Des. Codes Cryptogr. (2016) 79:487–505
DOI 10.1007/s10623-015-0073-7

Complete $(k, 3)$-arcs from quartic curves

Daniele Bartoli[1] · Massimo Giulietti[2] · Giovanni Zini[3]

Received: 1 December 2014 / Revised: 12 March 2015 / Accepted: 23 March 2015 /
Published online: 12 April 2015

Abstract Complete $(k, 3)$-arcs in projective planes over finite fields are the geometric counterpart of linear non-extendible Near MDS codes of length k and dimension 3. A class of infinite families of complete $(k, 3)$-arcs in $PG(2, q)$ is constructed, 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 this paper from the previously known infinite families, whose size differs from q by at most $2\sqrt{q}$.

Keywords $(k, 3)$-arcs · NMDS codes · Quartic curves

Mathematics Subject Classification 51E21

1 Introduction

A (k, r)-arc in $PG(2, q)$, the projective Galois plane over the finite field with q elements $\mathbb{F}_q$, is a set of k points no $(r + 1)$ of which are collinear and such that there exist r collinear points.

This is one of several papers published in *Designs*, *Codes and Cryptography* comprising the "Special Issue on Finite Geometries".

✉ Massimo Giulietti
massimo.giulietti@unipg.it

Daniele Bartoli
daniele275@gmail.com

Giovanni Zini
gzini@math.unifi.it

1 Department of Mathematics, Ghent University, Krijgslaan 281- B, 9000 Ghent, Belgium

2 Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli, 1, 06123 Perugia, Italy

3 Dipartimento di Matematica e Informatica "Ulisse Dini", Università degli Studi di Firenze, Viale Morgagni, 67/A, 50134 Florence, Italy

A general introduction to (k, r)-arcs can be found in the monograph [13, Chapt. 12], as well as in the survey paper [16, Sect. 5]. A natural problem in this context is the construction of infinite families of *complete* (k, r)-arcs, that is, arcs that are maximal with respect to set theoretical inclusion. From the standpoint of Coding Theory, complete (k, r)-arcs correspond to linear $[k, 3, k-r]_q$-codes which cannot be extended to a code with a larger minimum distance. If $r = 3$ the associated code is a Near MDS code, that is, a code C such that the Singleton defects of C and its dual $C^\perp$ is equal to 1 (see [6,7]).

In the case $r = 2$, the theory is well developed and quite rich of constructions; see e.g. [1–3,14–16,22,23] and the references therein, as well as [13, Chapt. 8–10]. On the other hand, for most $r > 2$, the only known infinite families either consist of the set of $\mathbb{F}_q$-rational points of some irreducible curve of degree r (see [10,17,24] for $r = 3$, as well as [11] for $r > 3$), or arise from the theory of 2-character sets in $\mathrm{PG}(2, q)$ (see Sects. 12.2 and 12.3 in [13], as well as the more recent work [12]). In particular, no general description of a complete $(k, 3)$-arc other than the set of $\mathbb{F}_q$-rational points of an irreducible cubic seems to be known. Computational results about the smallest size of a complete $(k, 3)$-arc in $\mathrm{PG}(2, q)$ have been obtained for $q \le 16$; see [4,5,19].

The aim of this paper is to provide a new class of infinite families of complete $(k, 3)$-arcs in $\mathrm{PG}(2, q)$. Our main result is the following.

Theorem 1 *Let σ be a non-square power of a prime $p > 2$, with $p \equiv 2 \pmod 3$. Define*

$$\tau(\sigma) = \begin{cases} \frac{p+5}{4} & \text{if } \sigma = p \ge 29\,, \\ 2\sqrt{\sigma p} + p - 4 & \text{if } \sigma \ge p^3. \end{cases}$$

Then, for each power q of σ with $q \ge 3600\,\sigma^6$, there exists a complete $(k, 3)$-arc in $\mathrm{PG}(2, q)$ of size

$$k \le \frac{\tau(\sigma)}{\sigma} q + 6.$$

The order of magnitude of the $(k, 3)$-arcs constructed in Theorem 1 is significantly smaller than that of the previously known families. In fact, complete $(k, 3)$-arcs arising from cubic curves have at least $q + 1 - 2\sqrt{q}$ points; on the other hand, the size of the arcs of Theorem 1 is asymptotically smaller than q. For example, if $\sigma = p^3$ with $p > 13$, then $q = \sigma^7$ can be chosen and the bound on k is roughly $q^{20/21}$.

