash \left\{ \frac{p-i}{5} + j \;\middle|\; 1 \leq j \leq i - 1 \right\}.$$

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

$$\begin{aligned} 4^\wedge \mathcal{E} &= \{-4\} \cup (-3+\mathcal{E}^*) \cup (-2+2^\wedge\mathcal{E}^*) \cup (-1+3^\wedge\mathcal{E}^*) \cup 4^\wedge\mathcal{E}^* = \\ &\{-4\} \cup \{-2,0\} \cup \left[2, \frac{p-i-15}{5}\right] \cup \{0,2\} \cup \\ &\left[4, \frac{2p-2i-10}{5}\right] \cup \{2,4\} \cup \left[6, \frac{3p-3i-5}{5}\right] \cup \{4,6\} \cup \left[8, \frac{4p-4i}{5}\right] = \\ &\{-4,-2,0\} \cup \left[2, \frac{4p-4i}{5}\right] \end{aligned}$$

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 off $\mathcal{E}$ is

$$-4^\wedge\mathcal{E} = \{0,2,4\} \cup \left[\frac{p+4i}{5}, p-2\right].$$

The noncovered 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 $h' \geq 3$. 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

$$\mathcal{E} = \mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3, \tag{12}$$

where $\mathcal{E}_1 = \{(a,1,1) \mid a \in A\backslash\{-4\}\}$, $\mathcal{E}_2 = \{(1,b,1) \mid b \in B\backslash\{-4\}\}$, $\mathcal{E}_3 = \{(1,1,c) \mid c \in C\backslash\{-4\}\}$. 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 6.3. *Let $h' \geq 3$, $p > 5$, and let $\mathcal{E}$ be as in (12). Then $\mathcal{E}$ is a 5-independent subset of $\mathbb{Z}_p^{h'}$ of size $2p^{\frac{h'-1}{2}} + p - 5$ not covering three 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 $e = (x,y,z) \in \mathbb{Z}_p^{h'} \backslash \mathcal{E}$ 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 $(-4, 1, 1)$, $(1, -4, 1), (1, 1, -4)$. □

7. 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 (5), 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 4.1, the four points P, A_1, A_2, and A_3 are collinear if and only if

$$\begin{cases} t^3 + t^2 (x^\sigma - x + e_1 + y^\sigma - y + e_2) \\ +t \left((x^\sigma - x + e_1)^2 + (x^\sigma - x + e_1)(y^\sigma - y + e_2) + (y^\sigma - y + e_2)^2\right) \\ + (x^\sigma - x + e_1 + y^\sigma - y + e_2) \left((x^\sigma - x + e_1)^2 + (y^\sigma - y + e_2)^2\right) = 0 \\ \\ (z^\sigma - z + e_3)^2 + (z^\sigma - z + e_3)(x^\sigma - x + e_1 + y^\sigma - y + e_2 + t) + (x^\sigma - x + e_1)^2 \\ + (y^\sigma - y + e_2)^2 + t^2 + (x^\sigma - x + e_1)(y^\sigma - y + e_2) \\ +(x^\sigma - x + e_1)t + (y^\sigma - y + e_2)t = 0. \end{cases} \qquad (13)$$

Consider the following sequence of function fields:

$$\begin{array}{ll} L_5 = L_4(z) : & z^\sigma - z = w \\ \quad \Big| \ \sigma & \\ L_4 = L_3(w) : & (w + e_3)^2 + (w + e_3)(x^\sigma - x + e_1 + y^\sigma - y + e_2 + t) \\ & + (x^\sigma - x + e_1)^2 + (y^\sigma - y + e_2)^2 + t^2 \\ & + (x^\sigma - x + e_1)(y^\sigma - y + e_2) + (x^\sigma - x + e_1)t + (y^\sigma - y + e_2)t = 0 \\ \quad \Big| \ 2 & \\ L_3 = L_2(y) : & y^\sigma - y = v \\ \quad \Big| \ \sigma & \\ L_2 = L_1(x) : & x^\sigma - x = u \\ \quad \Big| \ \sigma & \\ L_1 = \mathbb{F}_q(u, v) : & t^3 + t^2 (u + e_1 + v + e_2) + t \left((u + e_1)^2 + (u + e_1)(v + e_2) + (v + e_2)^2\right) \\ & + (u + e_1 + v + e_2)\left((u + e_1)^2 + (v + e_2)^2\right) = 0 \end{array}$$

We are going to show that each extension $L_i : L_{i-1}$ is well-defined and that the field of constants of each L_i is $\mathbb{F}_q$. We will also estimate the genus of L_i. Finally, by using the Hasse–Weil bound, we will show that if q is large enough, then L_5 has a large number of $\mathbb{F}_q$-rational places, so that Eq. (13) have a suitable solution.

