Elation KM-arcs

Maarten De Boeck [*] Geertrui Van de Voorde [†]

Abstract

In this paper, we study *KM-arcs* in $\mathrm{PG}(2,q)$, the Desarguesian projective plane of order q. A KM-arc $\mathcal{A}$ of type t is a natural generalisation of a *hyperoval*: it is a set of $q+t$ points in $\mathrm{PG}(2,q)$ such that every line of $\mathrm{PG}(2,q)$ meets $\mathcal{A}$ in $0, 2$ or t points.

We study a particular class of KM-arcs, namely, *elation* KM-arcs. These KM-arcs are highly symmetrical and moreover, many of the known examples are elation KM-arcs. We provide an algebraic framework and show that all elation KM-arcs of type $q/4$ in $\mathrm{PG}(2,q)$ are translation KM-arcs. Using a result of [2], this concludes the classification problem for elation KM-arcs of type $q/4$.

Furthermore, we construct for all $q = 2^h$, $h > 3$, an infinite family of elation KM-arcs of type $q/8$, and for $q = 2^h$, where $4, 6, 7 \mid h$ an infinite family of KM-arcs of type $q/16$. Both families contain new examples of KM-arcs.

Keywords: KM-arc, $(0,2,t)$-arc, set of even type, elation arc, translation arc

MSC 2010 codes: 51E20, 51E21

1 Introduction and definitions

Point sets in $\mathrm{PG}(2,q)$, the Desarguesian projective plane over the finite field $\mathbb{F}_q$ of order q, that have few different intersections sizes with lines have been a research subject throughout the last decades. A point set $\mathcal{S}$ of *type* $(i_1,\dots,i_m)$ in $\mathrm{PG}(2,q)$ is a point set such that for every line in $\mathrm{PG}(2,q)$ the intersection size $\ell \cap \mathcal{S}$ equals i_j for some j and such that each value i_j occurs as intersection size for some line. In [9] point sets of type $(0,2,q/2)$ of size $\frac{3q}{2}$ were studied. This led to the following generalisation by Korchmáros and Mazzocca in [6].

Definition 1.1. A *KM-arc of type* t in $\mathrm{PG}(2,q)$ is a point set of type $(0,2,t)$ with size $q+t$. A line containing i of its points is called an i*-secant*.

Originally these KM-arcs were denoted as $(q+t)$*-arcs of type* $(0,2,t)$ [6] or $(q+t,t)$*-arcs of type* $(0,2,t)$ [3] but in honour of Korchmáros and Mazzocca, the notation 'KM-arcs' was introduced in [14]. KM-arcs of type $t=2$ are *hyperovals*, which have their own theory; the classification of hyperovals seems far out of reach at this moment. KM-arcs of type $t=q$ in $\mathrm{PG}(2,q)$ on the other hand, are easily seen to be the symmetric difference of two lines. For KM-arcs of type $2<t<q$, further combinatorial information and conditions on t and q can be deduced. The following results were obtained in [3, Theorem 2.5] and [6, Proposition 2.1].

Theorem 1.2. *If $\mathcal{A}$ is a KM-arc of type t in $\mathrm{PG}(2,q)$, $2<t<q$, then*

- *q is even;*
- *t is a divisor of q;*
- *there are $q/t+1$ different t-secants to $\mathcal{A}$, and they are concurrent.*

If $\mathcal{A}$ is a KM-arc of type $t>2$, then the point contained in all t-secants to $\mathcal{A}$ is called the t*-nucleus* of $\mathcal{A}$.

The main questions in the study of the KM-arcs are for which values of q and t, a KM-arc of type t in $\mathrm{PG}(2,q)$ exists, and which nonequivalent KM-arcs of type t in $\mathrm{PG}(2,q)$ exist for given admissible q and t.

Recall that every element of $\mathrm{P\Gamma L}(3,q)$ defines a *collineation* of the projective plane $\mathrm{PG}(2,q)$ and vice versa, where a collineation is an incidence preserving mapping. KM-arcs are studied up to $\mathrm{P\Gamma L}$-equivalence. *Elations*

[*] This author is supported by the BOF (Special Research Fund) of Ghent University

[†] This author is a postdoctoral fellow of the Research Foundation – Flanders (FWO).

of a projective plane are particular collineations that will play an important role in this paper. An *elation* with axis the line ℓ and centre the point R on ℓ is a collineation which fixes the points of ℓ and stabilises the lines through the centre R. We see that the set of all elations with a fixed centre and a fixed axis form a subgroup of $\mathrm{P\Gamma L}$.

A KM-arc is a *translation* KM-arc with translation line ℓ_∞ if the group of all elations with axis ℓ_∞ that stabilise $\mathcal{A}$, acts transitively on the points of $\mathcal{A} \setminus \ell_\infty$ (see [6]).

Definition 1.3. Let $\mathcal{A}$ be a KM-arc of type $t > 2$ in $\mathrm{PG}(2, q)$ with t-nucleus N. Then $\mathcal{A}$ is an *elation KM-arc* with elation line ℓ_∞ if and only if for every t-secant $\ell \neq \ell_\infty$ to $\mathcal{A}$, the group of elations with axis ℓ_∞ that stabilise $\mathcal{A}$ acts transitively on the points of ℓ.

A hyperoval (KM-arc of type 2) $\mathcal{H}$ in $\mathrm{PG}(2, q)$ is called an *elation hyperoval* with elation line ℓ_∞ if a non-trivial elation with axis ℓ_∞ which stabilises $\mathcal{H}$ exists.

It is immediate that all collineations which stabilise a KM-arc of type $t > 2$, fix its t-nucleus. Hence, the t-nucleus of a KM-arc of type t lies on the elation line since all fixed points of an elation lie on the axis. Moreover the t-nucleus will be the centre of all elations stabilising the t-secants. So, for an elation KM-arc $\mathcal{A}$ of type $t > 2$ the group of elations with axis the elation line and centre the t-nucleus, stabilising $\mathcal{A}$, acts sharply transitively on the points of $\mathcal{A} \cap \ell$ with ℓ an arbitrary t-secant.

For hyperovals there is no concurrency point of all 2-secants. Hence, for elation hyperovals, we have presented a slightly modified version of the definition of an elation KM-arc. We will see in Lemmas 2.1 and 2.2 that we can work with both definitions in the same way. Considering that hyperovals are KM-arcs we will call elation hyperovals also elation KM-arcs

It follows from the definitions that every translation KM-arc is an elation KM-arc. The following theorem was shown for translation KM-arcs in [6, Prop. 6.2]. The proof presented there however cannot be generalised to the case of elation KM-arcs.

Theorem 1.4. *Let $\mathcal{A}$ be an elation KM-arc of type t in $\mathrm{PG}(2, q)$, $2 \leq t < q$, with elation line m, then m is a t-secant to $\mathcal{A}$.*

Proof. Recall that any collineation that stabilises $\mathcal{A}$ has to fix the t-nucleus N of $\mathcal{A}$ if $t > 2$ and hence, that the elation line m is a line through N. If $t = 2$, we define N as the centre of the given non-trivial elation that stabilises $\mathcal{A}$.

Suppose that the elation line m is not a t-secant and let G be the group of elations with centre N and axis m stabilising $\mathcal{A}$. Then G acts transitively on the points of $\mathcal{A} \cap \ell$ for every t-secant ℓ. Note that G has size t.

Let ℓ_1 and ℓ_2 be two t-secants of $\mathcal{A}$ trough N (recall that all t-secants contain N if $t > 2$), and let $P \in \ell_1$ and $Q \in \ell_2$ be two points of $\mathcal{A}$. Denote the intersection $\langle P, Q\rangle \cap m$ by R. The orbit of the line $\langle P, Q\rangle$ under G is a set of t lines through R. Moreover, every line through R which meets $\mathcal{A}$ in 2 points, is contained in an orbit of G of length t. Hence, the number of 2-secants through R is a multiple of t. Given the fact that $\mathcal{A}$ has $q + t$ points and every line through R meets $\mathcal{A}$ in 0 or 2 points, we know that there are $\frac{q+t}{2}$ distinct 2-secants to $\mathcal{A}$ through R. We have that $\frac{q+t}{2} = t\left(\frac{q}{2t} + \frac{1}{2}\right)$, and since $q = 2^h$ and $t = 2^j$ for some $j < h$, we have that $2t \mid q$. Hence, the number of 2-secants through R, $(q + t)/2$, is not a multiple of t, a contradiction. □

We first introduce the 'classical' examples constructed by Korchmáros-Mazzocca and Gács-Weiner and then give a survey of the known results in Table 1.

Construction 1. [6] Let $q = 2^h$ and $q' = 2^{h-i}$, with $h - i \mid h$, and let L be the relative trace function from $\mathbb{F}_q$ to $\mathbb{F}_{q'}$. Let g be an o-polynomial in $\mathbb{F}_{q'}$, i.e. $(1, g(x), x)$ is the affine part of a hyperoval (KM-arc of type 2) in $\mathrm{PG}(2, q')$ containing $(0, 1, 0)$ and $(0, 0, 1)$. Then, the point set $\{(1, g(L(x)), x) \mid x \in \mathbb{F}_q\}$ can uniquely be extended to a KM-arc $\mathcal{A}_{km}$ of type 2^i in $\mathrm{PG}(2, q)$. It has 2^i-nucleus $(0, 0, 1)$.

We will show in Lemma 2.3 that all the KM-arcs arising from Construction 1 are elation KM-arcs. It was already shown in [6, Proposition 6.4] that a KM-arc in $\mathrm{PG}(2, q)$ constructed in this way is a translation KM-arc if and only if g is the o-polynomial $x \mapsto x^{2^n}$, for an integer n admitting $\gcd(h', n) = 1$. Note that g is the o-polynomial corresponding to a translation hyperoval in $\mathrm{PG}(2, q')$.

We now recall the three different constructions from Gács and Weiner [3].

Construction 2. [3, Construction 3.4] Let I be a direct complement of $\mathbb{F}_q$ in the additive group of $\mathbb{F}_{q^h}$, $h > 1$. Let H be a hyperoval or a KM-arc of type t with affine part $\{(1, x_k, y_k) : x_k, y_k \in \mathbb{F}_q\} \subseteq \mathrm{PG}(2, q)$. Construct the following point set in $\mathrm{AG}(2, q^h)$:

$$J = \{(1, x_k, y_k + i) \mid (1, x_k, y_k) \in H, i \in I\} .$$

(A) If H is a hyperoval and $(0,0,1) \in H$, then J can be uniquely extended to a KM-arc of type q^{h-1} in $\mathrm{PG}(2,q^h)$. This KM-arc has q^{h-1}-nucleus $(0,0,1)$.

(B) if H is a hyperoval and $(0,0,1) \notin H$, then J can be uniquely extended to a KM-arc of type $2q^{h-1}$ in $\mathrm{PG}(2,q^h)$. This KM-arc has $2q^{h-1}$-nucleus $(0,0,1)$.

(C) If H is a KM-arc of type t and $(0,0,1)$ is the t-nucleus of H, then J can be uniquely extended to a KM-arc of type tq^{h-1} in $\mathrm{PG}(2,q^h)$. This KM-arc has tq^{h-1}-nucleus $(0,0,1)$.

Note that in construction (A) the hyperoval H contains one more point on $X=0$ in $\mathrm{PG}(2,q)$, next to $(0,0,1)$. Hence, to extend J to a KM-arc of type q^{h-1} we need q^{h-1} points on $X=0$ in $\mathrm{PG}(2,q^h)$. In constructions (B) and (C) the KM-arc H of type t, which can be a hyperoval, can either be completely contained in the affine part of $\mathrm{PG}(2,q)$ or else have t points on $X=0$. In the latter case, to extend J to a KM-arc of type tq^{h-1} we need tq^{h-1} points on $X=0$ in $\mathrm{PG}(2,q^h)$. In the former case no points need to be added.

Remark 1.5. It was already noted by Gács and Weiner [3, p.138] that Construction 2 (A) is equivalent to Construction 1, where the o-polynomial g used in Construction 1 is the o-polynomial of the hyperoval H used in Construction 2 (A).

Remark 1.6. If I and I' are different direct complements of $\mathbb{F}_q$ in $\mathbb{F}_{q^h}$, then the affine point set $J = \{(1,x_k,y_k+i) : (1,x_k,y_k) \in H, i \in I\}$ and the affine point set $J' = \{(1,x_k,y_k+i) : (1,x_k,y_k) \in H, i \in I'\}$ in $\mathrm{PG}(2,q)$ are PGL-equivalent. To see this, we will see below that there is an $\mathbb{F}_q$-linear map τ acting on $\mathbb{F}_{q^h}$ which fixes $\mathbb{F}_q$ but maps I onto I'. The map $\phi_\tau : (1,x,y) \mapsto (1,x,\tau(y))$ then induces a collineation of $\mathrm{PG}(2,q^h)$ mapping the point set J onto J', since $\phi_\tau(1,x_k,y_k+I) = (1,x_k,\tau(y_k+I)) = (1,x_k,y_k+\tau(I)) = (1,x_k,y_k+I')$.

To see that there exists an $\mathbb{F}_q$-linear map τ acting on $\mathbb{F}_{q^h}$ which fixes $\mathbb{F}_q$ but maps I onto I', consider $\mathbb{F}_{q^h}$ as $\mathbb{F}_q^h$, and further consider $\mathbb{F}_q^h$ as a projective space $\mathrm{PG}(h-1,q)$. Then we need to find a collineation fixing the point V corresponding to $\mathbb{F}_q$ and mapping π_1 onto π_2 with π_1 and π_2 two different hyperplanes not through V. Clearly, there is an elation with axis $\langle V, \pi_1 \cap \pi_2\rangle$ which fulfils the requirements.

This paper is organised as follows. In Lemma 2.3, we will see that the KM-arcs constructed from Construction 2 (A) are always elation KM-arcs. We will prove in Lemma 2.4 and Theorem 2.5 that a KM-arc obtained in Construction 2 (B) and (C) is an elation KM-arc if and only if the KM-arc (or hyperoval) started with is an elation KM-arc with t-nucleus $(0,0,1)$ (or is an elation hyperoval stabilised by an elation with centre $(0,0,1)$).

q	t	Condition	Comments	Reference
2^h	2^i	$h-i \mid h$	elation, see Lemma 2.3	[6] (see Constr. 1 and 2 (A))
2^h	2^{i+1}	$h-i \mid h$	some elation, see Lemma 2.4	[3] (see Constr. 2 (B))
2^h	2^{i+m}	$h-i \mid h$, a KM-arc of type 2^m in $\mathrm{PG}(2,2^{h-i})$ exists	some elation, see Lemma 2.4	[3] (see Constr. 2 (C))
2^h	2^{h-1}		translation (all PGL-equivalent)	[2, 14]
2^h	2^{h-2}	$h \geq 3$	translation [2] non-translation elation iff translation	[14] [2] See Section 3
2^h	2^{h-3}	$h \geq 4$	elation, **new family**	See Section 4
32	4		one elation, see Remark 4.13	[5], [16]
2^h	2^{h-4}	$4 \mid h,\ 6 \mid h,$ or $7 \mid h$	elation, **new family for** $7 \mid h$	See Section 5

Table 1: An overview of the known KM-arcs of type t in $\mathrm{PG}(2,q)$

We have seen that every translation KM-arc is an elation KM-arc, but the converse does not necessarily hold. For KM-arcs of type $q/4$ in $\mathrm{PG}(2,q)$ however, we will show in Section 3 that every elation KM-arc is necessarily a translation KM-arc, which brings us to the full classification of elation KM-arcs of type $q/4$ in Theorem 3.12.

The other sections of this paper are devoted to the construction of new examples of KM-arcs; we present a family of elation KM-arcs of type $q/8$ for all values of $q=2^h$ in Section 4 and a family of elation KM-arcs of type $q/16$ for $q=2^h$, with h a multiple of 4, 6 or 7, in Section 5.

2 Elation KM-arcs: an algebraic approach

In the following lemma, we show that the *affine point set* of an elation KM-arc (i.e. the set of points not lying on the elation line) has a convenient algebraic description.

Lemma 2.1. *If $\mathcal{A}$ is an elation KM-arc of type $t > 2$ in $\mathrm{PG}(2,q)$, $q = 2^h$, with elation line $\ell_\infty : X = 0$ and t-nucleus $N(0,0,1)$, then there is an additive subgroup S of size t in $\mathbb{F}_q$, such that for any $\alpha \in \mathbb{F}_q$ the set $\{z \mid (1,\alpha,z) \in \mathcal{A}\}$ is either empty or a coset of S. Vice versa, if for a KM-arc $\mathcal{A}$ there is an additive subgroup S of size t in $\mathbb{F}_q$, such that for any $\alpha \in \mathbb{F}_q$ the set $\{z \mid (1,\alpha,z) \in \mathcal{A}\}$ is either empty or a coset of S, then $\mathcal{A}$ is an elation KM-arc with elation line $X = 0$ and t-nucleus $(0,0,1)$.*

Proof. Let $\mathcal{A}$ be an elation KM-arc of type t in $\mathrm{PG}(2,q)$, $q = 2^h$, with elation line $\ell_\infty : X = 0$ and t-nucleus $N(0,0,1)$. The t-secants, different from ℓ_∞, are of the form $Y = \alpha X$ for some $\alpha \in \mathbb{F}_q$. The group E of elations with centre N and axis ℓ_∞ consists of the elations induced by all matrices of the form $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \mu & 0 & 1 \end{smallmatrix}\right)$, where $\mu \in \mathbb{F}_q$. Here, the points are represented as column vectors, and matrices are acting from the left. It is straightforward to check that a set T is an additive subgroup of $\mathbb{F}_q$ if and only if the set $\psi(T)$ of elations corresponding to the matrices in $\left\{\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \nu & 0 & 1 \end{smallmatrix}\right) \mid \nu \in T\right\}$ is a subgroup of E. The orbit of a point $(1,x,y)$ under the action of $\psi(T)$ is the point set $\{(1,x,\nu+y) \mid \nu \in T\}$.

If $\mathcal{A}$ is an elation KM-arc, the orbit of the point $(1,\alpha_1,\beta_1) \in \mathcal{A}$ under the subgroup $E_{\mathcal{A}}$ of E stabilising $\mathcal{A}$ is exactly the set of t points of $\mathcal{A}$ on the t-secant $\ell : Y = \alpha_1 X$. Let S be the additive subgroup of $\mathbb{F}_q$ such that $\psi(S) = E_{\mathcal{A}}$. This implies that the set of points on $\ell \cap \mathcal{A}$ equals $\{(1,\alpha_1,\tau+\beta_1) \mid \tau \in S\}$.

Vice versa, we assume that S is an additive subgroup of size t in $\mathbb{F}_q$, such that for any $\alpha \in \mathbb{F}_q$ the set $\{z \mid (1,\alpha,z) \in \mathcal{A}\}$ is either empty or a coset of S. Let G be the group of elations induced by the matrices of the form $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \mu & 0 & 1 \end{smallmatrix}\right)$, where $\mu \in S$. Then G has size t and acts transitively on the set of points $\mathcal{A} \cap \ell$ with $\ell : Y = \alpha X$ a t-secant of $\mathcal{A}$, for any $\alpha \in \mathbb{F}_q$. This means exactly that $\mathcal{A}$ is an elation KM-arc with elation line $X = 0$ and t-nucleus $(0,0,1)$. □

For the hyperoval case we have a similar result.

Lemma 2.2. *If $\mathcal{H}$ is a hyperoval in $\mathrm{PG}(2,q)$, $q = 2^h$, that is stabilised by a non-trivial elation with elation line $\ell_\infty : X = 0$ and centre $N(0,0,1)$, then there is an additive subgroup S of size 2 in $\mathbb{F}_q$, such that for any $\alpha \in \mathbb{F}_q$ the set $\{z \mid (1,\alpha,z) \in \mathcal{H}\}$ is either empty or a coset of S. Vice versa, if for a hyperoval $\mathcal{H}$ there is an additive subgroup S of size 2 in $\mathbb{F}_q$, such that for any $\alpha \in \mathbb{F}_q$ the set $\{z \mid (1,\alpha,z) \in \mathcal{H}\}$ is either empty or a coset of S, then $\mathcal{H}$ is stabilised by a nontrivial elation with elation line $X = 0$ and centre $(0,0,1)$.*

Proof. This proof is similar to the proof of Lemma 2.1, with the 2-secants through the centre taking the place of the t-secants, and E the group consisting of the one non-trivial elation that stabilises $\mathcal{H}$ together with the trivial collineation. □

Now we check whether the known constructions give rise to elation KM-arcs. First we deal with the family of KM-arcs constructed by Korchmáros and Mazzocca

Lemma 2.3. *All KM-arcs in the family of Korchmáros and Mazzocca (Construction 1, [6]) are elation KM-arcs.*

Proof. Recall that the set of affine points of the KM-arc $\mathcal{A}_{km}$ in $\mathrm{PG}(2,q)$ is $\{(1,g(L(x)),x) \mid x \in \mathbb{F}_q\}$, where g is an o-polynomial in $\mathbb{F}_{q'}$ and L is the relative trace function from $\mathbb{F}_q$ to $\mathbb{F}_{q'}$, with $q' = 2^{h-i}$, $q = 2^h$ and $h - i \mid h$. Define $S = \{x \in \mathbb{F}_q \mid L(x) = 0\}$, then S is an additive subgroup of $\mathbb{F}_q$ of size 2^i. We claim that for every $\alpha \in \mathbb{F}_q$, the set $T_\alpha = \{x \in \mathbb{F}_q \mid g(L(x)) = \alpha\}$ is either empty or a coset of S. First note that $\{g(L(x)) \mid x \in \mathbb{F}_q\} = \mathbb{F}_{q'}$, so T_α is empty if $\alpha \notin \mathbb{F}_{q'}$. If $\alpha \in \mathbb{F}_{q'}$, we can find a $\beta \in \mathbb{F}_q$ such that $g(L(\beta)) = \alpha$. Then $g(L(\beta+s)) = g(L(\beta)+L(s)) = g(L(\beta)) = \alpha$ for all $s \in S$. Since there are exactly $|S|$ solutions x to the equation $g(L(x)) = \alpha$, we know $T_\alpha = \beta + S$. This proves the claim, and hence, by Lemma 2.1, the statement. □

Now we check the constructions by Gács and Weiner. For additive subgroups G_1 and G_2 of $\mathbb{F}_q$, the additive subgroup generated by subgroups G_1 and G_2 is denoted by $\langle G_1, G_2\rangle$. If $G_2 = \langle x\rangle$, then, by abuse of notation, we also write $\langle G_1, x\rangle$ instead of $\langle G_1, \langle x\rangle\rangle$. Using this convention, we denote the additive subgroup generated by the elements $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{F}_q$ (or equivalently, the $\mathbb{F}_2$-vector subspace spanned by these elements when considering $\mathbb{F}_q$ as a vector space over $\mathbb{F}_2$) by $\langle \alpha_1, \alpha_2, \ldots, \alpha_k\rangle$.