The points of the $(k, 3)$-arcs constructed in this paper belong, with at most 6 exceptions, to the set of $\mathbb{F}_q$-rational points of the quartic curve $\mathcal{Q}$ with equation $Y = X^4$. It should be remarked that for this reason they share at most 18 points with an irreducible cubic. The proof of their completeness is based on a classical idea going back to Segre [20] and Lombardo-Radice [18]. In order to show that the 3-secants of the $(k, 3)$-arc cover a point P off the quartic curve $\mathcal{Q}$, we construct an algebraic curve $\mathcal{H}_P$ defined over $\mathbb{F}_q$ describing the collinearity of three 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 three points in the arc. The main difficulty here is that $\mathcal{H}_P$ is not a plane curve, but a curve embedded in the 3-dimensional space; see Eq. (3). 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 construct a $(q/\sigma, 3)$-arc $\mathcal{K}_t$ lying on the quartic curve $\mathcal{Q}$; it is associated to an additive subgroup M

with index σ in $\mathbb{F}_q$. We show in Sect. 4 that under the conditions on p, σ, and q of Theorem 1, the 3-secants of $\mathcal{K}_t$ 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 4-independent subset in the factor group $\mathbb{F}_q/M$ is constructed in Sect. 5. This allows us to show in Sect. 6 how to cover the points of $\mathcal{Q}$, for q large enough, by joining more copies of $\mathcal{K}_t$.

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 [21]. 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 [21, Prop. 3.7.3 and Cor. 3.7.4] *Consider an algebraic function field $\mathbb{F}$ with constant field $\mathbb{L}$ containing a primitive n-th root of the unity ($n > 1$ and n relatively prime to the characteristic of $\mathbb{L}$). Let $u \in \mathbb{F}$ 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. $$e(P'|P) = \frac{n}{r_P} \quad \textit{where} \quad r_P := GCD(n, v_P(u)) > 0\,;$$
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 3 [21, Th. 3.7.10] *Consider an algebraic function field $\mathbb{F}$ with constant field $\mathbb{L}$ of characteristic $p > 0$, and an additive separable polynomial $a(T) \in \mathbb{L}[T]$ 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

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

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 or 3 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. Let $\mathbb{K}$ denote 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 [21, 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 4 (Hasse–Weil bound, [21, 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 1 *Let $\mathbb{F}_q(\beta_1, \ldots, \beta_n)$ be a function field with constant field $\mathbb{F}_q$. Suppose that $f \in \mathbb{F}_q(\beta_1, \ldots, \beta_n)[T]$ 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 $(k, 3)$-arcs from quartic curves

Throughout the paper, 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 $\mathbb{K} = \overline{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$.

Let

$$\mathcal{Q} = \{(x, x^4) \mid x \in \mathbb{F}_q\}$$

be the set of $\mathbb{F}_q$-rational affine points of the plane quartic curve with Equation $Y = X^4$. The following propositions show the collinearity condition of three and four points on the quartic $\mathcal{Q}$.

Proposition 1 *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 2 *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 1, 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 an $(n, 3)$-arc contained in $\mathcal{Q}$ from a coset of an additive subgroup of $\mathbb{F}_q$. Let

$$M := \{(a^\sigma - a) \mid a \in \mathbb{F}_q\}, \tag{1}$$

and

$$\mathcal{K}_t := \{(v, v^4) \mid v \in M + t\}, \tag{2}$$

with $t \notin M$.

Proposition 3 *No four points of $\mathcal{K}_t$ are collinear.*

Proof By Proposition 2, if four distinct points $(a_i + t, (a_i + t)^4)$, $a_i \in M$, $i = 1, \ldots, 4$, are collinear then

$$a_1 + t + a_2 + t + a_3 + t + a_4 + t = 0, \quad \text{hence} \quad -4t = a_1 + a_2 + a_3 + a_4 \in M.$$

Since $p \neq 2$ and M is closed under multiplication by elements of $\mathbb{F}_\sigma$, we have $t \in M$, a contradiction. □

4 Points off $\mathcal{Q}$ are covered by $\mathcal{K}_t$

Consider a point $P = (a, b) \in \mathrm{AG}(2, q) \setminus \mathcal{Q}$. Arguing as in Proposition 2, the following result is obtained.

Proposition 4 *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 Note that the first equation gives the collinearity condition for A, B, C, whereas the second 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 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 1 *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 an* $\mathbb{F}_q$*-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 equations*

$$\mathcal{H}_P : \begin{cases} (Z^\sigma - Z)^2 + (Z^\sigma - Z)((X^\sigma - X) + (Y^\sigma - Y) + 4t) + 4t(X^\sigma - X + Y^\sigma - Y) \\ + 6t^2 + (X^\sigma - X)(Y^\sigma - Y) + (X^\sigma - X)^2 + (Y^\sigma - Y)^2 = 0 \\ a((X^\sigma - X)^2 + (Y^\sigma - Y)^2 + 2t^2 + 2t(X^\sigma - X) + 2t(Y^\sigma - Y))(X^\sigma - X + Y^\sigma - Y + 2t) \\ - (X^\sigma - X + t)(Y^\sigma - Y + t) \\ \cdot ((X^\sigma - X)^2 + (Y^\sigma - Y)^2 + (X^\sigma - X)(Y^\sigma - Y) + 3t^2 + 3t(X^\sigma - X + Y^\sigma - Y)) - b = 0 \end{cases}. \tag{3}$$