Proposition 7.1. *The equation* $f_1(u,v)=0$*, where*

$$\begin{aligned} f_1(u,v) &= t^3 + t^2\left(u+e_1+v+e_2\right) \\ &+t\left((u+e_1)^2+(u+e_1)(v+e_2)+(v+e_2)^2\right) \\ &\quad + \left(u+e_1+v+e_2\right)\left((u+e_1)^2+(v+e_2)^2\right), \end{aligned} \tag{14}$$

defines a function field $L_1=\mathbb{F}_q(u,v)$ *with genus* 1 *whose field of constants is* $\mathbb{F}_q$.

Proof. Let Γ_1 be the plane curve with equation $f_1(U,V)=0$, whose function field over $\mathbb{F}_q$ is L_1. The curve Γ_1 has three distinct ideal points; hence, they are simple points. Since

$$\begin{aligned} \partial_U f_1(U,V) &= 3(U+e_1)^2+2(U+e_1)(V+e_2) \\ &\quad +(V+e_2)^2+2t(U+e_1)+t(V+e_2)+t^2, \\ \partial_V f_1(U,V) &= (U+e_1)^2+2(U+e_1)(V+e_2)+3(V+e_2)^2 \\ &\quad +t(U+e_1)+2t(V+e_2)+t^2, \end{aligned}$$

we have by direct computation that Γ_1 has no singular affine points; here we use that $t\neq 0$, $p>5$, and $\sigma\equiv 3 \pmod 4$. Therefore, Γ_1 is non-singular. Then Γ_1 is absolutely irreducible with genus 1. By Lemma 2.4, $\mathbb{F}_q$ is the constant field of L_1. The thesis follows. □

Let ξ 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 Γ_1.

Proposition 7.2. *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 Γ_1. Then, by Theorem 2.2, $\mathbb{K}(x,v):\mathbb{K}(u,v)$ is a Galois extension with $[\mathbb{K}(x,v):\mathbb{K}(u,v)]=\sigma$. Moreover, P_1^1, P_1^2, and P_1^3 are the unique totally ramified places, and

$$g_2=\sigma\cdot 1+\frac{\sigma-1}{2}\left(-2+3(1+1)\right)=3\sigma-2.$$

By Lemma 2.4, $\mathbb{F}_q$ 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 7.3. *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,

$$\begin{aligned} v-(\rho_i^\sigma-\rho_i) &= v-\xi^i x^\sigma + k_i x = v-\xi^i x^\sigma \\ &\quad +\xi^i x-\xi^i x+k_i x = v-\xi^i u+\left(k_i-\xi^i\right)x. \end{aligned}$$

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, by Theorem 2.2, $\mathbb{K}(x,y):\mathbb{K}(x,v)$ is a Galois extension with

$[\mathbb{K}(x, y) : \mathbb{K}(x, v)] = \sigma$. Moreover, P_2^1 and P_2^3 are the unique totally ramified places, and

$$g_3 = \sigma(3\sigma - 2) + \frac{\sigma - 1}{2}\left(-2 + 2(1 + 1)\right) = 3\sigma^2 - \sigma - 1.$$

Finally, by Lemma 2.4, $\mathbb{F}_q$ 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 7.4. *The equation*

$$\begin{aligned}(w + e_3)^2 + (w + e_3)\,(u + e_1 + v + e_2 + t) + (u + e_1)^2 + (v + e_2)^2 \\ + t^2 + (u + e_1)(v + e_2) + (u + e_1)t + (v + e_2)t = 0 \qquad (15)\end{aligned}$$

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

$$\begin{aligned}\theta^2 = \Theta(u, v) = -\tfrac{1}{4}\big[&3(u + e_1)^2 + 3(v + e_2)^2 + 3t^2 \\ &+ 2(u + e_1)(v + e_2) + 2(u + e_1)t + 2(v + e_2)t\big].\end{aligned}$$