Lemma 2.4. *Let $\mathcal{B}$ be an elation KM-arc in* $\mathrm{PG}(2,q)$ *with elation line* $X=0$ *and t-nucleus* $(0,0,1)$. *Let $\mathcal{A}$ be a KM-arc in* $\mathrm{PG}(2,q^h)$ *that arises from $\mathcal{B}$ as in Construction 2 (C), then $\mathcal{A}$ is an elation KM-arc with elation line* $X=0$ *and* tq^{h-1}*-nucleus* $(0,0,1)$. *Let $\mathcal{H}$ be a hyperoval in* $\mathrm{PG}(2,q)$ *that is stabilised by a non-trivial elation with elation line* $X=0$ *and centre* $(0,1,0)$ *and let $\mathcal{A}'$ be a KM-arc in* $\mathrm{PG}(2,q^h)$ *that arises from $\mathcal{H}$ as in Construction 2 (B), then $\mathcal{A}'$ is an elation KM-arc with elation line* $X=0$ *and* $2q^{h-1}$*-nucleus* $(0,0,1)$.

Proof. Since $\mathcal{B}$ is an elation KM-arc, by Lemma 2.1 we know that there exists an additive subgroup S of size t in $\mathbb{F}_q$ such that for any $\alpha \in \mathbb{F}_q$ the set $U_\alpha = \{z \mid (1,\alpha,z) \in \mathcal{B}\}$ is either empty or a coset of S. Now, from the description of $\mathcal{A}$ in Construction 2 (C) it follows that $U'_\alpha = \{z \mid (1,\alpha,z) \in \mathcal{A}\}$ equals $\{u+i \mid u \in U_\alpha, i \in I\}$ if $\alpha \in \mathbb{F}_q$, with I a direct complement of $\mathbb{F}_q$ in $\mathbb{F}_{q^h}$. It is immediate that U'_α is empty if U_α is empty or if $\alpha \notin \mathbb{F}_q$. If U'_α is non-empty, then it is a coset of the additive subgroup $\langle S, I\rangle$ of $\mathbb{F}_{q^h}$. It now follows from Lemma 2.1 that $\mathcal{A}$ is an elation KM-arc with elation line $X=0$ and tq^{h-1}-nucleus $(0,0,1)$.

The proof of the second part is very similar. We now apply Lemma 2.2 on $\mathcal{H}$ and then argue as in the first part of the proof. □

We recall that it is not required in Constructions 2 (B) and (C) to have non-affine points in the KM-arc to start with. From this point of view it is worthwhile to note that in both cases of the previous lemma non-affine points are required.

We will now prove the converse of Lemma 2.4.

Theorem 2.5. *Let $\mathcal{A}$ be a KM-arc of type* tq^{h-1}, $t>2$, *in* $\mathrm{PG}(2,q^h)$ *with* tq^{h-1}*-nucleus* $(0,0,1)$ *that arises from some KM-arc $\mathcal{B}$ of type t in* $\mathrm{PG}(2,q)$ *as in Construction 2 (C). If $\mathcal{A}$ is an elation KM-arc with elation line* $X=0$, *then $\mathcal{B}$ is an elation KM-arc with elation line* $X=0$ *and t-nucleus* $(0,0,1)$.

If $\mathcal{A}$ is an elation KM-arc of type $2q^{h-1}$ *in* $\mathrm{PG}(2,q^h)$ *with* $2q^{h-1}$*-nucleus* $(0,0,1)$ *and with elation line* $X=0$ *that arises from a hyperoval $\mathcal{H}$ as in Construction 2 (B), then $\mathcal{H}$ is an elation hyperoval stabilised by a non-trivial elation with axis* $X=0$ *and centre* $(0,0,1)$.

Proof. We consider the KM-arc $\mathcal{A}$ arising from $\mathcal{B}$ and assume that $\mathcal{A}$ is an elation KM-arc. By Lemma 2.1 we know that there is an additive subgroup S' of size tq^{h-1} in $\mathbb{F}_{q^h}$, such that for any $\alpha \in \mathbb{F}_{q^h}$ the set $U'_\alpha = \{z \mid (1,\alpha,z) \in \mathcal{A}\}$ is either empty or a coset of S'. For $\mathcal{B}$ we define $U_\alpha = \{z \mid (1,\alpha,z) \in \mathcal{B}\}$ for any $\alpha \in \mathbb{F}_q$. Through Construction 2 (C) we know that U'_α equals $\bigcup_{u \in U_\alpha} u + I$ for any $\alpha \in \mathbb{F}_q$, and that it is empty if $\alpha \notin \mathbb{F}_q$. We want to prove that there exists an additive subgroup of $\mathbb{F}_q$ such that any non-empty U_α is a coset of it.

It is easy to see that $I \subseteq S'$. Since I is a direct complement of $\mathbb{F}_q$ in $\mathbb{F}_{q^h}$ we can find an additive subgroup S of $\mathbb{F}_q$ such that $S' = \langle S, I\rangle$; necessarily $|S| = t$. Now fix a value $\alpha \in \mathbb{F}_q$ such that U_α (or equivalently U'_α) is non-empty. Let u be an element of U_α. We know that u is also an element of U'_α, hence we can write $U'_\alpha = u + S'$. For an arbitrary $v \in U_\alpha$ there exists an $s' \in S'$ such that $v = u + s'$ since v is also an element of U'_α. Since $S' = \langle S, I\rangle$, there are unique $s \in S$ and $i \in I$ such that $s' = s + i$. So, $v = u + s + i$ and as $v, u, s \in \mathbb{F}_q$ and I is a direct complement of $\mathbb{F}_q$ we know that $i = 0$ and that $v = u + s$. Since v was arbitrarily chosen, we see that $U_\alpha \subseteq u + S$. As $|U_\alpha| = t = |S|$ we conclude that $U_\alpha = u + S$. So, for any α we find that U_α is a coset of S. The theorem now follows from Lemma 2.1.

The proof of the second part follows by a very similar reasoning. □

Later in this paper, we will need the notion of $\mathbb{F}_q$-linear sets in a projective space. Let V be an r-dimensional vector space over $\mathbb{F}_{q^n}$, let Ω be the projective space $\mathrm{PG}(V) = \mathrm{PG}(r-1, q^n)$, $q = p^h$, p prime, and let T be a set of points of Ω. The set T is said to be an $\mathbb{F}_q$-*linear* set of Ω of rank t if it is defined by the non-zero vectors of an $\mathbb{F}_q$-vector subspace U of V of dimension t, i.e. $T = \mathcal{B}(U) = \{\langle u\rangle_{\mathbb{F}_{q^n}} : u \in U \setminus \{0\}\}$. For more information on $\mathbb{F}_q$-linear sets, we refer to [7] and [10].

If $\mathcal{S}$ is an $\mathbb{F}_q$-linear point set contained in a line of $\mathrm{PG}(2,q^n)$, then the (usual) dual of this point set defines a subset of the set of the lines through a fixed point. We will call such a set *an* $\mathbb{F}_q$*-linear pencil* as the terminology 'dual of a linear set' is already in use, see e.g. [10].

Remark 2.6. Consider an elation KM-arc as in Lemma 2.1. The set of points on the t-secant $Y = \alpha X$ is of the form $\{(1,\alpha,\beta+s) \mid s \in S\}$ for an additive subgroup S of $\mathbb{F}_q$. Now it is clear that this set of points, together with the t-nucleus $(0,0,1)$, forms an $\mathbb{F}_2$-linear set on the line $Y = \alpha X$. It has been conjectured by Vandendriessche in [14] that *all* KM-arcs have this property, i.e., that the points of a KM-arc of type t that lie on a given t-secant ℓ, together with the t-nucleus, form an $\mathbb{F}_2$-linear set on ℓ. Note that it has been shown in [3] that the set of points on a t-secant ℓ to a KM-arc of type t define a *Vandermonde set*, i.e. a set $\{y_1, \ldots, y_t\} \subseteq \mathbb{F}_q$, with $1 < t < q$, such that $\sum_i y_i^k = 0$ for all $1 \le k \le t-2$.

Every $\mathbb{F}_2$-linear set is a Vandermonde set, but not all Vandermonde sets are $\mathbb{F}_2$-linear sets. In $\mathbb{F}_{2^h}$, $h \leq 5$, Vandermonde and $\mathbb{F}_2$-linear are equivalent properties, however, in $\mathbb{F}_{2^6}$, where $z^6 = z^4 + z^3 + z + 1$ (the default polynomial used in the computer algebra package GAP), the set $\{0, z^{12}, z^{15}, z^{17}, z^{19}, z^{43}, z^{56}, z^{59}\}$ is Vandermonde, but not $\mathbb{F}_2$-linear. Considering that all elation KM-arcs have the conjectured property, that the non-elation KM-arcs constructed in [2, Section 4] (see Section 3) have the conjectured property and that in [16] the conjecture was checked for all KM-arcs in $\mathrm{PG}(2, 2^h)$, $h \leq 5$, it would be interesting to know whether the Vandermonde property really can be strengthened to the $\mathbb{F}_2$-linear property.

3 Elation KM-arcs of type $q/4$

Recall the construction from [2] where we have permuted the first and third coordinate:

Theorem 3.1. *Let* Tr *be the absolute trace function from $\mathbb{F}_q$ to $\mathbb{F}_2$, $q = 2^h \geq 8$. Choose $\alpha, \beta \in \mathbb{F}_q \setminus \{0, 1\}$ such that $\alpha\beta \neq 1$ and define*

$$\gamma = \frac{\beta + 1}{\alpha\beta + 1}\ , \quad \xi = \alpha\beta\gamma\ .$$

Now choose $a, b \in \mathbb{F}_2 \subset \mathbb{F}_q$, and define the following sets

$$\begin{aligned}
\mathcal{S}_0 &= \left\{(0, 1, z) \mid z \in \mathbb{F}_q, \mathrm{Tr}(z) = 0, \mathrm{Tr}\left(\frac{z}{\alpha}\right) = a\right\}\ , \\
\mathcal{S}_1 &= \left\{(1, 0, z) \mid z \in \mathbb{F}_q, \mathrm{Tr}(z) = 0, \mathrm{Tr}\left(\frac{z}{\alpha\gamma}\right) = 0\right\}\ , \\
\mathcal{S}_2 &= \left\{(1, 1, z) \mid z \in \mathbb{F}_q, \mathrm{Tr}(z) = 1, \mathrm{Tr}\left(\frac{z}{\alpha\beta}\right) = b\right\}\ , \\
\mathcal{S}_3 &= \left\{(1, \gamma, z) \mid z \in \mathbb{F}_q, \mathrm{Tr}\left(\frac{z}{\alpha\gamma}\right) = a + 1, \mathrm{Tr}\left(\frac{z}{\xi}\right) = b + 1\right\}\ , \\
\mathcal{S}_4 &= \left\{(1, \beta + 1, z) \mid z \in \mathbb{F}_q, \mathrm{Tr}\left(\frac{z}{\alpha\beta}\right) = a + b + 1, \mathrm{Tr}\left(\frac{z}{\xi}\right) = b\right\}\ .
\end{aligned}$$

Then, $\mathcal{A}_{\alpha,\beta,a,b} = \cup_{i=0}^{4} \mathcal{S}_i$ is a KM-arc of type $q/4$ in $\mathrm{PG}(2, q)$.

It is easy to prove (see also [2, Theorem 4.8]), that $\mathcal{A}_{\alpha,\beta,a,b}$ is PGL-equivalent to $\mathcal{A}_{\alpha,\beta,0,0}$.

Theorem 3.2. *[2, Theorem 4.9] Let $\alpha, \beta \in \mathbb{F}_q \setminus \{0, 1\}$, with $\alpha\beta \neq 1$. The KM-arc $\mathcal{A}_{\alpha,\beta,0,0}$ is a translation KM-arc if and only if $\alpha \in \left\{\frac{1}{\beta^2}, 1 + \frac{1}{\beta}, \beta, \frac{1}{\sqrt{\beta}}, \frac{1}{\beta+1}\right\}$.*

Consider an $\mathbb{F}_2$-linear set $\mathcal{S}$ of size 5 in $\mathrm{PG}(1, 2^h)$. By definition, we know that there is an $\mathbb{F}_2$-subspace U of $\mathbb{F}_{2^h}^2$ such that $\mathcal{S} = \mathcal{B}(U)$. Note that U is not uniquely determined by $\mathcal{S}$. It is not too hard to check that either $\dim(\langle U\rangle_2) = 2$ or $\dim(\langle U\rangle_2) = 3$, where $\langle U\rangle_2$ denotes the projective space defined by the vector space U over $\mathbb{F}_2$. If $\langle U\rangle_2$ is a solid, then every point of $\mathcal{B}(U)$ is defined by the projective points of one line of $\langle U\rangle_2$. If $\langle U\rangle_2$ is a plane, then there is exactly one point H of $\mathcal{B}(U)$ such that H is determined by the points of a projective line of $\langle U\rangle_2$, and each of the other four points of $\mathcal{B}(U)$ is determined by exactly one of the four remaining points of $\langle U\rangle_2$. In the latter case, $\mathcal{S}$ is called a *club* or more specifically, a 2-*club of rank* 3 and the point H is called the *head* of the club. In the former case, $\mathcal{S} = \mathcal{B}(U)$ with $\dim(\langle U\rangle_2) = 3$, we see that for every plane $\langle V\rangle_2$ of $\langle U\rangle_2$, also $\mathcal{S} = \mathcal{B}(V)$, and $\mathcal{S}$ is a club, with the head determined by choice of the plane $\langle V\rangle_2$. We see from this argument that the head is not uniquely determined in this case, and that any point of $\mathcal{S}$ can play the role of the head. It will follow from the proof of the following theorem that in the latter case, the club forms an $\mathbb{F}_4$-subline.

Lemma 3.3. *The set $\mathcal{C} = \{(1, 0), (0, 1), (1, 1), (\gamma, 1), (\beta + 1, 1)\} \subseteq \mathrm{PG}(1, 2^h)$ is an $\mathbb{F}_2$-linear set if and only if $\beta \in \{\gamma, \frac{1}{\gamma+1}, \sqrt{\gamma + 1}, 1 + \frac{1}{\gamma}, 1 + \gamma^2\}$. If two of the values in this set coincide, they all coincide and $\mathcal{C}$ forms an $\mathbb{F}_4$-subline.*

Proof. First suppose that $(1, 0)$ is the head of the $\mathbb{F}_2$-linear set. Then $(0, 1), (1, 1), (\gamma, 1), (\beta + 1, 1)$ are linearly dependent over $\mathbb{F}_2$ if and only if $\beta = \gamma$. If the head is $(0, 1)$, then $\{(1, 0), (1, 1), (\gamma, 1), (\beta + 1, 1)\} = \left\{(1, 0), (1, 1), (1, \frac{1}{\gamma}), (1, \frac{1}{\beta+1})\right\}$ is an $\mathbb{F}_2$-linear set if an only if $1 + \frac{1}{\gamma} + \frac{1}{\beta+1} = 0$, equivalently $\beta = \frac{1}{\gamma+1}$. If the head is $(1, 1)$, we use the collineation induced by the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ to map the head $(1, 1)$ onto $(1, 0)$, and the other points to the points with coordinates $(0, 1), (1, 1), (\gamma, \gamma + 1)$ and $(\beta + 1, \beta)$. It follows that $\mathcal{C}$ is an $\mathbb{F}_2$-linear set with head $(1,0)$ if and only if $1+\frac{\gamma}{\gamma+1}+\frac{\beta+1}{\beta}=0$, equivalently $\beta=1+\frac{1}{\gamma}$. If the head is $(\gamma,1)$, then similarly, we use the matrix $\left(\begin{smallmatrix}1&\gamma\\0&1\end{smallmatrix}\right)$ to map the head to $(0,1)$ and the other points to $(1,0)$, $(\gamma,1)$, $(1+\gamma,1)$ and $(\beta+\gamma+1,1)$, which forms an $\mathbb{F}_2$-linear set if and only if $\gamma^2=\beta+1$. Finally, if the head is $(\beta+1,1)$, we get that $\beta^2=\gamma+1$ in order for $\mathcal{C}$ to define an $\mathbb{F}_2$-linear set.

If two values in $\{\gamma,\frac{1}{\gamma+1},\sqrt{\gamma+1},1+\frac{1}{\gamma},1+\gamma^2\}$ coincide, then we know from the previous reasoning that the linear set $\mathcal{C}$ has more than one head, and hence, that all points can play the role of the head, which implies that all values have to coincide (this can be deduced by direct calculations as well). We find that $\gamma^3=1$ and $\beta=\gamma$. This implies that $\mathcal{C}=\{(1,x)\mid x\in\mathbb{F}_4\}\cup(0,1)$, and hence, $\mathcal{C}$ defines an $\mathbb{F}_4$-subline. □

Lemma 3.4. *The $q/4$-secants to the KM-arc $\mathcal{A}_{\alpha,\beta,a,b}$ in $\mathrm{PG}(2,q)$, $q=2^h$, define an $\mathbb{F}_2$-linear pencil if and only if the KM-arc is a translation arc.*

Proof. The $q/4$-secants to a KM-arc of the form $\mathcal{A}_{\alpha,\beta,a,b}$ define the set of points $\mathcal{C}=\{(1,0),\ (0,1),\ (1,1),\ (\gamma,1),\ (\beta+1,1)\}$ in $\mathrm{PG}(1,q)$. From Lemma 3.3, we get that $\mathcal{C}$ is an $\mathbb{F}_2$-linear set if and only if $\beta\in\left\{\gamma,\frac{1}{\gamma+1},\sqrt{\gamma+1},1+\frac{1}{\gamma},1+\gamma^2\right\}$. Plugging in $\gamma=\frac{\beta+1}{\alpha\beta+1}$, yields that this condition is equivalent to

$$\beta\in\left\{\frac{\beta+1}{\alpha\beta+1},\frac{\alpha\beta+1}{\alpha\beta+\beta},\sqrt{\frac{\beta+\alpha\beta}{\alpha\beta+1}},\frac{\alpha\beta+\beta}{\beta+1},\frac{\beta^2+\alpha^2\beta^2}{\alpha^2\beta^2+1}\right\}.$$

This in turn is equivalent to $\alpha\in\{\frac{1}{\beta^2},1+\frac{1}{\beta},\frac{1}{\beta+1},\beta,\frac{1}{\sqrt{\beta}}\}$, and hence, by Theorem 3.2, we conclude that the $q/4$-secants to the KM-arc $\mathcal{A}_{\alpha,\beta,a,b}$ define an $\mathbb{F}_2$-linear pencil if and only if the KM-arc is a translation arc. □

Lemma 3.5. *Every elation KM-arc of type $q/4$ is* PGL*-equivalent to a KM-arc whose elation line is given by $X=0$ and whose affine points are given by $\{(1,0,s)\mid s\in S\}\cup\{(1,1,1+s)\mid s\in S\}\cup\{(1,\alpha,\alpha'+s)\mid s\in S\}\cup\{(1,\beta,\beta'+s)\mid s\in S\}$ with S an additive subgroup of size $q/4$ of $\mathbb{F}_q$, and with $\alpha,\alpha',\beta,\beta'\in\mathbb{F}_q$.*

Proof. As $\mathrm{PGL}(3,q)$ acts transitively on the frames (4 points in standard position), we may take the $q/4$-nucleus to be $(0,0,1)$, the elation line to be $X=0$, and the points $(1,0,0)$ and $(1,1,1)$ to be contained in the KM-arc. The statement now follows from Lemma 2.1. □

Note that an additive subgroup of $\mathbb{F}_q$ corresponds to a vector subspace of the h-dimensional vector space $\mathbb{F}_2^h$. It is well-known (see e.g [8, 2.24]) that the hyperplanes of this h-dimensional vector space are in one-to-one correspondence with the sets $\{x\in\mathbb{F}_q\mid \mathrm{Tr}(\alpha x)=0\}$ where $\alpha\in\mathbb{F}_q^*$. Vector subspaces of codimension two can be written as the intersection of two different hyperplanes, which gives us the following lemma.

Lemma 3.6. *If S is an additive subgroup of order $q/4$ of $\mathbb{F}_q$, $q=2^h$, then $S=\{x\in\mathbb{F}_q\mid \mathrm{Tr}(\mu_1x)=\mathrm{Tr}(\mu_2x)=0\}$ for some $\mu_1\neq\mu_2\in\mathbb{F}_q^*$.*

Lemma 3.7. *Let S be an additive subgroup of order $q/4$ of $\mathbb{F}_q$, $q=2^h$. If $S=\alpha S$, for some $\alpha\in\mathbb{F}_q^*\setminus\{1\}$, then $\alpha\in\mathbb{F}_4$ and hence h is even and $S=\{x\in\mathbb{F}_q\mid \mathrm{Tr}(\mu x)=\mathrm{Tr}(\alpha\mu x)=0\}$ for some $\mu\in\mathbb{F}_q$. Moreover, in this case for every $\beta\in\mathbb{F}_q\setminus\mathbb{F}_4$, we have $\langle S,\beta S\rangle=\mathbb{F}_q$ and for every $\beta\in\mathbb{F}_4^*$, we have $S=\beta S$.*

Proof. By Lemma 3.6, we have that $S=\{x\in\mathbb{F}_q\mid \mathrm{Tr}(\mu_1x)=\mathrm{Tr}(\mu_2x)=0\}$ for some $\mu_1,\mu_2\in\mathbb{F}_q^*$, $\mu_1\neq\mu_2$. Clearly $\alpha S=\{x\in\mathbb{F}_q\mid \mathrm{Tr}((\mu_1/\alpha)x)=\mathrm{Tr}((\mu_2/\alpha)x)=0\}$. Suppose that $S=\alpha S$, for some $\alpha\neq1$, then both μ_1 and μ_2 have to be contained in the set $\{\mu_1/\alpha,\mu_2/\alpha,(\mu_1+\mu_2)/\alpha\}$. If $\mu_1=\mu_1/\alpha$, then $\alpha=1$, a contradiction.