Consider the following sequence of function field extensions:

$$\begin{array}{l} F_5 = F_4(z) : \; z^\sigma - z = w \\ \quad \Big| \; \sigma \\ F_4 = F_3(w) : \; \begin{array}{l} w^2 + w((x^\sigma - x) + (y^\sigma - y) + 4t) + 4t(x^\sigma - x + y^\sigma - y) \\ + 6t^2 + (x^\sigma - x)(y^\sigma - y) + (x^\sigma - x)^2 + (y^\sigma - y)^2 = 0 \end{array} \\ \quad \Big| \; 2 \\ F_3 = F_2(y) : \; y^\sigma - y = v \\ \quad \Big| \; \sigma \\ F_2 = F_1(x) : \; x^\sigma - x = u \\ \quad \Big| \; \sigma \\ F_1 = \mathbb{F}_q(u, v) : \; \begin{array}{l} a(u^2 + v^2 + 2t^2 + 2tu + 2tv)(u + v + 2t) \\ -(u + t)(v + t)(u^2 + v^2 + uv + 3t^2 + 3t(u + v)) - b = 0 \end{array} \end{array}$$

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_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 $\mathbb{F}_q$-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 5 below. Equivalently, the plane quartic curve with equation

$$\mathcal{H}_1 : a(U^2+V^2+2t^2+2tU+2tV)(U+V+2t)-(U+t)(V+t)(U^2+V^2+UV+3t^2+3t(U+V))-b=0 \tag{4}$$

is non-singular. We start by investigating an auxiliary cubic curve.

Lemma 2 *Let $a, b \in \mathbb{F}_q$ with $b \neq 0$, $b \neq a^4$. The plane curve with equation*

$$a(C^2+2t^2+2tC-2D)(C+2t)-(D+tC+t^2)(C^2-D+3t^2+3tC)-b=0 \tag{5}$$

is absolutely irreducible and has genus $g_0 = 1$.

Proof After the affine transformation $\xi = D + tC + t^2$, $\zeta = C + 2t$ Eq. 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 5 *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. 5. Then the equations*

$$u + v = c, \qquad uv = d$$

define a function field $\mathbb{F}_q(u, v)$ of genus 3, with equation

$$\begin{aligned} &a(u^2+v^2+2t^2+2tu+2tv)(u+v+2t) \\ &\quad -(u+t)(v+t)(u^2+v^2+uv+3t^2+3t(u+v))-b=0 \end{aligned}$$

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 μ is a non-square in $\mathbb{K}(c, d)$. By substituting $D = C^2/4$ in (5) we obtain

$$-3/16\,C^4+(1/2\,a-3/2\,t)C^3+(3at-9/2\,t^2)C^2+(6at^2-6t^3)C+4at^3-b-3t^4=0. \tag{6}$$

Derivation with respect to C gives

$$-\frac{3}{4}(C+2t)^2(C-2a+2t).$$

Then, the only possible multiple solutions of (6) are $C = -2t$ and $C = 2a - 2t$. By straightforward computation, this actually happens only if $b = 0$ or $b = a^4$, which is excluded by our hypothesis. Therefore, there exist four distinct simple zeros of μ in $\mathbb{K}(c, d)$. Let P_∞ and Q_∞ be the places centered at the ideal points $(0, 1, 0)$ and $(1, a - t, 0)$, respectively. It is easily seen that

$$v_{P_\infty}(c^2 - 4d) = -2 \quad \text{and} \quad v_{Q_\infty}(c^2 - 4d) = -2.$$

By Theorem 2, the extension $\mathbb{K}(c,d)(\eta):\mathbb{K}(c,d)$, with $\eta^2=\mu$ is a Kummer extension of degree 2 and genus

$$g_1 = 1 + 2(g_0-1) + \frac{1}{2}\sum_{P\in\mathbb{P}(\mathbb{K}(c,d))}(n-r_P)\deg P = 1+\frac{1}{2}4 = 3.$$

Also, by Lemma 1, $\mathbb{F}_q$ 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

$$u=\eta+\frac{c}{2}, \qquad v=-\eta+\frac{c}{2}.$$

$\square$

Proposition 6 *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). By Proposition 5, $\mathcal{H}_1$ 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

$$\ell_{P_1}: V=(a-t), \qquad \ell_{Q_1}: U=(a-t),$$
$$\ell_{R_1}: U+(\alpha+1)V+\frac{(\alpha+2)(a+3t)}{3}=0, \qquad \ell_{S_1}: U-\alpha V-\frac{(\alpha-1)(a+3t)}{3}=0.$$