The poles of w and θ in $\mathbb{K}(u, v)$ are P_1^1, P_1^2, and P_1^3; θ^2 has valuation 2 at each of them. Hence, the number of zeros of θ^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. 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 (14). By direct computation, $R \neq 0$. Since $f_1(U, V)$ has odd degree, this implies that θ has a zero in $\mathbb{K}(u, v)$ with odd multiplicity. Then, by Theorem 2.1, $\mathbb{K}(u, v, \theta) : \mathbb{K}(u, v)$ is a Galois extension with $[\mathbb{K}(u, v, \theta) : \mathbb{K}(u, v)] = 2$. Moreover, the unique totally ramified places are the zeros of θ^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 2.4, $\mathbb{F}_q$ 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 σ^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 points $(1, -1, \xi, 0)$, $(1, -1, -\xi, 0)$.

Proposition 7.5. *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 $k \in \sigma$ and $k \neq \sigma$. Let $\rho = kx$; then $w - (\rho^\sigma - \rho) = (k - \xi)x + \Phi$. Since $v_{Q_2^1}(\Phi) = e(Q_2^1 \mid \widetilde{Q}_2^1) \cdot v_{\widetilde{Q}_2^1}(\Phi) \geq 0$ and $v_{Q_2^1}(x) = e(Q_2^1 \mid P_2) \cdot v_{P_2}(x) = -1$, $v_{Q_2^1}(w - (\rho^\sigma - \rho)) = -1$. Arguing as in the proof of Proposition 5.8, 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 [5] 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 σ. Also, by Lemma 2.4, $\mathbb{F}_q$ is the constant field of $\mathbb{F}_q(x,y,z)$. Finally, we give a bound on g_5. By Castelnuovo's Inequality (see Theorem 3.11.3 in [17]),

$$\begin{aligned} g_5 \leq\ & [L_5 : L_3] \cdot g_3 + [L_5 : \mathbb{F}_q(u,v,z)] \cdot g(\mathbb{F}_q(u,v,z)) \\ & + ([L_5 : L_3] - 1) \cdot ([L_5 : \mathbb{F}_q(u,v,z)] - 1) \,. \end{aligned}$$

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 a basis of L_5 over $\mathbb{F}_q(u,v,z)$ is $\{x^i y^j \mid i,j = 1,\ldots,\sigma\}$; 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 (15), 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, by Theorem 2.2, $\mathbb{K}(u,v,z) : \mathbb{K}(u,v,w)$ is a Galois 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 7.6. *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 (13) 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

$$\begin{aligned} Z_2 &\leq \textstyle\sum_{\lambda \in \mathbb{F}_\sigma} \deg(x - y - \lambda)_0 = \sum_{\lambda \in \mathbb{F}_\sigma} \deg(x - y - \lambda)_\infty \\ &= |\{P_1^1, P_1^2, P_1^3\}| \cdot [L_5 : L_1] = 6\sigma^3. \end{aligned}$$

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 Theorem 2.3,

$$N_q \geq q + 1 - 2g_5\sqrt{q} \geq q + 1 - 2\left(21\sigma^3 - 9\sigma^2 - 6\sigma + 1\right)\sqrt{q}.$$

The hypothesis $q \geq 1764\sigma^6$ implies $N_q \geq 18\sigma^3 + 2\sigma^2 + 4\sigma + 1$. □

Proposition 7.7. *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 7.6, 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 7.6, 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 Theorem 2.3. □

Henceforth, $\mathcal{E}$ denotes a 5-independent subset of $\mathbb{F}_q/M$, for M as in (4). Let

$$\mathcal{K}_{\mathcal{E}} = \bigcup_{M+e\in\mathcal{E}} \mathcal{K}_e. \tag{16}$$

Proposition 7.8. *The set $\mathcal{K}_{\mathcal{E}}$ is a $(k,4)$-arc.*

Proof. By Proposition 4.2, 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 7.9. *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 7.7, 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, $e_P + e_1 + e_2 + e_3 + e_4' \in M$. 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 7.10. *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 (16). 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 5.11, 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 7.9, 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 1.1. Identify the additive groups $\mathbb{Z}_p^{h'}$ and $\mathbb{F}_q/M$. From Propositions 6.2 and 6.3 the following values of n and m occur in Theorem 7.10:

- 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 $\sigma \geq p^3$,

$$n = 2p^{\frac{h'-1}{2}} + p - 5 \quad \text{and} \quad m = 3.$$

References

[1] Anbar, N., Giulietti, M.: *Bicovering arcs and small complete caps from elliptic curves*. J. Algebr. Comb. **38**, 371–392 (2013)

[2] Anbar, N., Bartoli, D., Giulietti, M., Platoni, I.: *Small complete caps from singular cubics*. J. Comb. Des. **22**(10), 409–424 (2014)

[3] Anbar, N., Bartoli, D., Giulietti, M., Platoni, I.: *Small complete caps from singular cubics, II*. J. Algebr. Comb. **41**, 185–216 (2015)

[4] Bartoli, D., Giulietti, M., Zini, G.: *Complete (k,3)-arcs from quartic curves*. Des. Codes Cryptogr. **79**(3), 487–505 (2016)

[5] Garcia, A., Stichtenoth, H.: *Elementary abelian p-extensions of algebraic function fields*. Manuscr. Math. **72**, 67–79 (1991)

[6] Giulietti, M., Pambianco, F., Torres, F., Ughi, E.: *On complete arcs arising from plane curves*. Des. Codes Cryptogr. **25**, 237–246 (2002)

[7] Giulietti, M., Pasticci, F.: *On the completeness of certain n-tracks arising from elliptic curves*. Finite Fields Appl. **13**(4), 988–1000 (2007)

[8] Hamilton, N., Penttila, T.: *Sets of type (a, b) from subgroups of $\Gamma L(1, p^R)$*. J. Algebr. Comb. **13**, 67–76 (2001)

[9] Hirschfeld, J.W.P.: Algebraic Curves, Arcs, and Caps over Finite Fields. Quaderni del Dipartimento di Matematica dell'Università del Salento, Lecce (1986)

[10] Hirschfeld, J.W.P.: Projective Geometries over Finite Fields, 2nd edn. Oxford University Press, Oxford (1998)

[11] Hirschfeld, J.W.P., Pichanick, E.V.D.: *Bounds for arcs of arbitrary degree in finite Desarguesian planes*. J. Comb. Des. **24**, 184–196 (2016)

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

[13] Hirschfeld, J.W.P., Storme, L.: The packing problem in statistics, coding theory, and finite projective spaces: update 2001. In: Blokhuis A., Hirschfeld J. W. P., Jungnickel D., Thas J. A., (eds.) Finite Geometries, Proceedings of the Fourth Isle of Thorns Conference. Developments in Mathematics 3, pp. 201–246. Kluwer Academic Publishers, Boston (2001)

[14] Hirschfeld, J.W.P., Voloch, J.F.: *The characterization of elliptic curves over finite fields*. J. Aust. Math. Soc. **45**, 275–286 (1988)

[15] Lombardo-Radice, L.: *Sul problema dei k-archi completi in* $S_{2,q}$ ($q = p^t$, *p primo dispari*). Boll. Un. Mat. Ital. **11**(3), 178–181 (1956)

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

[17] Stichtenoth, H.: Algebraic Function Fields and Codes, Volume 254 of Graduate Texts in Mathematics, 2nd edn. Springer, Berlin (2009)

[18] Szöni, T.: Complete arcs in Galois planes: a survey. Quaderni del Seminario di Geometrie Combinatorie 94, Dipartimento di Matematica "G. Castelnuovo", Università degli Studi di Roma "La Sapienza", Roma (1989)

[19] Szöni, T.: Some applications of algebraic curves in finite geometry and combinatorics. In: Surveys in combinatorics, 1997 (London), vol. **241** of London Mathematical Society Lecture Note Series, pp. 197–236. Cambridge University Press, Cambridge, (1997)

[20] Tallini Scafati, M.: Graphic Curves on a Galois Plane. Atti del Convegno di Geometria Combinatoria e sue Applicazioni, Perugia (1970)

Daniele Bartoli
Università degli Studi di Perugia
Perugia
Italy
e-mail: daniele.bartoli@dmi.unipg.it

Pietro Speziali
Università degli Studi della Basilicata
Potenza
Italy

Giovanni Zini
Università degli Studi di Firenze
Firenze
Italy

Received: January 29, 2017.