Note that μ_2 and $\mu_1+\mu_2$ can be interchanged, hence without loss of generality we may assume $\mu_1=\mu_2/\alpha$. Then, either $\mu_2=\mu_1/\alpha$ or $\mu_2=(\mu_1+\mu_2)/\alpha$ since $\mu_2=\mu_2/\alpha$ implies that $\alpha=1$. In the former case, we have that $\alpha^2=1$ and hence, $\alpha=1$, a contradiction. In the latter case, we have that $\alpha^2=\alpha+1$ and hence, $\alpha\in\mathbb{F}_4$ and h is even. Also S is given by $\{x\in\mathbb{F}_q\mid \mathrm{Tr}(\mu_2x)=\mathrm{Tr}(\alpha\mu_2x)=0\}$.

Consider $\beta\in\mathbb{F}_q^*$. The subgroup βS equals $\{x\in\mathbb{F}_q\mid \mathrm{Tr}((\mu_1/\beta)x)=\mathrm{Tr}((\mu_2/\beta)x)=0\}$. Now suppose that $\langle S,\beta S\rangle$ is a subgroup of order $q/2$ (or equivalently, defines a hyperplane of $\mathbb{F}_q$), then we have that the elements in the set $V=\{\mu_1/\beta,\mu_2/\beta,\mu_1,\mu_2\}$ are linearly dependent over $\mathbb{F}_2$. Since $\mu_1=\mu_2/\alpha$, it follows that the elements in $V=\{\mu_1/\beta,\alpha\mu_1/\beta,\mu_1,\alpha\mu_1\}$ are linearly dependent, and hence, since $\mu_1\neq0$ and $\alpha^{-1}=\alpha^2=\alpha+1$, we know that $1/\beta$ is an $\mathbb{F}_2$-linear combination of α and 1. It follows that $\beta\in\mathbb{F}_4^*$. If $\beta\in\mathbb{F}_q\setminus\mathbb{F}_4$, we conclude that $\langle S,\beta S\rangle$ cannot be a subgroup of order $q/2$, but neither can it have order $q/4$ by the first part of the proof. Hence, $\langle S,\beta S\rangle$ equals $\mathbb{F}_q$. If $\beta=\alpha+1$, then $S=\alpha S$ implies that also $S=(\alpha+1)S=\beta S$. Hence, for every $\beta\in\mathbb{F}_4^*=\{1,\alpha,\alpha+1\}$, we have $S=\beta S$. □

Lemma 3.8. *Let S be an additive subgroup of order $q/4$ in $\mathbb{F}_q$, $q = 2^h$, and let $\alpha, \beta \in \mathbb{F}_q$. If $\langle S, \alpha S\rangle$, $\langle S, \beta S\rangle$, $\langle \alpha S, \beta S\rangle$ and $\langle (\alpha+1)S, (\beta+1)S\rangle$ are subgroups of order $q/2$, then either $\beta = \alpha+1$ and $S = \{x \in \mathbb{F}_q \mid \mathrm{Tr}(\gamma x) = \mathrm{Tr}(\alpha\gamma x) = 0\}$ for some $\gamma \in \mathbb{F}_q$, or $3 \mid h$, $\alpha, \beta \in \mathbb{F}_8 \subseteq \mathbb{F}_q$ and there is an additive subgroup S' of order $q/8$ in $\mathbb{F}_q$ such that $S' = S \cap \alpha S \cap \beta S \cap (\alpha+1)S \cap (\beta+1)S$. Moreover, if in this case $\langle S, \alpha S\rangle = \{x \in \mathbb{F}_q \mid \mathrm{Tr}(\gamma x) = 0\}$ for some $\gamma \in \mathbb{F}_q$, then $S' = \{x \in \mathbb{F}_q \mid \forall y \in \mathbb{F}_8 : \mathrm{Tr}(xy\gamma) = 0\}$.*

Proof. First note that the conditions of the lemma imply that $\alpha \neq \beta$ and that $\alpha, \beta \notin \{0, 1\}$. For convenience, we consider the subgroups as subspaces of the projective space $\mathrm{PG}(\mathbb{F}_2^h) = \mathrm{PG}(h-1, 2)$, and dualise. The dualisation is induced by the bijection that maps the hyperplane $\{x \mid \mathrm{Tr}(kx) = 0\}$ onto the vector line k and vice versa. By T^D we denote the dual of a subspace T. The subspaces S^D, $(\alpha S)^D$ and $(\beta S)^D$ are vector planes of $\mathbb{F}_2^h$ hence, we consider them as lines of $\mathrm{PG}(h-1, 2)$.

The condition that the subgroup generated by any two elements of $\{S, \alpha S, \beta S\}$ has order $q/2$ translates into the condition that the lines S^D, $(\alpha S)^D$ and $(\beta S)^D$ mutually intersect in a point. Note that $\langle S, \alpha S\rangle$ always contains $(\alpha+1)S$, which implies that the line $((\alpha+1)S)^D$ goes through $S^D \cap (\alpha S)^D$, and similarly, the line $((\beta+1)S)^D$ goes through $S^D \cap (\beta S)^D$. We denote the hyperplane $\langle S, \alpha S\rangle$ by $\{x \in \mathbb{F}_q \mid \mathrm{Tr}(\gamma x) = 0\}$. Then, $S = \{x \in \mathbb{F}_q \mid \mathrm{Tr}(\gamma x) = \mathrm{Tr}(\alpha\gamma x) = 0\}$ and $\alpha S = \{x \in \mathbb{F}_q \mid \mathrm{Tr}(\gamma x) = \mathrm{Tr}((\gamma/\alpha)x) = 0\}$. Note that $S \neq \alpha S$ also implies that $\alpha^2 \neq \alpha + 1$ (see Lemma 3.7).

Recall that the lines S^D, $(\alpha S)^D$ and $(\beta S)^D$ mutually intersect in a point. The first possibility is that the lines $S^D = \langle \gamma, \alpha\gamma\rangle$, $(\alpha S)^D = \langle \gamma, \frac{\gamma}{\alpha}\rangle$ and $(\beta S)^D = \left\langle \frac{\gamma}{\beta}, \frac{\alpha\gamma}{\beta}\right\rangle$ go through a common point. Then, we have that $1/\beta = 1$, $\alpha/\beta = 1$ or $(\alpha+1)/\beta = 1$. The first and the second lead immediately to a contradiction, so $\beta = \alpha+1$.

The second possibility is that the lines S^D, $(\alpha S)^D$ and $(\beta S)^D$ are contained in a common plane but are not concurrent. The plane spanned by S^D and $(\alpha S)^D$ is the plane $\langle \gamma, \alpha\gamma, \frac{\gamma}{\alpha}\rangle$. Since $(\beta S)^D$ lies in this plane, $\frac{\gamma}{\beta}$ and $\frac{\alpha\gamma}{\beta}$ are both a linear combination of γ, $\alpha\gamma$ and $\frac{\gamma}{\alpha}$. Hence, $\frac{1}{\beta}$ and $\frac{\alpha}{\beta}$ are both a linear combination of α, 1 and $\frac{1}{\alpha}$. So, $\frac{\alpha}{\beta}$ is both a linear combination of α, 1 and $\frac{1}{\alpha}$ and of α^2, α and 1. Then, either $\frac{\alpha}{\beta} = \alpha+1$ or else there exist $\lambda_1, \lambda_2 \in \mathbb{F}_2$ such that $\alpha^2 + \lambda_2\alpha + \lambda_1 + \frac{1}{\alpha} = 0$, equivalently such that $\alpha^3 + \lambda_2\alpha^2 + \lambda_1\alpha + 1 = 0$. In the latter case we must have that $\alpha^3 + \alpha + 1 = 0$ or $\alpha^3 + \alpha^2 + 1 = 0$, since $(\alpha+1)^3 \neq 0$. Hence $\alpha \in \mathbb{F}_8$ and consequently also $\beta \in \mathbb{F}_8$ and $3 \mid h$.

In the former case we have that $\beta = \frac{\alpha}{\alpha+1}$. Then, $((\beta+1)S)^D = \langle (\alpha+1)\gamma, \alpha(\alpha+1)\gamma\rangle$. We also have that $(\alpha+1)S = \left\langle \gamma, \frac{\gamma}{\alpha+1}\right\rangle$. Since $((\alpha+1)S)^D$ and $((\beta+1)S)^D$ have a point in common, the sets $\{\alpha+1, \alpha^2+\alpha, \alpha^2+1\}$ and $\left\{1, \frac{1}{\alpha+1}, \frac{\alpha}{\alpha+1}\right\}$ have an element in common. If follows that either $\alpha^2 = \alpha+1$, in which case $\beta = \alpha+1$, or else $\alpha^3 + \alpha^j + 1 = 0$ with $j \in \{1, 2\}$, in which case $\alpha \in \mathbb{F}_8$ and hence also $\beta \in \mathbb{F}_8$ and $3 \mid h$.

Note that in the cases with $\alpha, \beta \in \mathbb{F}_8$, we have that the lines S^D, $(\alpha S)^D$, $(\beta S)^D$, $((\alpha+1)S)^D$, $((\beta+1)S)^D$ are contained in the plane $\langle \gamma, \alpha\gamma, \frac{\gamma}{\alpha}\rangle = \langle \gamma, \alpha\gamma, \alpha^2\gamma\rangle$. Hence, the subgroup $\langle \gamma, \alpha\gamma, \alpha^2\gamma\rangle^D = S' = \{x \in \mathbb{F}_q \mid \forall y \in \mathbb{F}_8 : \mathrm{Tr}(xy\gamma) = 0\}$ equals the intersection $S \cap \alpha S \cap \beta S \cap (\alpha+1)S \cap (\beta+1)S$. □

Lemma 3.9. *Let $\mathbb{F}_q$ be a field that admits $\mathbb{F}_8$ as a subfield. Let $\alpha, \beta \in \mathbb{F}_8 \setminus \{0, 1\}$ with $\beta \notin \{\alpha, \alpha+1\}$ and let S be an additive subgroup of order $q/4$ of $\mathbb{F}_q$. Assume that $\langle S, \alpha S\rangle = \{x \in \mathbb{F}_q \mid \mathrm{Tr}(k_1 x) = 0\}$, $\langle S, \beta S\rangle = \{x \in \mathbb{F}_q \mid \mathrm{Tr}(k_2 x) = 0\}$, $\langle \alpha S, \beta S\rangle = \{x \in \mathbb{F}_q \mid \mathrm{Tr}(k_3 x) = 0\}$ and $\langle (\alpha+1)S, (\beta+1)S\rangle = \{x \in \mathbb{F}_q \mid \mathrm{Tr}(k_4 x) = 0\}$ for certain pairwise different $k_1, k_2, k_3, k_4 \in \mathbb{F}_q^*$. Then the system of equations*

$$\begin{cases} \mathrm{Tr}(k_1(X+\alpha)) = 1 & (1) \\ \mathrm{Tr}(k_2(Y+\beta)) = 1 & (2) \\ \mathrm{Tr}(k_3(\alpha Y + \beta X)) = 1 & (3) \\ \mathrm{Tr}(k_4((\alpha+\beta) + (\beta+1)X + (\alpha+1)Y)) = 1 & (4) \end{cases}$$

has no solutions $(X, Y) \in \mathbb{F}_q^2$.

Proof. Using the same dualisation and notation as in the proof of Lemma 3.8, we consider the lines $S^D, (\alpha S)^D$, $(\beta S)^D$, $((\alpha+1)S)^D$ and $((\beta+1)S)^D$. It follows from the conditions of the lemma that these lines are all different. From Lemma 3.8 we know that these lines are contained in a plane π, the dual of the subgroup $\{x \mid \forall y \in \mathbb{F}_8 : \mathrm{Tr}(k_1 xy) = 0\}$. As the line $((\alpha+1)S)^D$ goes through $S^D \cap (\alpha S)^D$, it is the unique third line in π through $S^D \cap (\alpha S)^D$, different from S^D and $(\alpha S)^D$. Since $\langle S, \alpha S\rangle = \{x \in \mathbb{F}_q \mid \mathrm{Tr}(k_1 x) = 0\}$, the point $S^D \cap (\alpha S)^D$ is the point k_1. Similarly, the line $((\beta+1)S)^D$ is the unique line which goes through $S^D \cap (\beta S)^D = k_2$, and is different from S^D and $(\beta S)^D$. The lines $(\alpha S)^D$ and $(\beta S)^D$ meet in the point k_3. The plane π is generated by k_1, k_1 and k_3. It follows that the point k_4, which is the intersection of $((\alpha+1)S)^D$ and $((\beta+1)S)^D$ (and also is contained in $((\alpha+\beta)S)^D$) is equal to $k_1+k_2+k_3$, as it is the unique point of the plane, not on the lines S^D, $(\alpha S)^D$ and $(\beta S)^D$.

Since $\langle S, \alpha S\rangle = \{x \in \mathbb{F}_q \mid \mathrm{Tr}(k_1x) = 0\}$, we know that $S = \{x \in \mathbb{F}_q \mid \mathrm{Tr}(k_1x) = \mathrm{Tr}(\alpha k_1 x) = 0\}$ and $\alpha S = \{x \in \mathbb{F}_q \mid \mathrm{Tr}(k_1x) = \mathrm{Tr}((k_1/\alpha)x) = 0\}$. Analogously it follows from $\langle S, \beta S\rangle = \{x \in \mathbb{F}_q \mid \mathrm{Tr}(k_2x) = 0\}$ that $S = \{x \in \mathbb{F}_q \mid \mathrm{Tr}(k_2x) = \mathrm{Tr}(\beta k_2x) = 0\}$ and $\beta S = \{x \in \mathbb{F}_q \mid \mathrm{Tr}(k_2x) = \mathrm{Tr}((k_2/\beta)x) = 0\}$. Comparing the expressions for S, this implies that

$$k_2/k_1 \in \{\alpha, \alpha+1\} \tag{5}$$

and

$$k_2/k_1 \in \{\alpha/\beta, 1/\beta, (\alpha+1)/\beta\}\ . \tag{6}$$

Similarly, from $\langle \alpha S, \beta S\rangle = \{x \in \mathbb{F}_q \mid \mathrm{Tr}(k_3x) = 0\}$ it follows that $\alpha S = \{x \in \mathbb{F}_q \mid \mathrm{Tr}(k_3x) = \mathrm{Tr}((\beta/\alpha)k_3x) = 0\}$ and $\beta S = \{x \in \mathbb{F}_q \mid \mathrm{Tr}(k_3x) = \mathrm{Tr}((\alpha/\beta)k_3x) = 0\}$, and we find that

$$k_3/k_1 \in \{1/\alpha, (\alpha+1)/\alpha\} \tag{7}$$

and

$$k_3/k_1 \in \{\alpha/\beta, 1/\beta, (\alpha+1)/\beta\}. \tag{8}$$

Looking at the system of equations, we see that a solution (X, Y) to (1) and (2) is of the form $\left(\frac{t}{k_1}+\alpha, \frac{t'}{k_2}+\beta\right)$ for some $t, t' \in \mathbb{F}_q$ with $\mathrm{Tr}(t) = \mathrm{Tr}(t') = 1$. Equation (3) gives us that

$$\frac{k_3}{k_2}\alpha t' + \frac{k_3}{k_1}\beta t = t'' \tag{9}$$

for some t'' with $\mathrm{Tr}(t'') = 1$. Finally, equation (4) with $k_4 = k_1+k_2+k_3$ yields

$$(k_1+k_2+k_3)\left(\frac{\beta+1}{k_1}t + \frac{\alpha+1}{k_2}t'\right) = t''' \tag{10}$$

for some $t''' \in \mathbb{F}_q$ with $\mathrm{Tr}(t''') = 1$.

We know that $\alpha^3 = \alpha+1$ or $\alpha^3 = \alpha^2+1$ and $\beta \in \{\alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$. Suppose first that $\alpha^3 = \alpha+1$ and $\beta = \alpha^2$. It follows from equations (5) and (6) that $k_2/k_1 = \alpha = (\alpha+1)/\beta$. From equations (7) and (8), we get that $k_3/k_1 = 1/\alpha = \alpha/\beta$. Hence, $k_4 = k_1(1+\alpha+1/\alpha)$. Equation (9) becomes $\alpha t + (\alpha^2+1)t' = t''$ while equation (10) becomes $(\alpha+1)t + (\alpha^2+1)t' = t'''$. This implies that $t + t'' = t'''$, a contradiction since $\mathrm{Tr}(t+t'') = 0$ and $\mathrm{Tr}(t''') = 1$.

A tedious calculation shows the following results.

- If $\alpha^3 = \alpha+1$ and $\beta = \alpha^2+1$, then $k_2/k_1 = \alpha$, $k_3/k_1 = (\alpha+1)/\alpha$.
- If $\alpha^3 = \alpha+1$ and $\beta = \alpha^2+\alpha$, then $k_2/k_1 = \alpha+1$, $k_3/k_1 = 1/\alpha$.
- If $\alpha^3 = \alpha+1$ and $\beta = \alpha^2+\alpha+1$, then $k_2/k_1 = \alpha+1$, $k_3/k_1 = (\alpha+1)/\alpha$.
- If $\alpha^3 = \alpha^2+1$ and $\beta = \alpha^2$, then $k_2/k_1 = \alpha+1$, $k_3/k_1 = 1/\alpha$.
- If $\alpha^3 = \alpha^2+1$ and $\beta = \alpha^2+1$, then $k_2/k_1 = \alpha+1$, $k_3/k_1 = (\alpha+1)/\alpha$.
- If $\alpha^3 = \alpha^2+1$ and $\beta = \alpha^2+\alpha$, then $k_2/k_1 = \alpha$, $k_3/k_1 = 1/\alpha$.
- If $\alpha^3 = \alpha^2+1$ and $\beta = \alpha^2+\alpha+1$, then $k_2/k_1 = \alpha$, $k_3/k_1 = (\alpha+1)/\alpha$.

In all of the above cases, one can check that plugging these values in equations (9) and (10) gives a contradiction in the same way as deduced above. □

Theorem 3.10. *If a KM-arc $\mathcal{A}$ of type $q/4$ in* $\mathrm{PG}(2,q)$ *is an elation KM-arc, then its $q/4$-secants define an $\mathbb{F}_2$-linear pencil with head corresponding to the elation line. Moreover, if the elation line is given by $X = 0$ and the linear pencil of $q/4$-secants is given by the set of lines with equation $Y = kX$ with $k \in \langle \alpha, 1\rangle$ up to* PGL-*equivalence, then the subgroup determined by the points of $\mathcal{A}$ on its $q/4$-secants is given by $S = \{x \mid \mathrm{Tr}(\mu x) = \mathrm{Tr}(\alpha\mu x) = 0\}$ for some $\mu \in \mathbb{F}_q$.*

Proof. By Lemma 3.5, we know that up to PGL-equivalence we can take the elation line to be $X = 0$ and the affine points of $\mathcal{A}$ to be $\{(1,0,s) \mid s \in S\} \cup \{(1,1,1+s) \mid s \in S\} \cup \{(1,\alpha,\alpha'+s) \mid s \in S\} \cup \{(1,\beta,\beta'+s) \mid s \in S\}$ for some $\alpha, \alpha', \beta, \beta' \in \mathbb{F}_q$, where S has order $q/4$. For any $a \in \mathbb{F}_q$ we denote the line $Y = aX$ by ℓ_a. Then we see that the affine points are contained in the lines $\ell_0, \ell_1, \ell_\alpha$ and ℓ_β.

Three points of $\mathcal{A}$ on the lines $\ell_0, \ell_1, \ell_\alpha$ respectively, cannot be collinear. Hence, we find that $\begin{vmatrix} 1 & 0 & s_1 \\ 1 & 1 & 1+s_2 \\ 1 & \alpha & \alpha'+s_3 \end{vmatrix} \neq 0$ for all $s_1, s_2, s_3 \in S$. This implies that for all $s_1, s_2, s_3 \in S$, $\alpha' + s_3 + \alpha + \alpha s_2 + \alpha s_1 + s_1 \neq 0$, and hence, that $\alpha + \alpha' \notin \langle S, \alpha S \rangle$. In particular, $\langle S, \alpha S \rangle$ cannot be the entire field $\mathbb{F}_q$. In a similar way, by looking at three points on $\ell_0, \ell_1, \ell_\beta$, we find that $\beta + \beta' \notin \langle S, \beta S \rangle$, hence, $\langle S, \beta S \rangle \neq \mathbb{F}_q$, and by looking at points on $\ell_0, \ell_\alpha, \ell_\beta$, that $\alpha\beta' + \beta\alpha' \notin \langle \alpha S, \beta S \rangle$, and hence $\langle \alpha S, \beta S \rangle$ is not $\mathbb{F}_q$. For three points on $\ell_1, \ell_\alpha, \ell_\beta$, we find that for all s_1, s_2, s_3 in $\mathbb{F}_q$,

$$\begin{aligned} & \alpha\beta' + \beta\alpha' + \alpha' + \beta' + \alpha + \beta + \alpha(s_1 + s_3) + \beta(s_1 + s_2) + s_2 + s_3 \neq 0 \\ \Leftrightarrow \quad & \alpha\beta' + \beta\alpha' + \alpha' + \beta' + \alpha + \beta + (\alpha + 1)(s_1 + s_3) + (\beta + 1)(s_1 + s_2) \neq 0 \,. \end{aligned}$$

Hence, we have that $\alpha\beta' + \beta\alpha' + \alpha' + \beta' + \alpha + \beta \notin \langle (\alpha+1)S, (\beta+1)S \rangle$ and so $\langle (\alpha+1)S, (\beta+1)S \rangle$ cannot be $\mathbb{F}_q$.