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,

$$\begin{aligned} v_{P_1}(u)=v_{R_1}(u)=v_{S_1}(u)=-1, \quad v_{Q_1}(u)=0,\\ v_{Q_1}(v)=v_{R_1}(v)=v_{S_1}(v)=-1, \quad v_{P_1}(v)=0. \end{aligned} \tag{7}$$

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, we can apply Theorem 3, 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, R_1, and S_1 are the only totally ramified places; all other places are unramified. By Lemma 1, $\mathbb{F}_q$ is the constant field of $F_2=\mathbb{F}_q(x,v)$. The genus is given by

$$\begin{aligned} g_2 &= \sigma g_1 + \frac{\sigma-1}{2}\left(-2+\sum_{P\in\mathbb{P}(\mathbb{K}(\mathcal{H}_1))}(m_P+1)\deg P\right)\\ &= 3\sigma+\frac{\sigma-1}{2}(-2+3(1+1)) = 5\sigma-2. \end{aligned}$$

$\square$

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 $Q_2^1,\ldots,Q_2^\sigma$ the places lying over Q_1.

Proposition 7 *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

$$v_{P_2}(v) = 0, \quad v_{Q_2^i}(v) = -1, \quad v_{R_2}(v) = v_{S_2}(v) = -\sigma. \tag{8}$$

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 our assumptions on σ; in fact, $\sigma = p^{h'}$ with h' odd and $p \equiv 2 (\bmod 3)$ imply that 3 does not divide $\sigma - 1$. Thus, $v_{R_2}((A - \alpha)x) = -1$, and hence

$$v_{R_2}(v - (\rho^\sigma - \rho)) = -1.$$

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, by Theorem 3, $\mathbb{K}(x, y) : \mathbb{K}(x, v)$ is a Galois extension with $[\mathbb{K}(x, y) : \mathbb{K}(x, v)] = \sigma$ and

$$\begin{aligned} g_3 &= \sigma g_2 + \frac{\sigma - 1}{2} \left(-2 + \sum_{P \in \mathbb{P}(\mathbb{K}(x,v))} (m_P + 1) \deg P \right) \\ &= \sigma(5\sigma - 2) + \frac{\sigma - 1}{2} (-2(\sigma - 2)(1 + 1)) = 6\sigma^2 - 2\sigma - 1. \end{aligned}$$

Finally, by Lemma 1, $\mathbb{F}_q$ 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, 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 8 *Let $a, b \in \mathbb{F}_q$ with $b \neq 0$, $b \neq a^4$, and $a \neq t$. The equation*

$$\begin{aligned} &w^2 + w((x^\sigma - x) + (y^\sigma - y) + 4t) + 4t(x^\sigma - x + y^\sigma - y) + 6t^2 \\ &\quad + (x^\sigma - x)(y^\sigma - y) + (x^\sigma - x)^2 + (y^\sigma - y)^2 = 0 \end{aligned} \tag{9}$$

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

$$\theta = w + \frac{1}{2}(x^\sigma - x + y^\sigma - y + 4t)$$

we have $F_4 = F_3(\theta)$. By straightforward computations,

$$\theta^2 = -\frac{3}{4}(u+v)^2 + uv - 2t(u+v) - 2t^2 = -\frac{3}{4}\Big(u - \beta_1 v + (1-\beta_1)t\Big)\Big(u - \beta_2 v + (1-\beta_2)t\Big), \tag{10}$$

where β_1, β_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

$$\begin{aligned} &h_1(\beta_1 V + (\beta_1 - 1)t, V) = 0 \quad \text{if and only if} \quad r(V) \\ &\quad := (3 + 2\beta_1)(V + t)^4 + 2a(3 - \beta_1)(V + t)^3 - b = 0. \end{aligned}$$

The coefficients of $r(V)$ are non-zero by the assumptions on a, b and the characteristic p; as

$$r'(V) = 2(V+t)^2\,[2(3+2\beta_1)V + 3a(3-\beta_1)]\ ,$$

$(u-\beta_1 v+(1-\beta_1)t)$ provides at most one double zero of θ^2 in $\mathbb{K}(u,v)$, so at least two simple zeros; the same holds for the second factor $(u-\beta_2 v+(1-\beta_2)t)$. The two factors have at most one common zero; then, there exists a zero P of θ^2 in $\mathbb{K}(u,v)$ with multiplicity 1, and hence θ^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 θ^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 (10), θ^2 has valuation -2 at P_1, Q_1, R_1, and S_1; hence,

$$v_{P_3^i}(\theta^2) = v_{Q_3^i}(\theta^2) = -2\sigma\ , \quad v_{R_3}(\theta^2) = v_{S_3}(\theta^2) = -2\sigma^2 \qquad (i=1,\ldots,\sigma). \tag{11}$$