Since $S, \alpha S, \beta S, (\alpha+1)S$ and $(\beta+1)S$ are additive subgroups of $\mathbb{F}_q$ of size $q/4$, by Lemmas 3.7 and 3.8, we find that either $\beta = \alpha + 1$, and then $\ell_0, \ell_1, \ell_\alpha, \ell_\beta, \ell_\infty$ define an $\mathbb{F}_2$-linear pencil with ℓ_∞ as head, or $3|h$ and $\alpha, \beta \in \mathbb{F}_8$. Suppose we are in the latter case. Since $\alpha + \alpha' \notin \langle S, \alpha S \rangle$, we have that $\mathrm{Tr}(k_1(\alpha + \alpha')) = 1$ with k_1 such that $\langle S, \alpha S \rangle$ is the subgroup of all elements $\{x \mid \mathrm{Tr}(k_1 x) = 0\}$. Similarly, $\mathrm{Tr}(k_2(\beta + \beta')) = 1$, with k_2 such that $\langle S, \beta S \rangle = \{x \mid \mathrm{Tr}(k_2 x) = 0\}$, and $\mathrm{Tr}(k_3(\alpha\beta' + \beta\alpha')) = 1$, with k_3 such that $\langle \alpha S, \beta S \rangle = \{x \mid \mathrm{Tr}(k_3 x) = 0\}$, and $\mathrm{Tr}(k_4((\alpha+1)\beta' + (\beta+1)\alpha' + \alpha + \beta)) = 1$, with k_4 such that $\langle (\alpha+1)S, (\beta+1)S \rangle = \{x \mid \mathrm{Tr}(k_4 x) = 0\}$. But by Lemma 3.9, there is no solution (α', β') for this system of equations.

So, $\beta = \alpha + 1$ and the $q/4$-secants determine an $\mathbb{F}_2$-linear pencil with ℓ_∞ as head. Either $S = \alpha S$ or $\langle S, \alpha S \rangle$ has order $q/2$. In the former case, the second part of the statement follows from Lemma 3.7 and in the latter case it follows from Lemma 3.8. □

Remark 3.11. We believe that the statement of Theorem 3.10 holds for general elation KM-arcs of type t, i.e. that the t-secants to an elation KM-arc of type t define an $\mathbb{F}_2$-linear pencil (with the elation line as head). It is worth mentioning that this property also seems to hold for elation hyperovals, where the pencil that should be $\mathbb{F}_2$-linear is the set of 2-secants through the centre of the non-trivial elation.

Theorem 3.12. *Let $\mathcal{A}$ be an elation KM-arc of type $q/4$, then $\mathcal{A}$ is* PGL*-equivalent to the KM-arc $\mathcal{A}_{1/\beta^2,\beta,0,0}$. Hence, $\mathcal{A}$ is a translation KM-arc.*

Proof. By Theorem 3.10, we know that the $q/4$-secants to an elation KM-arc of type $q/4$ define an $\mathbb{F}_2$-linear pencil with head the elation line. Hence, by Lemmas 3.5 and 3.10 $\mathcal{A}$ is equivalent to a KM-arc with elation line $X = 0$ and affine point set $\{(1,0,s) \mid s \in S\} \cup \{(1,1,1+s) \mid s \in S\} \cup \{(1,\beta,\alpha_1+s) \mid s \in S\} \cup \{(1,\beta+1,\alpha_2+s) \mid s \in S\}$, where $\alpha_1, \alpha_2, \beta$ are elements of $\mathbb{F}_q$ and S is an additive subgroup of order $q/4$ of $\mathbb{F}_q$ given by $S = \{x \mid \mathrm{Tr}(\mu x) = \mathrm{Tr}(\beta\mu x) = 0\}$ for some $\mu \in \mathbb{F}_q$. We see that the KM-arc $\mathcal{A}$ is PGL-equivalent with the KM-arc $\mathcal{A}_{1/\beta^2,\beta,0,0}$.

The statement now follows from Theorem 3.2 or Lemma 3.4. □

4 A new family of elation KM-arcs of type $q/8$

We start by recalling the definition of the Kronecker delta.

Definition 4.1. For two integers i and j, the Kronecker delta $\delta_{i,j}$ equals 1 if $i = j$ and 0 otherwise.

We can consider the Kronecker delta as a $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ function that maps (i,j) onto $\delta_{i,j}$. We now define a similar function for vectors over $\mathbb{F}_2$.

Definition 4.2. The function $M_n^k : (\mathbb{F}_2^k)^n \to \mathbb{F}_2$ is the function taking n vectors of length k as argument and mapping them to 0 if two of these vectors are equal and to 1 otherwise.

The proof of the following lemma is straightforward.

Lemma 4.3. *Let x, y, z be vectors in $\mathbb{F}_2^k$.*

(i) $M_2^k(x,y) = 1 + \prod_{i=1}^{k}(x_i + y_i + 1)$

(ii) $M_3^k(x,y,z) = M_2^k(x,y) + M_2^k(y,z) + M_2^k(z,x)$

We now construct a new family of KM-arcs.

Theorem 4.4. *Let $q = 2^h$, $h \geq 4$. Let $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_q^*$ be $\mathbb{F}_2$-independent and define $S = \{x \in \mathbb{F}_q \mid \forall i : \mathrm{Tr}(\alpha_i x) = 0\}$. Let $\beta_1, \beta_2, \beta_3 \in \mathbb{F}_q^*$ be such that $\mathrm{Tr}(\alpha_i \beta_j) = \delta_{i,j}$. Let f_1, f_2, f_3 be the three functions $\mathbb{F}_2^3 \to \mathbb{F}_2$, given by $f_1 : (x,y,z) \mapsto x + y + z + yz$, $f_2 : (x,y,z) \mapsto y + z + xz$ and $f_3 : (x,y,z) \mapsto z + xy$.*

For any $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{F}_2^3$ we define

$$\mathcal{S}_{(\lambda_1,\lambda_2,\lambda_3)} = \left\{ \left(1, \sum_{i=1}^{3} \lambda_i \alpha_i, \sum_{i=1}^{3} f_i(\lambda_1,\lambda_2,\lambda_3)\beta_i + s \right) \middle| \; s \in S \right\} .$$

We also define $\mathcal{S}_0 = \{(0,1,x) \mid \forall i : \mathrm{Tr}(\alpha_i^2 x) = 0\}$ and $\mathcal{A} = \mathcal{S}_0 \cup \bigcup_{v \in \mathbb{F}_2^3} \mathcal{S}_v$. If $q > 16$, then $\mathcal{A}$ is an elation KM-arc of type $q/8$ in $\mathrm{PG}(2,q)$ with elation line $X = 0$ and $q/8$-nucleus $(0,0,1)$. If $q = 16$, then $\mathcal{A}$ is an elation hyperoval in $\mathrm{PG}(2,q)$ with elation line $X = 0$.

Proof. We know that S is an additive subgroup of $\mathbb{F}_q$ containing $q/8$ elements. Now note that the element β_j, $j = 1,2,3$ is a coset leader of the coset $\{x \in \mathbb{F}_q \mid \forall i : \mathrm{Tr}(\alpha_i x) = \delta_{i,j}\}$ which also implies that the existence of elements $\beta_1, \beta_2, \beta_3$ is guaranteed.

It is immediate that the points of $\mathcal{S}_{(\lambda_1,\lambda_2,\lambda_3)}$, with $(\lambda_1,\lambda_2,\lambda_3) \in \mathbb{F}_2^3$, are on the line $\ell_{(\lambda_1,\lambda_2,\lambda_3)}$ with equation $(\sum_{i=1}^3 \lambda_i \alpha_i)X + Y = 0$ and that the points of $\mathcal{S}_0$ are on the line ℓ_∞ with equation $X = 0$. Hence, all lines through $N(0,0,1)$ either contain $q/8$ or 0 points of $\mathcal{A}$.

Now we check that three points on different $q/8$-secants are not collinear. First we assume that ℓ_∞ is not among these three $q/8$-secants. Then the three points can be described as

$$\left(1, \sum_{i=1}^{3} \lambda_i \alpha_i, \sum_{i=1}^{3} f_i(\overline{\lambda})\beta_i + s\right), \left(1, \sum_{i=1}^{3} \lambda'_i \alpha_i, \sum_{i=1}^{3} f_i(\overline{\lambda}')\beta_i + s'\right) \text{ and } \left(1, \sum_{i=1}^{3} \lambda''_i \alpha_i, \sum_{i=1}^{3} f_i(\overline{\lambda}'')\beta_i + s''\right)$$

with $\overline{\lambda} = (\lambda_1,\lambda_2,\lambda_3)$, $\overline{\lambda}' = (\lambda'_1,\lambda'_2,\lambda'_3)$ and $\overline{\lambda}'' = (\lambda''_1,\lambda''_2,\lambda''_3)$ three pairwise different vectors in $\mathbb{F}_2^3$. We find that

$$\begin{aligned} \Delta &= \begin{vmatrix} 1 & \sum_{i=1}^3 \lambda_i \alpha_i & \sum_{i=1}^3 f_i(\overline{\lambda})\beta_i + s \\ 1 & \sum_{i=1}^3 \lambda'_i \alpha_i & \sum_{i=1}^3 f_i(\overline{\lambda}')\beta_i + s' \\ 1 & \sum_{i=1}^3 \lambda''_i \alpha_i & \sum_{i=1}^3 f_i(\overline{\lambda}'')\beta_i + s'' \end{vmatrix} \\ &= \sum_{cyc} \left(\sum_{i,j=1}^{3} (\lambda_i f_j(\overline{\lambda}') + \lambda'_i f_j(\overline{\lambda}))\alpha_i\beta_j + s\sum_{i=1}^{3} \lambda'_i \alpha_i + s' \sum_{i=1}^{3} \lambda_i \alpha_i \right) \end{aligned}$$

where the cyclic sum is taken over $(\overline{\lambda}, \overline{\lambda}', \overline{\lambda}'')$ and the corresponding (s, s', s''). We calculate the trace of both sides of this equation. Considering that $\mathrm{Tr}(\alpha_i t) = 0$ for all $t \in S$, $i = 1,2,3$, that $\mathrm{Tr}(\alpha_i \beta_j) = \delta_{i,j}$ and that the trace function is $\mathbb{F}_2$-linear, we find that

$$\begin{aligned} \mathrm{Tr}(\Delta) &= \sum_{cyc} \left(\sum_{i,j=1}^{3} (\lambda_i f_i(\overline{\lambda}') + \lambda'_i f_i(\overline{\lambda})) \right) \\ &= \sum_{cyc} (\lambda_1(\lambda'_1 + \lambda'_2 + \lambda'_3 + \lambda'_2\lambda'_3) + \lambda'_1(\lambda_1 + \lambda_2 + \lambda_3 + \lambda_2\lambda_3) + \lambda_2(\lambda'_2 + \lambda'_3 + \lambda'_1\lambda'_3) \\ &\qquad + \lambda'_2(\lambda_2 + \lambda_3 + \lambda_1\lambda_3) + \lambda_3(\lambda'_3 + \lambda'_1\lambda'_2) + \lambda'_3(\lambda_3 + \lambda_1\lambda_2)) \\ &= \sum_{cyc} \left(M_2^3(\overline{\lambda}, \overline{\lambda}') + \sum_{i=1}^{3} (\lambda_i + 1) + \sum_{i=1}^{3} (\lambda'_i + 1) + 1 \right) \\ &= M_2^3(\overline{\lambda}, \overline{\lambda}') + M_2^3(\overline{\lambda}', \overline{\lambda}'') + M_2^3(\overline{\lambda}'', \overline{\lambda}) \\ &= M_3^3(\overline{\lambda}, \overline{\lambda}', \overline{\lambda}'') \; . \end{aligned} \tag{11}$$

In the last step, we used Lemma 4.3(ii). It follows that $\Delta \neq 0$ because the vectors $\overline{\lambda}$, $\overline{\lambda}'$ and $\overline{\lambda}''$ are pairwise different, hence the three points that we considered are not collinear.

Now we assume that ℓ_∞ is among the three $q/8$-secants. Then, the three points can be described as

$$\left(1, \sum_{i=1}^{3} \lambda_i \alpha_i, \sum_{i=1}^{3} f_i(\overline{\lambda})\beta_i + s\right), \left(1, \sum_{i=1}^{3} \lambda_i' \alpha_i, \sum_{i=1}^{3} f_i(\overline{\lambda}')\beta_i + s'\right) \text{ and } (0,1,t)$$

with $\overline{\lambda} = (\lambda_1, \lambda_2, \lambda_3)$, $\overline{\lambda}' = (\lambda_1', \lambda_2', \lambda_3')$ two different vectors in $\mathbb{F}_2^3$ and $\mathrm{Tr}(\alpha_i^2 t) = 0$ for $i = 1, 2, 3$. We find that

$$\Delta' = \begin{vmatrix} 0 & 1 & t \\ 1 & \sum_{i=1}^{3} \lambda_i \alpha_i & \sum_{i=1}^{3} f_i(\overline{\lambda})\beta_i + s \\ 1 & \sum_{i=1}^{3} \lambda_i' \alpha_i & \sum_{i=1}^{3} f_i(\overline{\lambda}')\beta_i + s' \end{vmatrix} = t \sum_{i=1}^{3} (\lambda_i + \lambda_i')\alpha_i + \sum_{i=1}^{3} (f_i(\overline{\lambda}) + f_i(\overline{\lambda}'))\beta_i + s + s' \ .$$

It follows that

$$\begin{aligned} \mathrm{Tr}\left(\left(\sum_{i=1}^{3}(\lambda_i + \lambda_i')\alpha_i\right)\Delta'\right) &= \mathrm{Tr}\left(t \sum_{i=1}^{3}(\lambda_i + \lambda_i')\alpha_i^2 + \sum_{i,j=1}^{3}(f_j(\overline{\lambda}) + f_j(\overline{\lambda}'))(\lambda_i + \lambda_i')\alpha_i\beta_j \right. \\ &\qquad \left. + (s+s')\left(\sum_{i=1}^{3}(\lambda_i + \lambda_i')\alpha_i\right)\right) \\ &= \sum_{i=1}^{3}(f_i(\overline{\lambda}) + f_i(\overline{\lambda}'))(\lambda_i + \lambda_i') \\ &= (\lambda_1 + \lambda_1')(\lambda_1 + \lambda_2 + \lambda_3 + \lambda_2\lambda_3 + \lambda_1' + \lambda_2' + \lambda_3' + \lambda_2'\lambda_3') \\ &\quad + (\lambda_2 + \lambda_2')(\lambda_2 + \lambda_3 + \lambda_1\lambda_3 + \lambda_2' + \lambda_3' + \lambda_1'\lambda_3') \\ &\quad + (\lambda_3 + \lambda_3')(\lambda_3 + \lambda_1\lambda_2 + \lambda_3' + \lambda_1'\lambda_2') \\ &= M_2^3(\overline{\lambda}, \overline{\lambda}') \ . \end{aligned} \tag{12}$$

In the final step we used that all elements of $\mathbb{F}_2$ equal their square. Again we find that $\Delta' \neq 0$, hence the three points are not collinear.

We conclude that all lines not through N contain at most two points of $\mathcal{A}$. For any point $P \in \mathcal{A}$ there are q points of $\mathcal{A}$ not on the $q/8$-secant $\ell_P = \langle P, N \rangle$ so all q lines through P different from ℓ_P contain precisely two points of $\mathcal{A}$. Consequently, all lines of $\mathrm{PG}(2,q)$ contain 0, 2 or $q/8$ points of $\mathcal{A}$. So, $\mathcal{A}$ is a KM-arc of type $q/8$. From its definition and Lemmas 2.1 and 2.2 it follows immediately that $\mathcal{A}$ is an elation KM-arc with elation line $X = 0$ if $q > 16$ and that $\mathcal{A}$ is an elation hyperoval with elation line $X = 0$ if $q = 16$. □

Corollary 4.5. *A KM-arc of type $q/8$ in $\mathrm{PG}(2,q)$, q even, exists for all $q \geq 16$.*

This result follows immediately from the preceding theorem. The existence of KM-arcs of type $q/8$ was previously not generally known. We will discuss this in detail in Remark 4.17

Remark 4.6. Instead of the three $\mathbb{F}_2^3 \to \mathbb{F}_2$ functions $f_1 : (x,y,z) \mapsto x + y + z + yz$, $f_2 : (x,y,z) \mapsto y + z + xz$ and $f_3 : (x,y,z) \mapsto z + xy$ that we used in Theorem 4.4 we could have used other $\mathbb{F}_2^3 \to \mathbb{F}_2$ functions. E.g., $f_1 : (x,y,z) \mapsto y + z + yz$, $f_2 : (x,y,z) \mapsto z + xz$ and $f_3 : (x,y,z) \mapsto xy$ work as well. We chose the current representation because it also has a neat description of the points on the elation line.

We mention an interesting property on this class of KM-arcs.

Theorem 4.7. *The $q/8$-secants of the elation KM-arc of type $q/8$ constructed in Theorem 4.4 define an $\mathbb{F}_2$-linear pencil, $q > 16$.*

It would be interesting to know whether Theorem 3.10 is valid for all KM-arcs of type $q/8$ (see also Remark 3.11).

In Theorem 4.11 we will give a negative answer to the question whether there are translation KM-arcs contained in the family of KM-arcs constructed in Theorem 4.4, but in order to prove this, we need some lemmas.

Lemma 4.8. *The KM-arc constructed in Theorem 4.4 is not a translation KM-arc with the elation line as translation line.*

Proof. We use the notation introduced in the statement of Theorem 4.4. The elation line ℓ is given by $X = 0$. We can see that $P_1(1, 0, 0)$, $P_2(1, \alpha_1, \beta_1)$ and $P(1, \alpha_2, \beta_1 + \beta_2)$ are points of $\mathcal{A}$. The unique translation τ with translation line ℓ mapping P_1 onto P_2 is given by $\left(\begin{smallmatrix} 1 & 0 & 0 \\ \alpha_1 & 1 & 0 \\ \beta_1 & 0 & 1 \end{smallmatrix}\right)$. Then P^τ is $(1, \alpha_1 + \alpha_2, \beta_2)$. From the construction it follows that all points of $\mathcal{A}$ on the line $Y + (\alpha_1 + \alpha_2)X = 0$ can be written as $(1, \alpha_1 + \alpha_2, t)$ with $\operatorname{Tr}(\alpha_1 t) = 0$ and $\operatorname{Tr}(\alpha_2 t) = \operatorname{Tr}(\alpha_3 t) = 1$. Since $\operatorname{Tr}(\alpha_3 \beta_2) = 0$, the point P^τ is not in $\mathcal{A}$. Hence, $\mathcal{A}$ is not a translation KM-arc. □

Instead of this direct proof we could have applied [2, Theorem 2.2], but that would not have made the calculations easier.

It is clear that for any set $\{\alpha_1, \alpha_2, \alpha_3\} \subset \mathbb{F}_q$ that is an $\mathbb{F}_2$-independent triple, we can construct a KM-arc in $\mathrm{PG}(2, q)$ through Theorem 4.4. However some of the obtained KM-arcs will be $\mathrm{P\Gamma L}$-equivalent.

We first prove that the construction in Theorem 4.4 only depends on the subgroup $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$ and not on the choice of $\alpha_1, \alpha_2, \alpha_3$.

Lemma 4.9. *Let $\{\alpha_1, \alpha_2, \alpha_3\} \subset \mathbb{F}_q^*$ and $\{\alpha_1', \alpha_2', \alpha_3'\} \subset \mathbb{F}_q^*$ be $\mathbb{F}_2$-independent sets such that $\langle \alpha_1, \alpha_2, \alpha_3 \rangle = \langle \alpha_1', \alpha_2', \alpha_3' \rangle$. Let $\mathcal{A}$ be the KM-arc constructed through Theorem 4.4 using the triple $(\alpha_1, \alpha_2, \alpha_3)$ and let $\mathcal{A}'$ be the KM-arc constructed through Theorem 4.4 using the triple $(\alpha_1', \alpha_2', \alpha_3')$. Then $\mathcal{A}$ and $\mathcal{A}'$ are* PGL*-equivalent.*

Proof. We can find a matrix $M \in \mathrm{GL}_3(\mathbb{F}_2)$ such that $(\alpha_1, \alpha_2, \alpha_3)M = (\alpha_1', \alpha_2', \alpha_3')$. The multiplicative group $\mathrm{GL}_3(\mathbb{F}_2)$ can be generated by the matrices $M_1 = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$ and $M_2 = \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right)$ and hence it is sufficient to prove the statement for $M = M_1$ and for $M = M_2$. Let $\beta_1, \beta_2, \beta_3$ be as in the construction presented in Theorem 4.4, so $\operatorname{Tr}(\alpha_i \beta_j) = 1$.

We first look at $M = M_1$. In this case $(\alpha_1', \alpha_2', \alpha_3') = (\alpha_1 + \alpha_2, \alpha_2, \alpha_3)$. Then $(\beta_1', \beta_2', \beta_3') = (\beta_1, \beta_1 + \beta_2, \beta_3)$ fulfils $\operatorname{Tr}(\alpha_i' \beta_j') = \delta_{i,j}$. We know that the construction in Theorem 4.4 does not depend on the choice of the coset leaders. So, when constructing the KM-arc using the triple $(\alpha_1', \alpha_2', \alpha_3')$ we may use $\beta_1', \beta_2', \beta_3'$ as coset leaders. The point set of $\mathcal{A}$ is given by $\mathcal{S}_0 \cup \bigcup_{v \in \mathbb{F}_2^3} \mathcal{S}_v$ with

$$\mathcal{S}_0 = \{(0, 1, x) \mid \forall i : \operatorname{Tr}(\alpha_i^2 x) = 0\} \text{ and}$$
$$\mathcal{S}_{(\lambda_1, \lambda_2, \lambda_3)} = \left\{ \left(1, \sum_{i=1}^{3} \lambda_i \alpha_i, \sum_{i=1}^{3} f_i(\lambda_1, \lambda_2, \lambda_3)\beta_i + s\right) \,\middle|\, s \in S \right\},$$

and the point set of $\mathcal{A}'$ is given by $\mathcal{S}_0' \cup \bigcup_{v \in \mathbb{F}_2^3} \mathcal{S}_v'$ with

$$\mathcal{S}_0' = \{(0, 1, x) \mid \forall i : \operatorname{Tr}(\alpha_i'^2 x) = 0\} \text{ and}$$
$$\mathcal{S}'_{(\lambda_1, \lambda_2, \lambda_3)} = \left\{ \left(1, \sum_{i=1}^{3} \lambda_i \alpha_i', \sum_{i=1}^{3} f_i(\lambda_1, \lambda_2, \lambda_3)\beta_i' + s\right) \,\middle|\, s \in S \right\}.$$

We know that $\langle \alpha_1^2, \alpha_2^2, \alpha_3^2 \rangle = \langle \alpha_1'^2, \alpha_2'^2, \alpha_3'^2 \rangle$. Keeping this in mind and using the above expressions for the α_i''s and β_i''s, it can readily be checked that the collineation induced by the matrix $\left(\begin{smallmatrix} 1 & 0 & 0 \\ \alpha_2+\alpha_3 & 1 & 0 \\ \beta_1+\beta_3 & 0 & 1 \end{smallmatrix}\right)$ maps $\mathcal{A}$ onto $\mathcal{A}'$.

Now we look at the case $M = M_2$, hence at $(\alpha_1', \alpha_2', \alpha_3') = (\alpha_3, \alpha_1, \alpha_2)$. Then $(\beta_1', \beta_2', \beta_3') = (\beta_3, \beta_1, \beta_2)$ fulfils $\operatorname{Tr}(\alpha_i' \beta_j') = \delta_{i,j}$. Again we can construct $\mathcal{A}'$ (note that $\mathcal{A}$ is as above). Here we can check that the collineation induced by the matrix $\left(\begin{smallmatrix} 1 & 0 & 0 \\ \alpha_1+\alpha_2 & 1 & 0 \\ \beta_2+\beta_3 & 0 & 1 \end{smallmatrix}\right)$ maps $\mathcal{A}$ onto $\mathcal{A}'$. □

Lemma 4.10. *Let $\mathcal{A}$ be a KM-arc of type $q/8$ in $\mathrm{PG}(2, q)$ obtained by the construction in Theorem 4.4 using the admissible tuple $(\alpha_1, \alpha_2, \alpha_3)$ and let $\mathcal{A}'$ be a KM-arc of type $q/8$ in $\mathrm{PG}(2, q)$ obtained by the construction in Theorem 4.4 using $(k\alpha_1^\varphi, k\alpha_2^\varphi, k\alpha_3^\varphi)$, with $k \in \mathbb{F}_q^*$ and φ a field automorphism of $\mathbb{F}_q$. Then $\mathcal{A}$ and $\mathcal{A}'$ are* $\mathrm{P\Gamma L}$*-equivalent.*

Proof. Denote the set $\{s \mid \forall i : \operatorname{Tr}(\alpha_i s) = 0\}$ by S and the set $\{s \mid \forall i : \operatorname{Tr}(k\alpha_i^\varphi s) = 0\}$ by S'. These sets are used in the construction of $\mathcal{A}$ and $\mathcal{A}'$, respectively. Let γ be the collineation induced by the matrix $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & k & 0 \\ 0 & 0 & k^{-1} \end{smallmatrix}\right)$ and the field automorphism φ. Then $\mathcal{A}^\gamma = \mathcal{A}'$ since

$$\begin{aligned}
\{k^{-1}s^\varphi \mid s \in S\} &= \{k^{-1}s^\varphi \mid \forall i : \mathrm{Tr}(\alpha_i s) = 0\} = \{k^{-1}s^\varphi \mid \forall i : \mathrm{Tr}(\alpha_i^\varphi s^\varphi) = 0\} \\
&= \{k^{-1}t \mid \forall i : \mathrm{Tr}(\alpha_i^\varphi t) = 0\} = \{s \mid \forall i : \mathrm{Tr}(\alpha_i^\varphi ks) = 0\} = S' \ , \\
\{(0,k,k^{-1}x^\varphi) \mid \forall i : \mathrm{Tr}(\alpha_i^2 x) = 0\} &= \{(0,1,k^{-2}x^\varphi) \mid \forall i : \mathrm{Tr}(\alpha_i^2 x) = 0\} \\
&= \{(0,1,k^{-2}x^\varphi) \mid \forall i : \mathrm{Tr}((\alpha_i^\varphi)^2 x^\varphi) = 0\} \\
&= \{(0,1,x) \mid \forall i : \mathrm{Tr}((k\alpha_i^\varphi)^2 x) = 0\}
\end{aligned}$$

and $\mathrm{Tr}((k\alpha_i^\varphi)(k^{-1}\beta_j^\varphi)) = \delta_{i,j}$. In both calculations we used that $\mathrm{Tr}(x^\varphi) = \mathrm{Tr}(x)$ for the arbitrary field automorphism φ and for any $x \in \mathbb{F}_q$. □

Combining the previous lemma with Lemma 4.8 yields that the constructed KM-arcs are not translation KM-arcs.

Theorem 4.11. *If $\mathcal{A}$ is a KM-arc in* $\mathrm{PG}(2,q)$ *arising from the construction in Theorem 4.4, then $\mathcal{A}$ is not a translation KM-arc.*

Proof. For $q = 16$ this result will follow from Theorem 4.12. Let $\mathcal{A}$ be a KM-arc in $\mathrm{PG}(2,q)$, $q \geq 32$, constructed through Theorem 4.4 using the admissible tuple $(\alpha_1, \alpha_2, \alpha_3)$. We assume that $\mathcal{A}$ is a translation KM-arc. By [6, Prop. 6.2] (see also Theorem 1.4) the translation line must be a $q/8$-secant of $\mathcal{A}$. It follows from Theorem 4.8 that the translation line cannot be the elation line. So we assume that the translation line is a $q/8$-secant different from the elation line. Then, the subgroups $\{x \in \mathbb{F}_q \mid \forall i : \mathrm{Tr}(\alpha_i x) = 0\}$ and $\{x \in \mathbb{F}_q \mid \forall i : \mathrm{Tr}(\alpha_i^2 x) = 0\}$ have to coincide, hence the subgroups $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$ and $\langle \alpha_1^2, \alpha_2^2, \alpha_3^2 \rangle$ coincide. By Lemma 4.9, for every $k \in \mathbb{F}_q^*$, the admissible tuple $(k\alpha_1, k\alpha_2, k\alpha_3)$, gives rise to a KM-arc $\mathcal{A}'$ $\mathrm{P\Gamma L}$-equivalent to $\mathcal{A}$, which is hence also a translation KM-arcs. As before, we find that the subgroups $\langle k\alpha_1, k\alpha_2, k\alpha_3 \rangle$ and $\langle k^2\alpha_1^2, k^2\alpha_2^2, k^2\alpha_3^2 \rangle$ coincide. It follows that for all $k \in \mathbb{F}_q^*$, the subgroups $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$ and $k\langle \alpha_1, \alpha_2, \alpha_3 \rangle$ coincide, a contradiction, so the assumption is false. □

We now discuss the construction of Theorem 4.4 for $q = 16$ and 32. For $q = 16$ the construction of Theorem 4.4 yields a hyperoval in $\mathrm{PG}(2,16)$. It is long known that up to isomorphism there are only two hyperovals in $\mathrm{PG}(2,16)$: the regular hyperoval and the Lunelli-Sce hyperoval ([4, 11]). The regular hyperoval has a stabiliser isomorphic to $\mathrm{P\Gamma L}(2,q)$ and hence has order 16320, while the Lunelli-Sce has a stabiliser of order 144 (see [11, 12]).

Theorem 4.12. *For all admissible triples, the construction of Theorem 4.4 for $q = 16$ gives rise to the same hyperoval in* $\mathrm{PG}(2,16)$ *up to* $\mathrm{P\Gamma L}$*-equivalence; this hyperoval is the Lunelli-Sce hyperoval.*

Proof. By Lemma 4.9 we know that the projective equivalence class of the KM-arc does not depend on the choice of the parameters $\alpha_1, \alpha_2, \alpha_3$ (using the notation of Theorem 4.4) but only on the additive subgroup they generate. We know that $\mathbb{F}_{16}$ has precisely 15 additive subgroups of order 8. For any subgroup S of order 8 and any $k \in \mathbb{F}_{16}^* \setminus \{1\}$ clearly $kS \neq S$, so the 15 additive subgroups of order 8 can be written as kT with $k \in \mathbb{F}_{16}^*$ and T a fixed subgroup of order 8. By Theorem 4.10 we then know that all admissible triples give rise to the same hyperoval up to projective equivalence. Using the GAP-package FinInG ([1]) we computed the stabiliser of one KM-arc in $\mathrm{PG}(2,16)$ constructed through Theorem 4.4. We found it to have size 144, hence the conclusion. □

Remark 4.13. The KM-arcs of type 4 in $\mathrm{PG}(2,32)$ have been classified up to projective equivalence in [14, Result 2.14]. There are 8 equivalence classes. One of these classes was already described in [5]. It is straightforward to check that only one of the 8 given KM-arcs is an elation KM-arc, the one whose affine points are given by $\{(1, f(z), z) \mid z \in \mathbb{F}_{32}\}$ with $f(z) = z^{24} + z^{20} + \alpha^{18}z^{18} + \alpha^5 z^{16} + \alpha^2 z^{12} + \alpha^{18}z^{10} + \alpha^{18}z^8 + \alpha^{23}z^6 + \alpha^5 z^4 + \alpha^{22}z^2 + \alpha^{26}z$. The following result is immediate.

Theorem 4.14. *For all admissible triples the construction of Theorem 4.4 for $q = 32$ gives rise to the same elation KM-arc of type* 4 *in* $\mathrm{PG}(2,32)$ *up to* $\mathrm{P\Gamma L}$*-equivalence.*

Using the above results we can now give a computer free proof of this result.

Proof. By Lemma 4.9 we know that the projective equivalence class of the KM-arc only depends on the additive subgroup $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$ with $\alpha_1, \alpha_2, \alpha_3$ as in the statement of Theorem 4.4. It is immediate that $\mathbb{F}_{32}$ has 155 additive subgroups of order 8. By Lemma 4.10 we also know that for any subgroup T the KM-arcs arising from T and kT^φ, respectively, are $\mathrm{P\Gamma L}$-equivalent for any $k \in \mathbb{F}_{32}^*$ and any field automorphism φ of $\mathbb{F}_{32}$.

Assume that $\langle \alpha_1, \alpha_2, \alpha_3 \rangle_2^{\varphi} = k \langle \alpha_1, \alpha_2, \alpha_3 \rangle$, with $k \in \mathbb{F}_{32}^*$ and $\varphi \in \mathrm{Aut}(\mathbb{F}_{32})$. Then we can find a matrix $A \in \mathrm{GL}_3(\mathbb{F}_2)$ such that $(\alpha_1^{\varphi}, \alpha_2^{\varphi}, \alpha_3^{\varphi}) = k(\alpha_1, \alpha_2, \alpha_3)A$. Applying this repetitively it follows that

$$(\alpha_1, \alpha_2, \alpha_3) = (\alpha_1^{\varphi^5}, \alpha_2^{\varphi^5}, \alpha_3^{\varphi^5}) = k^{1+\varphi+\varphi^2+\varphi^3+\varphi^4}(\alpha_1, \alpha_2, \alpha_3)A^5 = (\alpha_1, \alpha_2, \alpha_3)A^5$$

since $\mathrm{Aut}(\mathbb{F}_{32})$ is a cyclic group of order 5 which implies that $k^{1+\varphi+\varphi^2+\varphi^3+\varphi^4} = k^{31} = 1$. As $|\operatorname{GL}_3(\mathbb{F}_2)| = 168$, the matrix A cannot have order 5, so A is the identity matrix; here we also use that $\alpha_1, \alpha_2, \alpha_3$ are $\mathbb{F}_2$-independent. We find that $\alpha_i^{\varphi} = k\alpha_i$ for $i = 1, 2, 3$. Consequently, $\frac{\alpha_1}{\alpha_2}$ is fixed by φ. As $\mathbb{F}_2$ is the only subfield of $\mathbb{F}_{32}$ and $\alpha_1 \neq \alpha_2$, the field automorphism φ must be trivial, and so also $k = 1$.

So, for a fixed additive subgroup T of order 8 in $\mathbb{F}_{32}$ all subgroups kT^{φ}, with $k \in \mathbb{F}_{32}^*$ and $\varphi \in \mathrm{Aut}(\mathbb{F}_{32})$, are different. For a fixed T there are thus $31 \cdot 5 = 155$ subgroups of the form kT^{φ}. We conclude that all subgroups of order 8 in $\mathbb{F}_{32}$ give rise to the same KM-arc of type 4 up to projective equivalence. □

From [16] we also know that the stabiliser G_{32} of this unique elation KM-arc $\mathcal{A}_{32}$ of type 4 is a group of order 16. So, next to the four elations (including the identity) that G_{32} contains by definition, there are other collineations stabilising $\mathcal{A}_{32}$; all of them fix only one point, the 4-nucleus. It is clear that $\mathcal{A}_{32}$ is not translation.

Now we cover the larger values for q. First we recall a result from [3]. It learns us that the iterative process admitted by Construction 2 (C) does not always construct 'new' examples.

Theorem 4.15 ([3, Remark 1])**.** *If $\mathcal{A}$ is the KM-arc in $\mathrm{PG}(2, q^h)$ obtained from a hyperoval $\mathcal{H}$ in $\mathrm{PG}(2, q)$, q even, through Construction 2 (A) or (B), and $\mathcal{A}'$ is the KM-arc in $\mathrm{PG}(2, q^{hr})$ obtained from $\mathcal{A}$ through Construction 2 (C), then $\mathcal{A}'$ also arises from $\mathcal{H}$ through a direct application of Construction 2 (A) or (B).*

The proof of this theorem is straightforward; it can immediately be deduced from the descriptions in Construction 2. We now present an analogous theorem for the KM-arcs constructed in this section.

Theorem 4.16. *Let $\mathcal{A}_0$ be the KM-arc of type $q/8$ in $\mathrm{PG}(2, q)$, q even, with $q/8$-nucleus $N(0, 0, 1)$ and elation line $X = 0$ constructed from Theorem 4.4 by the admissible tuple $(\alpha_1, \alpha_2, \alpha_3)$ and let β be a collineation that stabilises N. Let $\mathcal{A}'$ be a KM-arc of type $q^h/8$ in $\mathrm{PG}(2, q^h)$ obtained from $\mathcal{A}_0^{\beta}$ through Construction 2 (B) or (C). Then $\mathcal{A}'$ is $\mathrm{P\Gamma L}$-equivalent to a KM-arc in $\mathrm{PG}(2, q^h)$ obtained by the construction in Theorem 4.4 using the admissible tuple $(\alpha_1, \alpha_2, \alpha_3)$.*

Proof. We denote the trace function $\mathbb{F}_{q^h} \to \mathbb{F}_2$ by Tr_{q^h}, the trace function $\mathbb{F}_q \to \mathbb{F}_2$ by Tr_q and the trace function $\mathbb{F}_{q^h} \to \mathbb{F}_q$ by $\mathrm{Tr}_{q^h,q}$.

We define $S = \{x \in \mathbb{F}_q \mid \forall i : \mathrm{Tr}_q(\alpha_i x) = 0\}$. Then $\mathcal{A}_0$ is given by $\mathcal{S}_0 \cup \bigcup_{v \in \mathbb{F}_2^3} \mathcal{S}_v$ with

$$\mathcal{S}_{(\lambda_1,\lambda_2,\lambda_3)} = \left\{ \left(1, \sum_{i=1}^{3} \lambda_i \alpha_i, \sum_{i=1}^{3} f_i(\lambda_1, \lambda_2, \lambda_3)\beta_i + s\right) \middle| \; s \in S \right\}$$

and $\mathcal{S}_0 = \{(0, 1, x) \mid \forall j : \mathrm{Tr}_q(\alpha_j^2 x) = 0\}$. Here, $\beta_1, \beta_2, \beta_3 \in \mathbb{F}_q$ are such that $\mathrm{Tr}_q(\alpha_i \beta_j) = \delta_{i,j}$. The collineation β is defined by a matrix $C = \left(\begin{smallmatrix} a_{00} & a_{01} & 0 \\ a_{10} & a_{11} & 0 \\ a_{20} & a_{21} & 1 \end{smallmatrix}\right)$ and an automorphism ϕ of $\mathbb{F}_q$.

Let $k \in \mathbb{F}_{q^h}$ be such that $\mathrm{Tr}_{q^h,q}(k) = 1$; such an element can always be found. Now, we define $S' = \{x \in \mathbb{F}_{q^h} \mid \forall i : \mathrm{Tr}_{q^h}(k\alpha_i x) = 0\}$. On the one hand, for any element $x \in \mathbb{F}_q \subseteq \mathbb{F}_{q^h}$ we know that $\mathrm{Tr}_{q^h}(k\alpha_i x) = \mathrm{Tr}_q(\alpha_i x \,\mathrm{Tr}_{q^h,q}(k)) = \mathrm{Tr}_q(\alpha_i x)$. Hence, $S' \cap \mathbb{F}_q = S$. On the other hand, for any element $x \in \mathbb{F}_{q^h}$ with $\mathrm{Tr}_{q^h,q}(kx) = 0$ we know that $\mathrm{Tr}_{q^h}(k\alpha_i x) = \mathrm{Tr}_q(\alpha_i \,\mathrm{Tr}_{q^h,q}(kx)) = 0$. Moreover, if $x \in \mathbb{F}_q \subseteq \mathbb{F}_{q^h}$ admits $\mathrm{Tr}_{q^h,q}(kx) = 0$ then $x = 0$. So the set $I = \{x \in \mathbb{F}_{q^h} \mid \mathrm{Tr}_{q^h,q}(kx) = 0\}$ is a direct complement of $\mathbb{F}_q$ in $\mathbb{F}_{q^h}$ such that $S' = \langle S, I \rangle$. We can also find an automorphism ϕ' of $\mathbb{F}_{q^h}$ of which ϕ is the restriction to $\mathbb{F}_q$. Then $I^{\phi'}$ is also a direct complement of $\mathbb{F}_q$ in $\mathbb{F}_{q^h}$.

By Remark 1.6 we may use $I^{\phi'}$ in the construction of $\mathcal{A}'$ without loss of generality. The KM-arc $\mathcal{A}'$ is then given by $\mathcal{S}'_0 \cup \bigcup_{v \in \mathbb{F}_2^3} \mathcal{S}'_v$ with $\mathcal{S}'_0 = \{(0, 1, x^{\phi} + i^{\phi'})C^t \mid \forall j : \mathrm{Tr}_q(\alpha_j^2 x) = 0, i \in I\}$ and

$$\begin{aligned} \mathcal{S}'_{(\lambda_1,\lambda_2,\lambda_3)} &= \left\{ \left(1, \sum_{i=1}^{3} \lambda_i \alpha_i^{\phi}, \sum_{i=1}^{3} f_i(\lambda_1, \lambda_2, \lambda_3)\beta_i^{\phi} + s^{\phi} + i^{\phi'}\right) C^t \middle| \; s \in S, i \in I \right\} \\ &= \left\{ \left(1, \sum_{i=1}^{3} \lambda_i \alpha_i^{\phi}, \sum_{i=1}^{3} f_i(\lambda_1, \lambda_2, \lambda_3)\beta_i^{\phi} + s^{\phi'}\right) C^t \middle| \; s \in S' \right\} . \end{aligned}$$

We define the KM-arc $\mathcal{A}''$ in $\mathrm{PG}(2,q^h)$ using the parameters $k\alpha_1, k\alpha_2, k\alpha_3$. Its point set is given by $\mathcal{S}_0''\cup\bigcup_{v\in\mathbb{F}_2^3}\mathcal{S}_v''$ with $\mathcal{S}_0''=\{(0,1,x)\mid\forall j:\mathrm{Tr}_{q^h}(k^2\alpha_j^2x)=0\}$ and

$$\mathcal{S}''_{(\lambda_1,\lambda_2,\lambda_3)}=\left\{\left(1,k\sum_{i=1}^{3}\lambda_i\alpha_i,\sum_{i=1}^{3}f_i(\lambda_1,\lambda_2,\lambda_3)\beta_i+s\right)\,\middle|\, s\in S'\right\}\ .$$

Note that $\beta_1,\beta_2,\beta_3\in\mathbb{F}_q\subseteq\mathbb{F}_{q^h}$ fulfil $\mathrm{Tr}_{q^h}((k\alpha_i)\beta_j)=\mathrm{Tr}_q(\alpha_i\beta_j)=\delta_{i,j}$. Let γ be the collineation induced by the $\mathbb{F}_{q^h}$-automorphism ϕ' and the matrix $C'=C\begin{pmatrix}1&0&0\\0&(k^{\phi'})^{-1}&0\\0&0&1\end{pmatrix}$ where we interpret C over $\mathbb{F}_{q^h}$. It is immediate that $\left(\mathcal{S}''_{(\lambda_1,\lambda_2,\lambda_3)}\right)^\gamma=\mathcal{S}'_{(\lambda_1,\lambda_2,\lambda_3)}$ for all $(\lambda_1,\lambda_2,\lambda_3)\in\mathbb{F}_2^3$. Furthermore,

$$\begin{aligned}(\mathcal{S}_0'')^\gamma&=\{(0,(k^{\phi'})^{-1},x^{\phi'})C^t\mid\forall j:\mathrm{Tr}_{q^h}(k^2\alpha_j^2x)=0\}\\&=\{(0,1,(kx)^{\phi'})C^t\mid\forall j:\mathrm{Tr}_{q^h}(k^2\alpha_j^2x)=0\}\\&=\{(0,1,y^{\phi'})C^t\mid\forall j:\mathrm{Tr}_{q^h}(k\alpha_j^2y)=0\}\ .\end{aligned}$$

So, $(\mathcal{S}_0'')^\gamma=\mathcal{S}_0'$ iff $\mathrm{Tr}_{q^h}(k\alpha_j^2(x+i))=0$ for all $i\in I$ and all $x\in\mathbb{F}_q$ such that $\mathrm{Tr}_q(\alpha_j^2x)=0$. We find

$$\mathrm{Tr}_{q^h}(k\alpha_j^2(x+i))=\mathrm{Tr}_{q^h}(k\alpha_j^2x)+\mathrm{Tr}_{q^h}(k\alpha_j^2i)=\mathrm{Tr}_q(\alpha_j^2x\,\mathrm{Tr}_{q^h,q}(k))+\mathrm{Tr}_q(\alpha_j^2\,\mathrm{Tr}_{q^h,q}(ki))=0$$

by the definition of k and the definition of I. We conclude that $\mathcal{A}'=(\mathcal{A}'')^\gamma$. This proves the theorem since the tuples $(\alpha_1,\alpha_2,\alpha_3)$ and $(k\alpha_1,k\alpha_2,k\alpha_3)$ give rise to PΓL-equivalent KM-arcs by Lemma 4.10. □

We now discuss in detail the result of Theorem 4.4 and Corollary 4.5.