The number of zeros of θ^2 in $\mathbb{K}(x,y,\theta)$ is σ^2 times the number of its zeros in $\mathbb{K}(u,v)$, so at most $8\sigma^2$. By Theorem 3,

$$\begin{aligned} g_4 &= 1 + 2(g_3-1) + \frac{1}{2}\sum_{P\in\mathbb{P}(\mathbb{K}(x,y))}(2-r_P)\deg P \\ &\le 1 + 2(6\sigma^2-2\sigma-2) + \frac{1}{2}\,8\sigma^2 = 16\sigma^2 - 4\sigma - 3. \end{aligned}$$

Finally, by Lemma 1, $\mathbb{F}_q$ is the constant field of $\mathbb{F}_q(x,y,\theta) = F_4$. □

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 9 *Let $a, b \in \mathbb{F}_q$ with $b \ne 0$, $b \ne a^4$, and $a \ne t$. The equation $z^\sigma - z = w$ defines an extension $F_5 = F_4(z)$ with genus $g_5 \le 30\sigma^3 - 12\sigma^2 - 4\sigma + 1$ whose field of constants is $\mathbb{F}_q$.*

Proof Arguing as in the proof of Proposition 8, 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 θ^2 with odd multiplicity, and

$$g(\mathbb{K}(u,v,\theta)) \le 1 + 2(g(\mathbb{K}(u,v)) - 1) + \frac{1}{2}\cdot 8 = 9.$$

Let $\tilde{P}_1^j$, $\tilde{Q}_1^j$, $\tilde{R}_1^j$, and $\tilde{S}_1^j$ $(j=1,2)$ be the places of $\mathbb{K}(u,v,\theta)$ lying over P_1, Q_1, R_1, and S_1. As $v_{\tilde{P}_1^j}(\theta^2) = -2$, we have $v_{\tilde{P}_1^j}(\theta) = -1 = v_{\tilde{P}_1^j}(u)$ and we can write

$$\theta = ku + \Phi,$$

for some $k \in \mathbb{K}$, $\Phi \in \mathbb{K}(u,v,\theta)$ with $v_{\tilde{P}_1^j}(\Phi) \ge 0$. Thus,

$$v_{\tilde{P}_1^j}\left(\theta^2 - k^2u^2\right) = v_{\tilde{P}_1^j}\left(2ku\Phi + \Phi^2\right) \ge -1.$$

On the other hand, from (10) 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 $v_{\tilde{P}_1^j}\left(u^2\right) = -2$, whereas, by (7), the other terms have valuation greater than or equal to -1 at $\tilde{P}_1^j$. Therefore the coefficient $\left(-3/4 - k^2\right)$ must vanish. By our assumptions on σ,

-3 is not a square in $\mathbb{F}_\sigma$ (see Lemma 4.5 in [9]). Then $k \notin \mathbb{F}_\sigma$, and there exists a σ-th root $e_\sigma \in \mathbb{K}$ of k with $e_\sigma \neq k$. Let $\rho = e_\sigma x$; then

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

$\mathbb{K}(x, y, \theta)$ 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,

$$v_{P_4^{i,j}}(\theta - (\rho^\sigma - \rho)) = -1. \tag{12}$$

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 (12),

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

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 [8] 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 σ. Also, by Lemma 1, $\mathbb{F}_q$ 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 [21]),

$$\begin{aligned}g_5 \leq{} &[\mathbb{K}(x, y, z) : \mathbb{K}(x, y)] \cdot g(\mathbb{K}(x, y)) + [\mathbb{K}(x, y, z) : \mathbb{K}(u, v, z)] \cdot g(\mathbb{K}(u, v, z)) \\ &+ ([\mathbb{K}(x, y, z) : \mathbb{K}(x, y)] - 1) \cdot ([\mathbb{K}(x, y, z) : \mathbb{K}(u, v, z)] - 1)\,.\end{aligned}$$

We have

$$\begin{aligned}&[\mathbb{K}(x, y, z) : \mathbb{K}(x, y)] = [\mathbb{K}(x, y, z) : \mathbb{K}(x, y, \theta)] \cdot [\mathbb{K}(x, y, \theta) : \mathbb{K}(x, y)] = 2\sigma\,, \\ &g(\mathbb{K}(x, y)) = 6\sigma^2 - 2\sigma - 1.\end{aligned}$$