Remark 4.17. In $\mathrm{PG}(2,q)$, $q=2^h$, with $3\mid h$, KM-arcs of type $q/8$ were known to exist through Constructions 1 and 2 (A). However, since all o-polynomials in $\mathbb{F}_8$ give rise to a translation hyperoval (see [13]), all these KM-arcs are translation KM-arcs. By Theorem 4.15 all KM-arcs of type $q/8$ that are constructed through applying Construction 2 (C) on the previous ones, are also translation KM-arcs.

In $\mathrm{PG}(2,q)$, $q=2^h$, with $4\mid h$, KM-arcs of type $q/8$ were known to exist through Construction 2 (B). By Theorem 4.15 all KM-arcs that arise through Constructions 2 (B) and (C) arise from a hyperoval in $\mathrm{PG}(2,16)$. They are all elation KM-arcs.

In $\mathrm{PG}(2,q)$, $q=2^h$, with $5\mid h$, KM-arcs of type $q/8$ were known to exist through Remark 4.13 and Construction 2 (C). By Lemmas 2.4 and 2.5 this family contains both elation and non-elation KM-arcs.

By Theorem 4.11 we know that the KM-arcs constructed through Theorem 4.4 are not translation KM-arcs. We now elaborate on Corollary 4.5. For the discussion of the existence results of KM-arcs of type $q/8$ in $\mathrm{PG}(2,q)$, $q=2^h$, the residue class of h modulo 60 is what matters. If $h\not\equiv 0\pmod{m}$ for $m=3,4,5$ (there are 24 out of 60 residue classes in this case), then the existence of KM-arcs of type $q/8$ in $\mathrm{PG}(2,q)$ was previously not known. If h is divisible by 3, but not by 4 or 5 (there are 12 residue classes in this case), then the existence of KM-arcs of type $q/8$ in $\mathrm{PG}(2,q)$ was previously known, but all known examples are translation KM-arcs and hence different from the examples we introduced in Theorem 4.4 as they are not translation KM-arcs. If h is divisible by 4 or by 5 (there are 24 residue classes in this case), then the set of KM-arcs constructed in Theorem 4.4 does not necessarily contain previously unknown examples. E.g. for $h=4,5$ this construction provides no new KM-arcs.

5 A new family of elation KM-arcs of type $q/16$

In this section we first present the construction of a family of KM-arcs of type $q/16$ in $\mathrm{PG}(2,q)$, based on the idea underlying the construction of KM-arcs of type $q/8$ in Theorem 4.4. Afterwards we will discuss this family of KM-arcs. We start with a small technical lemma.

Lemma 5.1. *Let $\alpha_1,\alpha_2,\alpha_3,\alpha_4\in\mathbb{F}_q^*$ be $\mathbb{F}_2$-independent. If $\frac{\alpha_i^2}{\alpha_4}\in\langle\alpha_1,\alpha_2,\alpha_3,\alpha_4\rangle$ for $i=1,2,3$, then we can find an $\alpha\in\langle\alpha_1,\alpha_2,\alpha_3,\alpha_4\rangle$ such that $\{\alpha_1(\alpha_1+\alpha_4),\alpha_2(\alpha_2+\alpha_4),\alpha_3(\alpha_3+\alpha_4),\alpha_4\alpha\}$ is an $\mathbb{F}_2$-independent set.*

Proof. If the triple $(\mu_1, \mu_2, \mu_3) \in \mathbb{F}_2^{3*}$ admits $\sum_{i=1}^3 \mu_i\alpha_i(\alpha_i+\alpha_4) = 0$, then $\left(\sum_{i=1}^3 \mu_i\alpha_i\right)\left(\alpha_4 + \sum_{i=1}^3 \mu_i\alpha_i\right) = 0$, contradicting that $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ is an $\mathbb{F}_2$-independent set, so $\{\alpha_1(\alpha_1+\alpha_4), \alpha_2(\alpha_2+\alpha_4), \alpha_3(\alpha_3+\alpha_4)\}$ is an $\mathbb{F}_2$-independent set.

Since $\frac{\alpha_i^2}{\alpha_4} \in \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4\rangle$ for $i = 1, 2, 3$, there exist $a_{i,j} \in \mathbb{F}_2$ such that $\alpha_i^2 = \alpha_4\left(\sum_{j=1}^4 a_{i,j}\alpha_j\right)$. Let (b_1, b_2, b_3, b_4) be a vector in $\mathbb{F}_2^4$ which is not contained in the hyperplane

$$\langle (a_{1,1}+1, a_{1,2}, a_{1,3}, a_{1,4}), (a_{2,1}, a_{2,2}+1, a_{2,3}, a_{2,4}), (a_{3,1}, a_{3,2}, a_{3,3}+1, a_{3,4})\rangle \ .$$

We then know that for $\alpha = \sum_{i=1}^4 b_i\alpha_i$, the set $\{\alpha_1(\alpha_1+\alpha_4), \alpha_2(\alpha_2+\alpha_4), \alpha_3(\alpha_3+\alpha_4), \alpha_4\alpha\}$ is $\mathbb{F}_2$-independent. □

Now we present the construction. By the previous lemma we know that the existence of an α satisfying the condition in the theorem is guaranteed.

Theorem 5.2. *Let $q = 2^h$, $h > 5$, let $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{F}_q^*$ be $\mathbb{F}_2$-independent and define $S = \{x \in \mathbb{F}_q \mid \forall i : \mathrm{Tr}(\alpha_i x) = 0\}$. Assume that $\frac{\alpha_i^2}{\alpha_4} \in \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4\rangle$ for $i = 1, 2, 3$, and let $\alpha \in \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4\rangle$ be such that $\{\alpha_1(\alpha_1+\alpha_4), \alpha_2(\alpha_2+\alpha_4), \alpha_3(\alpha_3+\alpha_4), \alpha_4\alpha\}$ is an $\mathbb{F}_2$-independent set. Let $\beta_1, \beta_2, \beta_3 \in \mathbb{F}_q^*$ be such that $\mathrm{Tr}(\alpha_i\beta_j) = \delta_{i,j}$ for $i = 1, \dots, 4$ and $j = 1, 2, 3$, and let f_1, f_2, f_3 be as in Theorem 4.4.*

For any $\overline{\lambda} = (\lambda_1, \dots, \lambda_4) \in \mathbb{F}_2^4$ we define

$$\mathcal{S}_{\overline{\lambda}} = \left\{ \left(1, \sum_{i=1}^4 \lambda_i\alpha_i, \sum_{i=1}^3 f_i(\lambda_1, \lambda_2, \lambda_3)\beta_i + s\right) \,\middle|\, s \in S \right\} \ .$$

We also define $\mathcal{S}_0 = \{(0, 1, x) \mid \mathrm{Tr}(\alpha_i(\alpha_i+\alpha_4)x) = 0,\ i = 1, 2, 3 \ \wedge\ \mathrm{Tr}(\alpha_4\alpha x) = 1\}$. The point set $\mathcal{A} = \mathcal{S}_0 \cup \bigcup_{v\in\mathbb{F}_2^4} \mathcal{S}_v$ is an elation KM-arc of type $q/16$ in $\mathrm{PG}(2, q)$ with elation line $X = 0$ and $q/16$-nucleus $(0, 0, 1)$.

Proof. We follow the approach from the proof of Theorem 4.4. We know that S is a subgroup of $(\mathbb{F}_q, +)$ containing $q/16$ elements. The existence of elements $\beta_1, \beta_2, \beta_3$ is guaranteed as they are coset leaders of cosets of S (note that not all cosets of S are involved).

It is immediate that the points of $\mathcal{S}_{\overline{\lambda}}$, with $\overline{\lambda} = (\lambda_1, \lambda_2, \lambda_3, \lambda_4) \in \mathbb{F}_2^4$, are on the line $\ell_{\overline{\lambda}}$ with equation $(\sum_{i=1}^4 \lambda_i\alpha_i)X + Y = 0$ and that the points of $\mathcal{S}_0$ are on the line ℓ_∞ with equation $X = 0$. Hence, all lines through $N(0, 0, 1)$ either contain $q/16$ or 0 points of $\mathcal{A}$.

Now we check that three points on different $q/16$-secants are not collinear. First we assume that ℓ_∞ is not among these three $q/16$-secants. Then the three points can be described as

$$\left(1, \sum_{i=1}^4 \lambda_i\alpha_i, \sum_{i=1}^3 f_i(\widetilde{\lambda})\beta_i + s\right), \left(1, \sum_{i=1}^4 \lambda_i'\alpha_i, \sum_{i=1}^3 f_i(\widetilde{\lambda}')\beta_i + s'\right) \text{ and } \left(1, \sum_{i=1}^4 \lambda_i''\alpha_i, \sum_{i=1}^3 f_i(\widetilde{\lambda}'')\beta_i + s''\right)$$

with $\overline{\lambda} = (\lambda_1, \lambda_2, \lambda_3, \lambda_4)$, $\overline{\lambda}' = (\lambda_1', \lambda_2', \lambda_3', \lambda_4')$ and $\overline{\lambda}'' = (\lambda_1'', \lambda_2'', \lambda_3'', \lambda_4'')$ three pairwise different vectors in $\mathbb{F}_2^4$, and $\widetilde{\lambda} = (\lambda_1, \lambda_2, \lambda_3)$, $\widetilde{\lambda}' = (\lambda_1', \lambda_2', \lambda_3')$ and $\widetilde{\lambda}'' = (\lambda_1'', \lambda_2'', \lambda_3'')$. We find that

$$\begin{aligned}\Delta &= \begin{vmatrix} 1 & \sum_{i=1}^4 \lambda_i\alpha_i & \sum_{i=1}^3 f_i(\widetilde{\lambda})\beta_i + s \\ 1 & \sum_{i=1}^4 \lambda_i'\alpha_i & \sum_{i=1}^3 f_i(\widetilde{\lambda}')\beta_i + s' \\ 1 & \sum_{i=1}^4 \lambda_i''\alpha_i & \sum_{i=1}^3 f_i(\widetilde{\lambda}'')\beta_i + s'' \end{vmatrix} \\ &= \sum_{cyc}\left(\sum_{i=1}^4\sum_{j=1}^3 (\lambda_i f_j(\widetilde{\lambda}') + \lambda_i' f_j(\widetilde{\lambda}))\alpha_i\beta_j + s\sum_{i=1}^4 \lambda_i'\alpha_i + s'\sum_{i=1}^4 \lambda_i\alpha_i\right)\end{aligned}$$

where the cyclic sum is taken over $(\overline{\lambda}, \overline{\lambda}', \overline{\lambda}'')$ and the corresponding $(\widetilde{\lambda}, \widetilde{\lambda}', \widetilde{\lambda}'')$ and (s, s', s''). We calculate the trace of both sides of this equation. Considering that $\mathrm{Tr}(\alpha_i t) = 0$ for all $t \in S$ and $i = 1, \dots, 4$, that $\mathrm{Tr}(\alpha_i\beta_j) = \delta_{i,j}$ and that the trace function is $\mathbb{F}_2$-linear, we find (completely analogous to (11)) that

$$\mathrm{Tr}(\Delta) = M_3^3(\widetilde{\lambda}, \widetilde{\lambda}', \widetilde{\lambda}'') \ .$$

It follows that $\Delta \neq 0$ if $\widetilde{\lambda}$, $\widetilde{\lambda}'$ and $\widetilde{\lambda}''$ are three pairwise disjoint vectors. Hence, in this case the three points are not collinear. Now we look at the case in which $\widetilde{\lambda}$, $\widetilde{\lambda}'$ and $\widetilde{\lambda}''$ are not three pairwise disjoint vectors. Without loss of generality we can assume that $\widetilde{\lambda}' = \widetilde{\lambda}''$. Since $\overline{\lambda}' \neq \overline{\lambda}''$, we know that also $\lambda_4' = \lambda_4'' + 1$. In this case

$$\Delta = \alpha_4 \sum_{j=1}^{3} (f_j(\widetilde{\lambda}) + f_j(\widetilde{\lambda}'))\beta_j + (s+s')\alpha_4 + (s'+s'') \sum_{i=1}^{4} (\lambda_i + \lambda_i')\alpha_i$$

Since $\overline{\lambda} \neq \overline{\lambda}'$ by assumption, we know that $\sum_{i=1}^4 (\lambda_i + \lambda_i')\alpha_i \neq 0$. So now we compute the trace of the following nonzero multiple of Δ:

$$\begin{aligned}
\operatorname{Tr}\left(\frac{\sum_{i=1}^4 (\lambda_i + \lambda_i')\alpha_i}{\alpha_4} \Delta \right) &= \sum_{i=1}^{4} \sum_{j=1}^{3} (\lambda_i + \lambda_i')(f_j(\widetilde{\lambda}) + f_j(\widetilde{\lambda}')) \operatorname{Tr}(\alpha_i \beta_j) \\
&\quad + \sum_{i=1}^{4} (\lambda_i + \lambda_i') \operatorname{Tr}((s+s')\alpha_i) + \operatorname{Tr}\left((s'+s'') \frac{\sum_{i=1}^4 (\lambda_i + \lambda_i')\alpha_i^2}{\alpha_4} \right) \\
&= \sum_{i=1}^{3} (\lambda_i + \lambda_i')(f_i(\widetilde{\lambda}) + f_i(\widetilde{\lambda}')) \\
&= (\lambda_1 + \lambda_1')(\lambda_1 + \lambda_2 + \lambda_3 + \lambda_2\lambda_3 + \lambda_1' + \lambda_2' + \lambda_3' + \lambda_2'\lambda_3') \\
&\quad + (\lambda_2 + \lambda_2')(\lambda_2 + \lambda_3 + \lambda_1\lambda_3 + \lambda_2' + \lambda_3' + \lambda_1'\lambda_3') \\
&\quad + (\lambda_3 + \lambda_3')(\lambda_3 + \lambda_1\lambda_2 + \lambda_3' + \lambda_1'\lambda_2') \\
&= M_2^3(\widetilde{\lambda}, \widetilde{\lambda}') \; .
\end{aligned}$$

In the second step we used that $\frac{\alpha_i^2}{\alpha_4} \in \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle$, hence that $\operatorname{Tr}\left(s\frac{\alpha_i^2}{\alpha_4} \right) = 0$ for all $s \in S$. In the final step we used that all elements of $\mathbb{F}_2$ equal their square. As $\overline{\lambda}$ differs from both $\overline{\lambda}'$ and $\overline{\lambda}''$, which only differ on the final entry, the vector $\widetilde{\lambda}$ has to be different from $\widetilde{\lambda}'$. It follows that $\Delta \neq 0$, hence, also in this case the three points are not collinear.

Now we assume that ℓ_∞ is among the three $q/16$-secants. Then, the three points can be described as

$$\left(1, \sum_{i=1}^{4} \lambda_i \alpha_i, \sum_{i=1}^{3} f_i(\widetilde{\lambda})\beta_i + s \right), \left(1, \sum_{i=1}^{4} \lambda_i' \alpha_i, \sum_{i=1}^{3} f_i(\widetilde{\lambda}')\beta_i + s' \right) \text{ and } (0,1,t)$$

with $\overline{\lambda} = (\lambda_1, \lambda_2, \lambda_3, \lambda_4)$ and $\overline{\lambda}' = (\lambda_1', \lambda_2', \lambda_3', \lambda_4')$ two different vectors in $\mathbb{F}_2^3$, $\widetilde{\lambda} = (\lambda_1, \lambda_2, \lambda_3)$ and $\widetilde{\lambda}' = (\lambda_1', \lambda_2', \lambda_3')$, and t such that $\operatorname{Tr}(\alpha_i(\alpha_i + \alpha_4)t) = 0$ for $i = 1, 2, 3$ and $\operatorname{Tr}(\alpha_4 \alpha t) = 1$. We find that

$$\Delta' = \begin{vmatrix} 0 & 1 & t \\ 1 & \sum_{i=1}^4 \lambda_i \alpha_i & \sum_{i=1}^3 f_i(\widetilde{\lambda})\beta_i + s \\ 1 & \sum_{i=1}^4 \lambda_i' \alpha_i & \sum_{i=1}^3 f_i(\widetilde{\lambda}')\beta_i + s' \end{vmatrix} = t \sum_{i=1}^{4} (\lambda_i + \lambda_i')\alpha_i + \sum_{i=1}^{3} (f_i(\widetilde{\lambda}) + f_i(\widetilde{\lambda}'))\beta_i + s + s' \; .$$

We know that $\overline{\lambda} + \overline{\lambda}' \neq 0$ and hence $\sum_{i=1}^4 (\lambda_i + \lambda_i')\alpha_i \neq 0$. We distinguish between two cases. First we assume that $\widetilde{\lambda} \neq \widetilde{\lambda}'$. We compute the trace of a nonzero multiple of Δ':

$$\begin{aligned}
\operatorname{Tr}\left(\left(\alpha_4 + \sum_{i=1}^{4} (\lambda_i + \lambda_i')\alpha_i \right) \Delta' \right) &= \sum_{i=1}^{4} (\lambda_i + \lambda_i') \operatorname{Tr}\left(t\alpha_i(\alpha_i + \alpha_4) \right) + \sum_{j=1}^{3} (f_j(\widetilde{\lambda}) + f_j(\widetilde{\lambda}')) \operatorname{Tr}(\alpha_4 \beta_j) \\
&\quad + \sum_{i=1}^{4} \sum_{j=1}^{3} (\lambda_i + \lambda_i')(f_j(\widetilde{\lambda}) + f_j(\widetilde{\lambda}')) \operatorname{Tr}(\alpha_i \beta_j) \\
&\quad + \sum_{i=1}^{4} (\lambda_i + \lambda_i') \operatorname{Tr}\left((s+s')\alpha_i \right) + \operatorname{Tr}\left(\alpha_4(s+s') \right) \\
&= \sum_{i=1}^{3} (\lambda_i + \lambda_i')(f_i(\widetilde{\lambda}) + f_i(\widetilde{\lambda}')) \\
&= M_2^3(\widetilde{\lambda}, \widetilde{\lambda}') \; .
\end{aligned}$$

In the penultimate step we used that $\mathrm{Tr}(\alpha_i(\alpha_i+\alpha_4)t)=0$ for $i=1,2,3$ (and trivially also for $i=4$) and that $\mathrm{Tr}(\alpha_i\beta_i)=\delta_{i,j}$. In the final step we used the calculations in (12). We find that $\Delta\neq 0$, hence the three points are not collinear.

If $\widetilde{\lambda}=\widetilde{\lambda}'$, then $\overline{\lambda}+\overline{\lambda}'=\alpha_4$. In this case $\Delta'=t\alpha_4+s+s'$. We know that

$$\mathrm{Tr}(\alpha\Delta')=\mathrm{Tr}(\alpha(t\alpha_4+s+s'))=1$$

because $\mathrm{Tr}(\alpha_4\alpha t)=1$ and $\alpha\in\langle\alpha_1,\alpha_2,\alpha_3,\alpha_4\rangle$. Again we find that $\Delta\neq 0$, hence the three points are not collinear

We conclude that all lines not through N contain at most two points of $\mathcal{A}$. For any point $P\in\mathcal{A}$ there are q points of $\mathcal{A}$ not on the $q/16$-secant $\ell_P=\langle P,N\rangle$ so all q lines through P different from ℓ_P contain precisely two points of $\mathcal{A}$. Consequently, all lines of $\mathrm{PG}(2,q)$ contain 0, 2 or $q/16$ points of $\mathcal{A}$. So, $\mathcal{A}$ is a KM-arc of type $q/16$. From its definition and Lemma 2.1 it follows immediately that $\mathcal{A}$ is an elation KM-arc with elation line $X=0$. □

Remark 5.3. It is clear from the proof of Lemma 5.1 that there are 8 possible choices for the α used in the construction of Theorem 5.2. We can show that the construction is independent of the chosen α. Assume that α' and α'' are such that both $\{\alpha_1(\alpha_1+\alpha_4),\alpha_2(\alpha_2+\alpha_4),\alpha_3(\alpha_3+\alpha_4),\alpha_4\alpha'\}$ and $\{\alpha_1(\alpha_1+\alpha_4),\alpha_2(\alpha_2+\alpha_4),\alpha_3(\alpha_3+\alpha_4),\alpha_4\alpha''\}$ are $\mathbb{F}_2$-independent sets. We know that $\alpha_4(\alpha'+\alpha'')$ is contained in $\langle\alpha_1(\alpha_1+\alpha_4),\alpha_2(\alpha_2+\alpha_4),\alpha_3(\alpha_3+\alpha_4)\rangle$. Consequently,

$$\begin{aligned}&\{(0,1,x)\mid \mathrm{Tr}(\alpha_i(\alpha_i+\alpha_4)x)=0,\ i=1,2,3\ \wedge\ \mathrm{Tr}(\alpha_4\alpha'x)=1\}\\ =&\{(0,1,x)\mid \mathrm{Tr}(\alpha_i(\alpha_i+\alpha_4)x)=0,\ i=1,2,3\ \wedge\ \mathrm{Tr}(\alpha_4\alpha''x)=1\}\ ,\end{aligned}$$

which proves our claim.