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 $\mathbb{K}(x, v, z)$, we have that $\{x^i y^j \mid i, j = 1, \ldots, \sigma\}$ 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 $\mathbb{K}(u, v, \theta) : \mathbb{K}(u, v)$, we have that θ^2 has valuation -2 at the places lying over them; hence,

$$v_{\tilde{P}_1^j}(\theta) = v_{\tilde{Q}_1^j}(\theta) = v_{\tilde{R}_1^j}(\theta) = v_{\tilde{S}_1^j}(\theta) = -1\,, \quad \text{for } j = 1, 2\,,$$

whereas θ 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 σ and

$$g(\mathbb{K}(u, v, z)) = \sigma\, g(\mathbb{K}(u, v, \theta)) + \frac{\sigma - 1}{2}\left(-2 + \sum_{P \in \mathbb{P}(\mathbb{K}(u,v,\theta))} (m_P + 1) \deg P\right)$$
$$\leq 9\sigma + \frac{\sigma - 1}{2}(-2 + 8(1 + 1)) = 16\sigma - 7.$$

Therefore,

$$g_5 \leq 2\sigma(6\sigma^2 - 2\sigma - 1) + \sigma^2(16\sigma - 7) + (2\sigma - 1)(\sigma^2 - 1) = 30\sigma^3 - 12\sigma^2 - 4\sigma + 1.$$

□

Theorem 5 *Let $\mathcal{K}_t$ as in (2). If $q \geq 3600\,\sigma^6$ 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 $a \neq t$ and $b \neq 0$. 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 σ; then, by Theorem 3.1.11 in [21], $x^\sigma - x$ 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,

$$Z_1 \leq \sigma(2\sigma + 4) + \sigma(2\sigma + 4) + \sigma(4\sigma + 4) = 8\sigma^2 + 12\sigma.$$

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 Theorem 3.1.11 in [21],

$$\deg(x - y - \lambda)_\infty = 4 \cdot [F_5 : F_1] = 8\sigma^3 \quad \text{for all} \quad \lambda \in \mathbb{F}_\sigma;$$

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 Theorem 4 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 1, the point P is collinear with three distinct points in $\mathcal{K}_t$.

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. 9. Arguing as above, $\mathcal{K}_{t'}$ covers the point P. But clearly $\mathcal{K}_{t'} = \mathcal{K}_t$, and the assertion follows. □

5 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 1 Let G be a finite abelian group and let $\mathcal{T}$ be a subset of G. If

$$y_1 + y_2 + y_3 + y_4 \neq 0 \quad \text{for all} \quad y_1, y_2, y_3, y_4 \in \mathcal{T},$$

then $\mathcal{T}$ is said to be a *4-independent subset* of G. An element $g \in G$ is *covered* by $\mathcal{T}$ if either $g \in \mathcal{T}$ or

$$\text{there exist } \; y_1, y_2, y_3 \in \mathcal{T} \text{ such that } \; y_1 + y_2 + y_3 + g = 0.$$

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,

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

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 10 *Let $p \geq 29$ be a prime, with $p \equiv 1$ mod 4. Then*

$$\mathcal{T} = \{-1, 2\} \cup \left[4, \frac{p-1}{4}\right]$$

is a 4-independent subset of $\mathbb{Z}_p$ 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

$$\begin{aligned} 3^\wedge\mathcal{T} &= \{-3\} \cup (-2 + \mathcal{T}^*) \cup (-1 + 2^\wedge\mathcal{T}^*) \cup 3^\wedge\mathcal{T}^* \\ &= \{-3\} \cup \{0\} \cup \left[2, \frac{p-9}{4}\right] \cup \{3\} \cup \left[5, \frac{p-3}{2}\right] \cup \{6\} \cup \left[8, 3\frac{p-1}{4}\right] \\ &= \{-3, 0\} \cup \left[2, 3\frac{p-1}{4}\right]. \end{aligned}$$

Hence, the set of covered elements contains

$$-3^\wedge\mathcal{T} = \{0, 3\} \cup \left[\frac{p-1}{4} + 1, p-2\right].$$

Note that the non-covered element 1 cannot be added to $\mathcal{T}$ since $1 + 1 - 1 - 1 = 0$. □

Proposition 11 *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 in Proposition 10,

$$\begin{aligned}
3^\wedge\mathcal{T} &= \{y_1 + y_2 + y_3 \mid y_1, y_2, y_3 \in \mathcal{T}\} = \{-3\} \cup (-2 + \mathcal{T}^*) \cup (-1 + 2^\wedge\mathcal{T}^*) \cup 3^\wedge\mathcal{T}^* \\
&= \{-3\} \cup \{0\} \cup \left[2, \frac{p-11}{4}\right] \cup \{3\} \cup \left[5, \frac{p-5}{2}\right] \cup \{6\} \cup \left[8, 3\frac{p-3}{4}\right] \\
&= \{-3, 0\} \cup \left[2, 3\frac{p-3}{4}\right].
\end{aligned}$$

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

$$\begin{aligned}
1 + 1 - 1 - 1 = 0, \qquad & \frac{p+1}{4} + \frac{p+1}{4} + \frac{p+1}{4} + \frac{p-3}{4} = p, \\
& \frac{p+5}{4} + \frac{p+5}{4} + \frac{p-3}{4} + \frac{p-7}{4} = p.
\end{aligned}$$

□

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

$$\mathcal{T} = \mathcal{T}_1 \cup \mathcal{T}_2 \cup \mathcal{T}_3, \tag{13}$$

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 12 *Let $h' \geq 3$ and let $\mathcal{T}$ be as in (13). 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 $2\left(p^{\frac{h'+1}{2}} - p^{\frac{h'-1}{2}}\right)$ 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 $\mathcal{T}$. □

6 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 (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 1, the three points P, P_1, and P_2 are collinear if and only if

$$(x^\sigma - x + t_1)^2 + (y^\sigma - y + t_2)^2 + (x^\sigma - x + t_1)(y^\sigma - y + t_2) + w(x^\sigma - x + t_1 + y^\sigma - y + t_2) + w^2 = 0. \tag{14}$$

Proposition 13 *Equation 14, 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 Γ_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 Γ_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 Γ_0 is an irreducible conic. Let $L_0 = \mathbb{F}_q(u, v)$ be the function field of Γ_0, where $f_0(u, v) = 0$. Since Γ_0 is non-singular, places of $\mathbb{K}(u, v)$ can be identified with points of Γ_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 places centered at affine points of Γ_0. Then, by Theorem 3, $\mathbb{K}(x, v) : \mathbb{K}(u, v)$ with $u = x^\sigma - x$ is a generalized Artin–Schreier extension, and

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

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, $\mathbb{F}_q$ is the constant field of $\mathbb{F}_q(x, v)$.

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 σ, 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 $v_{\overline{S}_1}(v - (\rho^\sigma - \rho)) = -1$. At the places centered at affine points it is sufficient to take $\rho = 0$. Then, by Theorem 3, $\mathbb{K}(x, y) : \mathbb{K}(x, v)$

is a Galois 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,

$$\begin{aligned} g &= \sigma\, g(\mathbb{K}(x,v)) + \frac{\sigma-1}{2}\left(-2+\sum_{P\in\mathbb{P}(\mathbb{K}(x,v))}(m_P+1)\deg P\right)\\ &= \sigma(\sigma-1)+\frac{\sigma-1}{2}(-2+4)=\sigma^2-1. \end{aligned}$$

By Lemma 1, $\mathbb{F}_q$ is the constant field of L. □

Proposition 14 *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 (14) 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 $L : L_0$; 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 $L : L_0$; then, by Theorem 3.1.11 in [21],

$$\deg(x-y-\lambda)_\infty = 2\cdot[L:L_0] = 2\sigma^2 \quad \text{for all} \quad \lambda\in\mathbb{F}_\sigma\,;$$

hence, $Z \leq 2\sigma^3$ holds.

Therefore, if the number N_q of $\mathbb{F}_q$-rational places of Γ is greater than $2\sigma^3 + 2$, 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 15 *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 14, 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 $(i = 1, \ldots, 9)$. Arguing as in the proof of Proposition 14, 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 (1). Let

$$\mathcal{K}_{\mathcal{T}} = \bigcup_{M+t\in\mathcal{T}} \mathcal{K}_t. \tag{15}$$

Proposition 16 *The set $\mathcal{K}_{\mathcal{T}}$ is a $(k,3)$-arc.*

Proof By Proposition 2, 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-indipendent subset of $\mathbb{F}_q/M$. □

Proposition 17 *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 15, 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 2,

$$t_P + t_1 + t_2 + t_3' \in M.$$

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 is proved. □

Theorem 6 *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 (15). Assume $q \geq 3600\,\sigma^6$. Then there exists a complete $(k,3)$-arc $\mathcal{K}$ with $\mathcal{K}_{\mathcal{T}} \subset \mathcal{K} \subset \mathcal{Q}$ of size at most*

$$(n+m)\frac{q}{\sigma} + 6.$$

Proof Fix a coset $M+t$ in $\mathcal{T}$. By Theorem 5, 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 17, 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 1. Identify the additive groups $\mathbb{Z}_p^{h'}$ and $\mathbb{F}_q/M$. From Propositions 10, 11, and 12 the following values of n and m occur in Theorem 6:

- for $\sigma = p$, $p \equiv 1 \mod 4$, $p \geq 29$,

$$n = \frac{p-5}{4} \quad \text{and} \quad m = 1;$$

– for $\sigma = p$, $p \equiv 3 \mod 4$, $p > 29$,

$$n = \frac{p-7}{4} \quad \text{and} \quad m = 3\,;$$

– for $\sigma \geq p^3$, then

$$n = 2p^{\frac{h'-1}{2}} + p - 4\,, \qquad m = 2\big(p^{\frac{h'+1}{2}} - p^{\frac{h'-1}{2}}\big).$$

Acknowledgments This research was supported by the Italian Ministry MIUR, PRIN 2012 *Strutture Geometriche, Combinatoria e loro Applicazioni* and by INdAM. The first author acknowledges the support of the European Community under a Marie-Curie Intra-European Fellowship (FACE Project Number 626511).