The following result follows immediate from the definition of the KM-arcs of type $q/16$ constructed in Theorem 5.2.

Theorem 5.4. *The $q/16$-secants of the elation KM-arc of type $q/16$ constructed in Theorem 5.2 define an $\mathbb{F}_2$-linear pencil.*

This result is similar to Theorem 4.7 where we have showed that the same holds for KM-arcs constructed in Theorem 4.4. It would be interesting to know whether Theorem 3.10 is valid for all KM-arcs of type $q/16$ (see also Remark 3.11).

Lemma 5.5. *The KM-arc constructed in Theorem 5.2 is not a translation KM-arc with the elation line as translation line.*

Proof. Analogous to the proof of Lemma 4.8. □

We look at the elations stabilising a KM-arc constructed through Theorem 5.2. We know by Lemma 2.1 that all elation KM-arcs of type $q/16$ in $\mathrm{PG}(2,q)$ admit a group of elations of size $q/16$. We will now prove that the KM-arcs constructed through Theorem 5.2 are stabilised by a larger group of elations.

Theorem 5.6. *A KM-arc $\mathcal{A}$ of type $q/16$ in $\mathrm{PG}(2,q)$ constructed though Theorem 5.2 admits a group of elations of size $q/8$.*

Proof. We assume $\mathcal{A}$ is the point set given in the statement of Theorem 5.2 with $\alpha_1,\dots,\alpha_4$ and S as described there. It can readily be checked that all elations in $E=\left\{\left(\begin{smallmatrix}1&0&0\\k\alpha_4&1&0\\s&0&1\end{smallmatrix}\right)\mid s\in S,k\in\mathbb{F}_2\right\}$ fix $\mathcal{A}$. It is also immediate that E is a group of elations with axis $X=0$ and that E has size $q/8$. □

In Lemmas 4.9 and 4.10 we proved that the KM-arcs of type $q/8$ constructed in Theorem 4.4 are $\mathrm{P\Gamma L}$-equivalent under certain conditions. We will now prove similar results for the KM-arcs of type $q/16$ introduced above.

Lemma 5.7. *Let $\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}\subset\mathbb{F}_q^*$ and $\{\alpha_1',\alpha_2',\alpha_3',\alpha_4\}\subset\mathbb{F}_q^*$ be $\mathbb{F}_2$-independent sets such that $\langle\alpha_1,\alpha_2,\alpha_3,\alpha_4\rangle=\langle\alpha_1',\alpha_2',\alpha_3',\alpha_4\rangle$ and such that $\frac{\alpha_i^2}{\alpha_4}\in\langle\alpha_1,\alpha_2,\alpha_3,\alpha_4\rangle$ for $i=1,2,3$. Let $\mathcal{A}$ be the KM-arc constructed through Theorem 5.2 using the tuple $(\alpha_1,\alpha_2,\alpha_3,\alpha_4)$ and let $\mathcal{A}'$ be the KM-arc constructed through Theorem 5.2 using the tuple $(\alpha_1',\alpha_2',\alpha_3',\alpha_4)$. Then $\mathcal{A}$ and $\mathcal{A}'$ are $\mathrm{P\Gamma L}$-equivalent.*

Proof. We note that it follows from $\frac{\alpha_i^2}{\alpha_4} \in \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle$ for $i = 1, 2, 3$ and $\langle \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle = \langle \alpha_1', \alpha_2', \alpha_3', \alpha_4 \rangle$ that also $\frac{\alpha_i'^2}{\alpha_4} \in \langle \alpha_1', \alpha_2', \alpha_3', \alpha_4 \rangle$ for $i = 1, 2, 3$. We proceed as in the proof of Lemma 4.9. We can find a matrix $M \in \mathrm{GL}_4(\mathbb{F}_2)$ such that $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)M = (\alpha_1', \alpha_2', \alpha_3', \alpha_4)$. This matrix M is contained in the subgroup $H = \{C \in \mathrm{GL}_4(\mathbb{F}_2) \mid C_{i,4} = 0,\ i = 1, 2, 3\}$. This multiplicative group H is generated by the matrices $M_1 = \begin{pmatrix} 1&1&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 1&0&0&1 \end{pmatrix}$ and $M_2 = \begin{pmatrix} 0&1&0&0 \\ 0&0&1&0 \\ 1&0&0&0 \\ 0&0&0&1 \end{pmatrix}$ and hence it is sufficient to prove the statement for $M = M_1$ and for $M = M_2$. Let $\alpha, \beta_1, \beta_2, \beta_3$ be as in the construction presented in Theorem 5.2, so $\mathrm{Tr}(\alpha_i\beta_j) = 1$, and $\alpha \in \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle$ such that $\{\alpha_1(\alpha_1 + \alpha_4), \alpha_2(\alpha_2 + \alpha_4), \alpha_3(\alpha_3 + \alpha_4), \alpha_4\alpha\}$ is an $\mathbb{F}_2$-independent set.

We first look at $M = M_1$. In this case $(\alpha_1', \alpha_2', \alpha_3') = (\alpha_1 + \alpha_4, \alpha_1 + \alpha_2, \alpha_3)$. Then $(\beta_1', \beta_2', \beta_3') = (\beta_1 + \beta_2, \beta_2, \beta_3)$ fulfils $\mathrm{Tr}(\alpha_i'\beta_j') = \delta_{i,j}$. We know that the construction in Theorem 5.2 does not depend on the choice of the coset leaders, so when constructing the KM-arc using the tuple $(\alpha_1', \alpha_2', \alpha_3', \alpha_4)$ we may use $\beta_1', \beta_2', \beta_3'$ as coset leaders. A straightforward calculation shows that

$$\langle \alpha_1(\alpha_1 + \alpha_4), \alpha_2(\alpha_2 + \alpha_4), \alpha_3(\alpha_3 + \alpha_4) \rangle = \langle \alpha_1'(\alpha_1' + \alpha_4), \alpha_2'(\alpha_2' + \alpha_4), \alpha_3'(\alpha_3' + \alpha_4) \rangle \ ,$$

hence $\{\alpha_1'(\alpha_1' + \alpha_4), \alpha_2'(\alpha_2' + \alpha_4), \alpha_3'(\alpha_3' + \alpha_4), \alpha_4\alpha\}$ is also an $\mathbb{F}_2$-independent set. The point set of $\mathcal{A}$ is given by $\mathcal{S}_0 \cup \bigcup_{v \in \mathbb{F}_2^4} \mathcal{S}_v$ with

$$\mathcal{S}_0 = \{(0, 1, x) \mid \mathrm{Tr}(\alpha_i(\alpha_i + \alpha_4)x) = 0,\ i = 1, 2, 3 \ \wedge\ \mathrm{Tr}(\alpha_4\alpha x) = 1\} \text{ and}$$
$$\mathcal{S}_{(\lambda_1,\lambda_2,\lambda_3,\lambda_4)} = \left\{ \left(1, \sum_{i=1}^{4} \lambda_i\alpha_i, \sum_{i=1}^{3} f_i(\lambda_1, \lambda_2, \lambda_3)\beta_i + s \right) \,\middle|\, s \in S \right\} \ ,$$

and the point set of $\mathcal{A}'$ is given by $\mathcal{S}_0' \cup \bigcup_{v \in \mathbb{F}_2^3} \mathcal{S}_v'$ with

$$\mathcal{S}_0' = \{(0, 1, x) \mid \mathrm{Tr}(\alpha_i'(\alpha_i' + \alpha_4)x) = 0,\ i = 1, 2, 3 \ \wedge\ \mathrm{Tr}(\alpha_4\alpha x) = 1\} \text{ and}$$
$$\mathcal{S}'_{(\lambda_1,\lambda_2,\lambda_3,\lambda_4)} = \left\{ \left(1, \sum_{i=1}^{3} \lambda_i\alpha_i' + \lambda_4\alpha_4, \sum_{i=1}^{3} f_i(\lambda_1, \lambda_2, \lambda_3)\beta_i' + s \right) \,\middle|\, s \in S \right\} \ .$$

Note that $S = \{x \mid \mathrm{Tr}(\alpha_i x) = 0\} = \{x \mid \mathrm{Tr}(\alpha_i' x) = 0\}$.

Since $\langle \alpha_1(\alpha_1 + \alpha_4), \alpha_2(\alpha_2 + \alpha_4), \alpha_3(\alpha_3 + \alpha_4) \rangle = \langle \alpha_1'(\alpha_1' + \alpha_4), \alpha_2'(\alpha_2' + \alpha_4), \alpha_3'(\alpha_3' + \alpha_4) \rangle$, we know that $\mathcal{S}_0' = \mathcal{S}_0$. Keeping this in mind and using the above expressions for the α_i''s and β_i''s, it can readily be checked that the collineation induced by the matrix $\begin{pmatrix} 1 & 0 & 0 \\ \alpha_1+\alpha_3 & 1 & 0 \\ \beta_3 & 0 & 1 \end{pmatrix}$ maps $\mathcal{A}$ onto $\mathcal{A}'$.

Now we look at the case $M = M_2$, hence at $(\alpha_1', \alpha_2', \alpha_3') = (\alpha_3, \alpha_1, \alpha_2)$. Then $(\beta_1', \beta_2', \beta_3') = (\beta_3, \beta_1, \beta_2)$ fulfils $\mathrm{Tr}(\alpha_i'\beta_j') = \delta_{i,j}$. Again we can construct $\mathcal{A}'$ (note that $\mathcal{A}$ is as above). Here we can check that the collineation induced by the matrix $\begin{pmatrix} 1 & 0 & 0 \\ \alpha_1+\alpha_2 & 1 & 0 \\ \beta_2+\beta_3 & 0 & 1 \end{pmatrix}$ maps $\mathcal{A}$ onto $\mathcal{A}'$. □

Lemma 5.8. *Let $\mathcal{A}$ be a KM-arc of type $q/16$ in $\mathrm{PG}(2, q)$ obtained by the construction in Theorem 5.2 using the admissible tuple $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ and let $\mathcal{A}'$ be a KM-arc of type $q/16$ in $\mathrm{PG}(2, q)$ obtained by the construction in Theorem 5.2 using $(k\alpha_1^\varphi, k\alpha_2^\varphi, k\alpha_3^\varphi, k\alpha_4^\varphi)$, with $k \in \mathbb{F}_q^*$ and φ a field automorphism of $\mathbb{F}_q$. Then $\mathcal{A}$ and $\mathcal{A}'$ are $\mathrm{P\Gamma L}$-equivalent.*

Proof. We note that the condition $\forall i : \frac{\alpha_i^2}{\alpha_4} \in \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle$ and the condition $\forall i : \frac{(k\alpha_i^\varphi)^2}{k\alpha_4^\varphi} \in \langle k\alpha_1, k\alpha_2, k\alpha_3, k\alpha_4 \rangle$ are equivalent. We also note that if $\alpha \in \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle$ is such that $\{\alpha_1(\alpha_1 + \alpha_4), \alpha_2(\alpha_2 + \alpha_4), \alpha_3(\alpha_3 + \alpha_4), \alpha_4\alpha\}$ is an $\mathbb{F}_2$-independent set, then $k\alpha^\varphi \in \langle k\alpha_1^\varphi, k\alpha_2^\varphi, k\alpha_3^\varphi, k\alpha_4^\varphi \rangle$ is such that $\{k\alpha_1^\varphi(k\alpha_1^\varphi + k\alpha_4^\varphi), k\alpha_2^\varphi(k\alpha_2^\varphi + k\alpha_4^\varphi), k\alpha_3^\varphi(k\alpha_3^\varphi + k\alpha_4^\varphi), (k\alpha_4^\varphi)(k\alpha^\varphi)\}$ is an $\mathbb{F}_2$-independent set. The rest of the proof is analogous to the proof of Lemma 4.10. □

We proved before that the KM-arcs of type $q/8$ constructed in Theorem 5.2 are not translation KM-arcs. This also true for the KM-arcs of type $q/16$.

Theorem 5.9. *Any KM-arc in $\mathrm{PG}(2, q)$ constructed through Theorem 4.4 is not a translation KM-arc.*

Proof. The proof is similar to the proof of Theorem 4.11, now using Remark 5.13 and Lemmas 5.5 and 5.8. □

The following result is the analogue of Theorems 4.15 and 4.16. Its proof is similar to the proof of Theorem 4.16.

Theorem 5.10. *Let $\mathcal{A}_0$ be the KM-arc of type $q/16$ with $q/16$-nucleus $N(0,0,1)$ and elation line $X = 0$ constructed from Theorem 4.4 by the admissible tuple $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ and let β be a collineation that stabilises N. Let $\mathcal{A}'$ be a KM-arc of type $q^h/16$ in $\mathrm{PG}(2, q^h)$ obtained from $\mathcal{A}_0^\beta$ through Construction 2 (B) or (C). Then $\mathcal{A}'$ is $\mathrm{P\Gamma L}$-equivalent to a KM-arc obtained by the construction in Theorem 4.4 using the admissible tuple $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$.*

We now discuss the existence of the family of KM-arcs presented in Theorem 5.2.

Theorem 5.11. *A KM-arc $\mathcal{A}$ of type $q/16$ in $\mathrm{PG}(2, q)$, $q = 2^h$, constructed through Theorem 5.2 exists if and only if*

- *$4 \mid h$ and $\mathcal{A}$ is $\mathrm{P\Gamma L}$-equivalent to the KM-arc constructed through Theorem 5.2 using an admissible tuple $(\alpha_1, \alpha_2, \alpha_3, 1)$ with $\langle \alpha_1, \alpha_2, \alpha_3, 1\rangle = \mathbb{F}_{16} \subset \mathbb{F}_q$,*
- *$6 \mid h$ and $\mathcal{A}$ is $\mathrm{P\Gamma L}$-equivalent to the KM-arc constructed through Theorem 5.2 using an admissible tuple $(\alpha_1, \alpha_2, \alpha_3, 1)$ with $\langle \alpha_1, \alpha_2, \alpha_3, 1\rangle = \langle \mathbb{F}_4, \mathbb{F}_8\rangle \subseteq \mathbb{F}_q$ or*
- *$7 \mid h$ and $\mathcal{A}$ is $\mathrm{P\Gamma L}$-equivalent to the KM-arc constructed through Theorem 5.2 using the admissible tuple $(z, z^2, z^4, 1)$ with $z \in \mathbb{F}_q$ admitting $z^7 = z + 1$ or to the KM-arc constructed through Theorem 5.2 using the admissible tuple $(z^{11}, z^{22}, z^{44}, 1)$ with $z \in \mathbb{F}_q$ admitting $z^7 = z + 1$.*

Here we consider the subfields as additive subgroups of $(\mathbb{F}_q, +)$.

Proof. There exists a KM-arc constructed through Theorem 5.2 in $\mathrm{PG}(2, q)$ if we can find a tuple $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in \mathbb{F}_q^4$ such that $\langle \alpha_1, \alpha_2, \alpha_3, \alpha_4\rangle$ has order 16 and such that $\frac{\alpha_i^2}{\alpha_4} \in \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4\rangle$ for $i = 1, 2, 3$. So we look for all admissible tuples $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in \mathbb{F}_q^4$. By Lemma 5.8 we can assume that $\alpha_4 = 1$. We denote $T = \langle \alpha_1, \alpha_2, \alpha_3, 1\rangle$ We distinguish between different cases and subcases. In this discussion we denote the trace function $\mathbb{F}_{q'} \to \mathbb{F}_2$ by $\mathrm{Tr}_{q'}$.

1. *We assume that $\mathbb{F}_4 \subset T$.* In this case $2 \mid h$. By Lemma 5.7 we may assume that $\langle \alpha_1, 1\rangle = \mathbb{F}_4$. It follows that $\frac{\alpha_1^2}{\alpha_4} = \alpha_1^2 \in \langle \alpha_1, 1\rangle \subset T$. It is immediate that for any $x \in \mathbb{F}_q \setminus \mathbb{F}_4$ also $x^2 \in \mathbb{F}_q \setminus \mathbb{F}_4$. Further, if $x^2 + x \in \mathbb{F}_4$ for an element $x \in \mathbb{F}_q \setminus \mathbb{F}_4$, then $x^2 + x \in \mathbb{F}_4 \setminus \mathbb{F}_2$.

   (a) *There is an element $x \in T \setminus \mathbb{F}_4$ such that $x^2 \in \langle \mathbb{F}_4, x\rangle$.* By Lemma 5.7 we can put $\alpha_2 = x$. By the arguments above we know that $\alpha_2^2 \notin \mathbb{F}_4$ and that $\alpha_2^2 + \alpha_2 \in \mathbb{F}_4 \setminus \mathbb{F}_2$, hence $(\alpha_2^2 + \alpha_2)^2 + \alpha_2^2 + \alpha_2 = \alpha_2^4 + \alpha_2 = 1$. So, $\mathbb{F}_{16} \subset \mathbb{F}_q$ equivalently $4 \mid h$, and $\langle \alpha_1, \alpha_2, 1\rangle = \left\langle \alpha_2, \alpha_2^2, 1\right\rangle$ equals $\{x \in \mathbb{F}_{16} \subset \mathbb{F}_q \mid \mathrm{Tr}_{16}(x) = 0\}$.

   The element $\alpha_3 \in T \setminus \langle \alpha_1, \alpha_2, 1\rangle$ must fulfil $\alpha_3^2 \in T$, hence $\alpha_3^2 \in \langle \alpha_1, \alpha_2, 1\rangle$ or $\alpha_3^2 + \alpha_3 \in \langle \alpha_1, \alpha_2, 1\rangle$. Both conditions imply that $\alpha_3 \in \mathbb{F}_{16}$. Consequently, $T = \mathbb{F}_{16} \subset \mathbb{F}_q$.

   (b) *For any element $x \in T \setminus \mathbb{F}_4$ we have $x^2 \notin \langle \mathbb{F}_4, x\rangle$.* We know that $\alpha_2^2 \in T$ and since it is not contained in $\langle \alpha_1, \alpha_2, 1\rangle$, we can write $T = \left\langle \alpha_1, \alpha_2, \alpha_2^2, 1\right\rangle$. Now we must have $\alpha_2^4 \in T$. So we can find $a, b \in \mathbb{F}_2$ and $t \in \mathbb{F}_4$ such that $\alpha_2^4 + a\alpha_2^2 + b\alpha_2 + t = 0$. If $b = 0$, then $\alpha_2^2 + a\alpha_2 + t^2 = 0$, contradicting the assumption. If $(a, b) = (0, 1)$, then $0 = (\alpha_2^4 + \alpha_2 + t)^4 + \alpha_2^4 + \alpha_2 + t = \alpha_2^{16} + \alpha_2$ and hence $T = \mathbb{F}_{16}$, contradicting the assumption.

   So, we may assume that $\alpha_2^4 + \alpha_2^2 + \alpha_2 + t = 0$ for some $t \in \mathbb{F}_4$. It follows that $(\alpha_2 + t^2)^4 + (\alpha_2 + t^2)^2 + (\alpha_2 + t^2) = 0$, hence that

   $$\begin{aligned} 0 &= \left[(\alpha_2 + t^2)^4 + (\alpha_2 + t^2)^2 + (\alpha_2 + t^2)\right]^2 + (\alpha_2 + t^2)^4 + (\alpha_2 + t^2)^2 + (\alpha_2 + t^2) \\ &= (\alpha_2 + t^2)^8 + (\alpha_2 + t^2) \ . \end{aligned}$$

   The element $\alpha_2 + t^2 \in T \setminus \mathbb{F}_2$ is thus a generator of $\mathbb{F}_8$. Consequently, on the one hand $3 \mid h$ and on the other hand $\mathbb{F}_8 = \left\langle \alpha_2 + t^2, (\alpha_2 + t^2)^2, 1\right\rangle \subset T$. So, since also $2 \mid h$, we have $6 \mid h$ and since also $\mathbb{F}_4 \subset T$, we have that $T = \langle \mathbb{F}_4, \mathbb{F}_8\rangle$.

2. *We assume that $\mathbb{F}_4 \not\subset T$.* In this case $x^2 \notin \langle x, 1\rangle$ for any $x \in T \setminus \{0, 1\}$, but by the assumption on T we have $x^2 \in T$. Since also $x^4 \notin \left\langle x^2, 1\right\rangle$, we have two possibilities.

(a) *There is an element $x \in T \setminus \{0,1\}$ such that $x^4 + x \in \langle x^2, 1\rangle$.* By Lemma 4.10 we may assume without loss of generality that $\alpha_1^4 + \alpha_1 \in \langle \alpha_1^2, 1\rangle$ and that $\alpha_2 = \alpha_1^2$.

If $\alpha_1^4 + \alpha_1 = 0$ or $\alpha_1^4 + \alpha_1 = 1$, then we have $\langle \alpha_1, 1\rangle = \mathbb{F}_4$ or $\langle \alpha_1^2 + \alpha_1, 1\rangle = \mathbb{F}_4$, respectively, a contradiction. So, $\alpha_1^4 + \alpha_1 = \alpha_1^2$ or $\alpha_1^4 + \alpha_1 = \alpha_1^2 + 1$. In both cases we find that $\langle \alpha_1, \alpha_1^2, 1\rangle = \mathbb{F}_8$ and hence that $3 \mid h$. The element $\alpha_3 \in T \setminus \mathbb{F}_8$ either fulfils $\alpha_3^2 \in \mathbb{F}_8$ or $\alpha_3^2 + \alpha_3 \in \mathbb{F}_8$. The former would imply that $\alpha_3 \in \mathbb{F}_8$, a contradiction, so $\alpha_3^2 + \alpha_3 + t = 0$ for some $t \in \mathbb{F}_8$, where $\mathrm{Tr}_8(t) = 1$ since otherwise $\alpha_3^2 + \alpha_3 + t = 0$ would have a solution α_3 in $\mathbb{F}_8$. Furthermore, $\mathrm{Tr}_q(t) = 0$. Since for $t \in \mathbb{F}_8$, $\mathrm{Tr}_q(t) = \frac{h}{3}\mathrm{Tr}_8(t)$, we know that $6 \mid h$.