References

1. Anbar N., Giulietti M.: Bicovering arcs and small complete caps from elliptic curves. J. Algebr. Comb. **38**, 371–392 (2013). doi:10.1007/s10801-012-0407-8.
2. Anbar N., Bartoli D., Giulietti M., Platoni I.: Small complete caps from singular cubics. J. Comb. Des. **22**(10), 409–424 (2014). doi:10.1002/jcd.21366.
3. Anbar N., Bartoli D., Giulietti M., Platoni I.: Small complete caps from singular cubics. II. J. Algebr. Comb (to appear). (2014). doi:10.1007/s10801-014-0532-7 (published online May).
4. Bartoli D., Marcugini S., Pambianco F.: The non-existence of some NMDS codes and the extremal sizes of complete $(n, 3)$-arcs in PG(2,16). Des. Codes Cryptogr. **72**(1), 129–134 (2014). doi:10.1007/s10623-013-9837-0.
5. Coolsaet K., Sticker H.: The complete $(k, 3)$-arcs of PG$(2, q)$, $q \leq 13$. J. Comb. Des. **20**, 89–111 (2012). doi:10.1002/jcd.20293.
6. Dodunekov S., Landjev I.: Near-MDS codes. J. Geom. **54**, 30–43 (1995).
7. Dodunekov S., Landjev I.: Near-MDS codes over some small fields. Discret. Math. **213**, 55–65 (2000).
8. Garcia A., Stichtenoth H.: Elementary Abelian p-extensions of algebraic function fields. Manuscr. Math. **72**, 67–79 (1991).
9. Giulietti M.: On plane arcs contained in cubic curves. Finite Fields Appl. **8**, 69–90 (2002).
10. Giulietti M., Pasticci F.: On the completeness of certain n-tracks arising from elliptic curves. Finite Fields Appl. **13**(4), 988–1000 (2007).
11. Giulietti M., Pambianco F., Torres F., Ughi E.: On complete arcs arising from plane curves. Des. Codes Cryptogr. **25**, 237–246 (2002).
12. Hamilton N., Penttila, T.: Sets of Type (a, b) From Subgroups of $\Gamma L(1, p^R)$. J. Algebr. Comb. **13**, 67–76 (2001).
13. Hirschfeld J.W.P.: Projective Geometries over Finite Fields, 2nd edn. Oxford University Press, Oxford (1998).
14. Hirschfeld J.W.P.: Algebraic curves, arcs, and caps over finite fields. In: Quaderni del Dipartimento di Matematica dell' Università del Salento 5, Dipartimento di Matematica, Università del Salento, Lecce, (1986).
15. Hirschfeld J.W.P., Storme L.: The packing problem in statistics, coding theory and finite projective spaces. J. Stat. Plan. Inference. **72**(1–2), 355–380 (1998). R. C. Bose Memorial Conference (Fort Collins, CO, 1995).
16. 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, vol. 3, pp. 201–246. Kluwer Academic Publishers, Boston (2001).
17. Hirschfeld J.W.P., Voloch J.F.: The characterization of elliptic curves over finite fields. J. Austral. Math. Soc. **45**, 275–286 (1988).
18. Lombardo-Radice L.: Sul problema dei k-archi completi in $S_{2,q}$ ($q = p^t$, p primo dispari). Boll. Unione Mat. Ital. **3**(11), 178–181 (1956).
19. Marcugini S., Milani A., Pambianco F.: Classification of the $(n, 3)$-arcs in PG$(2, 7)$. J. Geom. **80**(1–2), 179–184 (2004).
20. 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).

21. Stichtenoth H.: Algebraic Function Fields and Codes. Graduate Texts in Mathematics, vol. 254, 2nd edn. Springer, Berlin (2009).
22. Szőnyi T.: Complete arcs in galois planes: a survey. In: Quaderni del Seminario di Geometrie Combinatorie, vol. 94, Dipartimento di Matematica G. Castelnuovo, Università degli Studi di Roma La Sapienza, Roma (1989).
23. Szőnyi T.: Some applications of algebraic curves in finite geometry and combinatorics. In: Surveys in combinatorics, London, 1997. London Mathematical Society Lecture Note Series, vol. 241, pp. 197–236. Cambridge University Press, Cambridge (1997).
24. Tallini Scafati M.: Graphic curves on a Galois plane. In: Atti del Convegno di Geometria Combinatoria e sue Applicazioni, Perugia, pp. 413–419 (1970).