Moreover, from $\alpha_3^2 + \alpha_3 = t$ it follows that $(\alpha_3 + \alpha_1)^2 + (\alpha_3 + \alpha_1) = t + \alpha_1^2 + \alpha_1$, that $(\alpha_3 + \alpha_1^2)^2 + (\alpha_3 + \alpha_1^2) = t + \alpha_1^4 + \alpha_1^2$ and that $(\alpha_3 + \alpha_1^2 + \alpha_1)^2 + (\alpha_3 + \alpha_1^2 + \alpha_1) = t + \alpha_1^4 + \alpha_1$. The elements $t, t+\alpha_1^2+\alpha_1, t+\alpha_1^4+\alpha_1^2, t+\alpha_1^4+\alpha_1$ are the elements of the set $\{x \in \mathbb{F}_8 \mid \mathrm{Tr}_8(x) = 1\}$, among which is 1. By Lemma 5.7 we can replace α_3 by $\alpha_3+\alpha_1$, $\alpha_3+\alpha_1^2$ or $\alpha_3+\alpha_1^2+\alpha_1$, so without loss of generality we may assume $t = 1$. However, now it immediately follows that $\langle \alpha_3, 1\rangle = \mathbb{F}_4$, a contradiction.

(b) *For any element $x \in T \setminus \{0,1\}$ we have $x^4 \notin \langle x, x^2, 1\rangle$.* In particular we have that $\alpha_1^4 \notin \langle \alpha_1, \alpha_1^2, 1\rangle$. In this case clearly $T = \langle \alpha_1, \alpha_1^2, \alpha_1^4, 1\rangle$ and also $\alpha_1^8 \in T$. Hence, there exist $a, b, c, d \in \mathbb{F}_2$ such that $\alpha_1^8 = a\alpha_1^4 + b\alpha_1^2 + c\alpha_1 + d$. If $c = 0$, then $\alpha_1^4 = a\alpha_1^2 + b\alpha_1 + d$ contradicting the assumption. We now look at all cases with $c = 1$.

If $\alpha_1^8 = \alpha_1$, then α_1 generates the subfield $\mathbb{F}_8$, and hence $\alpha_1^4 \in \langle \alpha_1, \alpha_1^2, 1\rangle$, a contradiction. If $\alpha_1^8 = \alpha_1 + 1$, then $\{x \in \mathbb{F}_q \mid x^8 + x + 1 = 0\} = \langle \alpha_1, \alpha_1^2, \alpha_1^4\rangle \subset T$. Clearly, this set is a coset of $\mathbb{F}_8$ (considered as an additive subgroup of $\mathbb{F}_q$). So, $T = \langle \alpha_1, \alpha_1^2, \alpha_1^4, 1\rangle$ contains $\mathbb{F}_8$ and we can find an element in T contradicting the assumption.

If $\alpha_1^8 = \alpha_1^2 + \alpha_1$, then $\alpha_1^7 = \alpha_1 + 1$. The element α_1 thus generates a subfield $\mathbb{F}_{128}$, and so $7 \mid h$. We find the first example from the third bullet point in the statement of the theorem. If $\alpha_1^8 = \alpha_1^2+\alpha_1+1$, then $(\alpha_1 + 1)^8 = (\alpha_1 + 1)^2 + (\alpha_1 + 1) = 0$, hence the element $\alpha_1 + 1 \in T$ generates a subfield $\mathbb{F}_{128}$. By Lemma 5.7 we find the same conclusion as in the previous case.

If $\alpha_1^8 = \alpha_1^4 + \alpha_1$, then $\alpha_1^7 = \alpha_1^3 + 1$. The element α_1 thus generates a subfield $\mathbb{F}_{128}$, and so $7 \mid h$. If $z \in \mathbb{F}_{128}$ is an element admitting $z^7 = z + 1$, then one can check that $\alpha_1 = z^{11\cdot 2^k}$ for some $k = 0, \dots, 6$. Using Lemmas 5.7 and 5.8 we find the second example from the third bullet point in the statement of the theorem. If $\alpha_1^8 = \alpha_1^4 + \alpha_1 + 1$, then $(\alpha_1 + 1)^8 = (\alpha_1 + 1)^4 + (\alpha_1 + 1)$, hence the element $\alpha_1 + 1 \in T$ generates a subfield $\mathbb{F}_{128}$. By Lemma 5.7 we find the same conclusion as in the previous case.

If $\alpha_1^8 = \alpha_1^4 + \alpha_1^2 + \alpha_1$, then $(\alpha_1^2 + \alpha_1)^4 = \alpha_1^2 + \alpha_1$, hence $\mathbb{F}_4 = \langle 1, \alpha_1^2 + \alpha_1\rangle \subset T$, a contradiction. If $\alpha_1^8 = \alpha_1^4+\alpha_1^2+\alpha_1+1$, then $(\alpha_1^4+\alpha_1)^2 = (\alpha_1^4+\alpha_1)+1$, hence $\mathbb{F}_4 = \langle 1, \alpha_1^4 + \alpha_1\rangle \subset T$, a contradiction.

We conclude that in all cases we find an admissible tuple corresponding to one of the KM-arcs of type $q/16$ given in the statement of the theorem. It also follows from the proof that these tuples are indeed admissible. □

Remark 5.12. In the case where $7 \mid h$, we have found in the previous theorem that $\mathcal{A}$ is PΓL-equivalent to the KM-arc constructed through Theorem 5.2 using the admissible tuple $(z, z^2, z^4, 1)$ or to the KM-arc constructed through Theorem 5.2 using the admissible tuple $(z^{11}, z^{22}, z^{44}, 1)$ with $z \in \mathbb{F}_{128}$ admitting $z^7 = z + 1$. We now check that these two possible KM-arcs, say $\mathcal{A}_1$ constructed using $(z, z^2, z^4, 1)$ and $\mathcal{A}_2$ constructed using $(z^{11}, z^{22}, z^{44}, 1)$, are not PΓL-equivalent.

Let S_1 be the subgroup used in the construction of $\mathcal{A}_1$, i.e. the set $\{x \in \mathbb{F}_q \mid \mathrm{Tr}(z^i x) = 0, i = 0, 1, 2, 4\}$, and let S_2 be the subgroup used in the construction of $\mathcal{A}_2$, i.e. the set $\{x \in \mathbb{F}_q \mid \mathrm{Tr}(z^i x) = 0, i = 0, 11, 22, 44\}$. In order for $\mathcal{A}_1$ and $\mathcal{A}_2$ to be PΓL-equivalent, there has to exist a collineation mapping the points of $\mathcal{A}_1$ on a $q/16$-secant of $\mathcal{A}_1$ onto the points of $\mathcal{A}_2$ on a $q/16$-secant of $\mathcal{A}_2$. This in turn implies that there has to be an automorphism $\phi \in \mathrm{Aut}(\mathbb{F}_q)$ and an element $k \in \mathbb{F}_q$ such that $kS_1^\phi = S_2$. Hence, for such couple (ϕ, k) we have

$$\begin{aligned}\langle z^{11}, z^{22}, z^{44}, 1\rangle &= \{x \in \mathbb{F}_q \mid \forall s \in S_2 : \mathrm{Tr}(sx) = 0\} = \{x \in \mathbb{F}_q \mid \forall s \in kS_1^\phi : \mathrm{Tr}(sx) = 0\} \\ &= \{x \in \mathbb{F}_q \mid \forall s \in S_1 : \mathrm{Tr}(ks^\phi x) = 0\} = \{k^{-1}y^\phi \in \mathbb{F}_q \mid \forall s \in S_1 : \mathrm{Tr}(s^\phi y^\phi) = 0\} \\ &= \{k^{-1}y^\phi \in \mathbb{F}_q \mid \forall s \in S_1 : \mathrm{Tr}(sy) = 0\} = \{k^{-1}y^\phi \in \mathbb{F}_q \mid y \in \langle z, z^2, z^4, 1\rangle\} \\ &= k^{-1}\langle z, z^2, z^4, 1\rangle^\phi\end{aligned}$$

Both $\langle z^{11}, z^{22}, z^{44}, 1\rangle$ and $\langle z^{11}, z^{22}, z^{44}, 1\rangle$ are contained in $\mathbb{F}_{128} \subseteq \mathbb{F}_q$. Any automorphism of $\mathbb{F}_q$ fixes the subfield $\mathbb{F}_{128}$, hence $k \in \mathbb{F}_{128}$ and for the restriction $\phi' \in \mathrm{Aut}(\mathbb{F}_{128})$ of ϕ to $\mathbb{F}_{128}$, we have $\langle z^{11}, z^{22}, z^{44}, 1\rangle =$

$k^{-1}\left\langle z,z^2,z^4,1\right\rangle^{\phi'}$. One can check by computer that there is no couple $(\phi',k)\in\mathrm{Aut}(\mathbb{F}_{128})\times\mathbb{F}_{128}$, hence no couple (ϕ,k).

The above theorem makes clear that the construction from Theorem 5.2 can only be applied for specific values of q. We now look at some small values of q.

Remark 5.13. The construction in Theorem 5.2 requires $q>32$, but it can be seen that applying this construction for $q=32$ would yield an elation hyperoval. However, it follows immediately from Theorem 5.11 that there exists no admissible tuple in $\mathbb{F}_{32}^4$, hence we cannot apply the construction in Theorem 5.2.

By Theorem 5.11 we can, up to PΓL-equivalence, construct a unique KM-arc of type 4 in $\mathrm{PG}(2,64)$ through the construction in Theorem 5.2. In [16] already a KM-arc of type 4 in $\mathrm{PG}(2,64)$ was described. It can be checked that this KM-arc is an elation KM-arc. Moreover, the KM-arc described in [16] is PΓL-equivalent to the KM-arc that can be constructed through Theorem 5.2 using the subgroup $\langle\mathbb{F}_4,\mathbb{F}_8\rangle$. The automorphism group G_{64} of this KM-arc of type 4 in $\mathrm{PG}(2,64)$ has size 192. Its subgroup $H_{64}=G_{64}\cap\mathrm{PGL}(3,64)$ of collineations with the identity mapping as field automorphism (subgroup of projectivities) has size 32 and its subgroup E_{64} of elations has size 8. These 8 elations are the ones described by Theorem 5.6. Both the group G_{64} and the group H_{64} have three orbits on the points of the KM-arcs: one orbit containing the four points on the line at infinity, one orbit containing the 32 points of the KM-arc on the 4-secants with equation $Y=aX$ with $a\in\mathbb{F}_8$ and one orbit containing the 32 points of the KM-arc on the 4-secants with equation $Y=aX$ with $a\notin\mathbb{F}_8$.

By Theorem 5.11 and Remark 5.12, we know that, up to PΓL-equivalence, we can construct two different KM-arcs of type 8 in $\mathrm{PG}(2,128)$ through the construction in Theorem 5.2, say $\mathcal{A}_{128,1}$ and $\mathcal{A}_{128,2}$. Denote the automorphism group of $\mathcal{A}_{128,i}$ by $G_{128,i}$ and denote $H_{128,i}=G_{128,i}\cap\mathrm{PGL}(3,128)$, $i=1,2$. The automorphism groups $G_{128,1}$ and $G_{128,2}$ have order 896, and their subgroups $H_{128,1}$ and $H_{128,2}$ have order 128. Both the group $G_{128,i}$ and its subgroup $H_{128,i}$ act transitively on the set of affine points of $\mathcal{A}_{128,i}$, $i=1,2$. It should be noted that these KM-arcs are not translation KM-arcs, since the respective groups of elations stabilising the KM-arcs only have size 16 (they equal the subgroup described in Theorem 5.6).

Theorem 5.14. *If $\mathcal{A}$ is a KM-arc of type $q/16$ in $\mathrm{PG}(2,q)$, $q=2^h$ and $h\mid 4$, obtained by the construction in Theorem 5.2 using an admissible tuple $(\alpha_1,\alpha_2,\alpha_3,1)$ with $\langle\alpha_1,\alpha_2,\alpha_3,1\rangle=\mathbb{F}_{16}$, then $\mathcal{A}$ also arises by applying Construction 2 (A) in $\mathrm{PG}(2,16)$ on the Lunelli-Sce hyperoval.*

Proof. We denote the trace function $\mathbb{F}_q\to\mathbb{F}_2$ by Tr_q, the trace function $\mathbb{F}_{16}\to\mathbb{F}_2$ by Tr_{16} and the trace function $\mathbb{F}_q\to\mathbb{F}_{16}$ by $\mathrm{Tr}_{q,16}$. Let ζ be a generator of $\mathbb{F}_{16}$ admitting $\zeta^4=\zeta+1$. By Lemma 5.7 we may assume that $\alpha_i=\zeta^i$, $i=1,2,3$. Then, $(\beta_1,\beta_2,\beta_3)=(\zeta^2,\zeta,1)$ admits $\mathrm{Tr}_{16}(\zeta^i\beta_j)=\delta_{i,j}$, $i,j\in\{1,2,3\}$ and $\mathrm{Tr}_{16}(1\cdot\beta_j)=0$. Let $\mathcal{S}$ be the set $\{x\in\mathbb{F}_q\mid\forall t\in\mathbb{F}_{16}:\mathrm{Tr}_q(tx)=0\}$.

Let $\alpha\in\mathbb{F}_{16}$ be such that $\{\zeta(\zeta+1),\zeta^2(\zeta^2+1),\zeta^3(\zeta^3+1),\alpha\}$ is an $\mathbb{F}_2$-independent set. Considering $\mathbb{F}_{16}$ as a subfield of $\mathbb{F}_q$, we may assume that $\mathcal{A}$ is given by $\mathcal{A}=\mathcal{S}_0\cup\bigcup_{v\in\mathbb{F}_2^4}\mathcal{S}_v$ with

$$\begin{aligned}\mathcal{S}_0&=\{(0,1,x)\mid\mathrm{Tr}_q(\zeta^i(\zeta^i+1)x)=0,\ i=1,2,3\ \wedge\ \mathrm{Tr}_q(\alpha x)=1\}\\&=\{(0,1,x)\mid\mathrm{Tr}_q(\zeta^i x)=0,\ i=0,1,2\ \wedge\ \mathrm{Tr}_q(\zeta^3x)=1\}\end{aligned}$$

and

$$\begin{aligned}\mathcal{S}_{\overline{\lambda}}&=\left\{\left(1,\sum_{i=1}^{3}\lambda_i\alpha_i+\lambda_4,\sum_{i=1}^{3}f_i(\lambda_1,\lambda_2,\lambda_3)\beta_i+s\right)\middle|\ s\in S\right\}\\&=\left\{\left(1,\sum_{i=1}^{3}\lambda_i\zeta^i+\lambda_4,\sum_{i=1}^{3}f_i(\lambda_1,\lambda_2,\lambda_3)\zeta^{3-i}+s\right)\middle|\ s\in S\right\}\end{aligned}$$

for any $\overline{\lambda}=(\lambda_1,\dots,\lambda_4)\in\mathbb{F}_2^4$. $\mathcal{A}$ is a KM-arc of type $q/16$ in $\mathrm{PG}(2,q)$ with $q/16$-nucleus $(0,0,1)$.

We define the point set $\mathcal{H}$ in $\mathrm{PG}(2,16)$ by $\mathcal{H}=\mathcal{H}'\cup\{(0,1,1),(0,0,1)\}$ and

$$\mathcal{H}'=\left\{\left(1,\sum_{i=1}^{3}\lambda_i\zeta^i+\lambda_4,\sum_{i=1}^{3}f_i(\lambda_1,\lambda_2,\lambda_3)\zeta^{3-i}\right)\middle|\ (\lambda_1,\lambda_2,\lambda_3,\lambda_4)\in\mathbb{F}_2^4\right\}.$$

It can readily be checked that $\mathcal{H}$ is the Lunelli-Sce hyperoval, having an automorphism group of size 144.

Let $k\in\mathbb{F}_q$ be such that $\mathrm{Tr}_{q,16}(k)=1$; such an element can always be found. Let I be the additive subgroup of $\mathbb{F}_q$ given by $\{x\mid\mathrm{Tr}_{q,16}(kx)=0\}$; it has size $q/16$. If $x\in\mathbb{F}_{16}\subseteq\mathbb{F}_q$ admits $\mathrm{Tr}_{q,16}(kx)=0$ then $x=0$. So,

I is a direct complement of $\mathbb{F}_{16}$ in $\mathbb{F}_q$. Moreover, for any element $x \in \mathbb{F}_q$ with $\mathrm{Tr}_{q,16}(kx) = 0$ we know that $\mathrm{Tr}_q(ktx) = \mathrm{Tr}_{16}(\mathrm{Tr}_{q,16}(kx)t) = 0$, for all $t \in \mathbb{F}_{16} \subseteq \mathbb{F}_q$. Hence I equals the set $\{x \mid \forall t \in \mathbb{F}_{16} : \mathrm{Tr}_q(kxt) = 0\}$.

We now apply Construction 2 (A) using $\mathcal{H}$ and I to construct the KM-arc $\mathcal{A}'$ of type $q/16$ in $\mathrm{PG}(2, q)$. The point set of $\mathcal{A}'$ is given by $\mathcal{S}'_0 \cup \bigcup_{v \in \mathbb{F}_2^4} \mathcal{S}'_v$ with $\mathcal{S}'_0 = \{(0, 1, 1 + i) \mid i \in I\}$ and

$$\mathcal{S}'_{(\lambda_1,\lambda_2,\lambda_3,\lambda_4)} = \left\{ \left(1, \sum_{i=1}^{3} \lambda_i \zeta^i + \lambda_4, \sum_{i=1}^{3} f_i(\lambda_1, \lambda_2, \lambda_3)\zeta^{3-i} + i\right) \middle| \, i \in I \right\}$$

for any $(\lambda_1, \lambda_2, \lambda_3, \lambda_4) \in \mathbb{F}_2^4$. We define the KM-arc $\mathcal{A}''$ in $\mathrm{PG}(2, q)$ using the tuple $(k\zeta, k\zeta^2, k\zeta^3, k)$. Its point set is given by $\mathcal{S}''_0 \cup \bigcup_{v \in \mathbb{F}_2^4} \mathcal{S}''_v$ with

$$\mathcal{S}''_0 = \{(0, 1, x) \mid \mathrm{Tr}_q(k^2\zeta^i x) = 0,\ i = 0, 1, 2\ \wedge\ \mathrm{Tr}_q(k^2\zeta^3 x) = 1\}$$

and

$$\mathcal{S}''_{(\lambda_1,\lambda_2,\lambda_3,\lambda_4)} = \left\{ \left(1, k\sum_{i=1}^{3} \lambda_i \zeta^i + k\lambda_4, \sum_{i=1}^{3} f_i(\lambda_1, \lambda_2, \lambda_3)\zeta^{3-i} + i\right) \middle| \, i \in I \right\}$$

since $\{x \mid \mathrm{Tr}_q(k\zeta^i x) = 0, i = 0, 1, 2, 3\} = \{x \mid \forall t \in \mathbb{F}_{16} : \mathrm{Tr}_q(ktx) = 0\}$ and $\mathrm{Tr}_q((k\zeta^i)\beta_j) = \mathrm{Tr}_{16}(\zeta^i\zeta^{3-j}) = \delta_{i,j}$ for $i = 0, 1, 2, 3$ and $j = 1, 2, 3$. Let γ be the collineation induced by the trivial field automorphism and the matrix $C' = C \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & k & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$ where we interpret C over $\mathbb{F}_q$. It is immediate that $\left(\mathcal{S}'_{\overline{\lambda}}\right)^{\gamma} = \mathcal{S}''_{\overline{\lambda}}$ for all $\overline{\lambda} \in \mathbb{F}_2^4$. Furthermore,

$$\begin{aligned}
(\mathcal{S}'_0)^{\gamma} &= \{(0, k, 1 + i) \mid i \in I\} = \{(0, 1, k^{-1}(1 + i)) \mid \forall t \in \mathbb{F}_{16} : \mathrm{Tr}_q(kit) = 0\} \\
&= \{(0, 1, x) \mid \forall t \in \mathbb{F}_{16} : \mathrm{Tr}_q(k^2xt + kt) = 0\} \\
&= \{(0, 1, x) \mid \forall t \in \mathbb{F}_{16} : \mathrm{Tr}_q(k^2xt) = \mathrm{Tr}_{16}(t)\} \\
&= \{(0, 1, x) \mid \mathrm{Tr}_q(k^2\zeta^i x) = 0,\ i = 0, 1, 2\ \wedge\ \mathrm{Tr}_q(k^2\zeta^3 x) = 1\} \\
&= \mathcal{S}''_0
\end{aligned}$$

In the penultimate step we used that Tr_q is $\mathbb{F}_2$-linear, that $\langle \zeta, \zeta^2, \zeta^3, 1\rangle = \mathbb{F}_{16}$ and that $\mathrm{Tr}_{16}(1) = \mathrm{Tr}_{16}(\zeta) = \mathrm{Tr}_{16}(\zeta^2) = 0$ and $\mathrm{Tr}_{16}(\zeta^3) = 1$.

We conclude that $\mathcal{A}' = (\mathcal{A}'')^{\gamma}$. We also know that $\mathcal{A}$ and $\mathcal{A}''$ are isomorphic since the tuples $(\alpha_1, \alpha_2, \alpha_3, 1)$ and $(k\alpha_1, k\alpha_2, k\alpha_3, k)$ give rise to PΓL-equivalent KM-arcs by Lemma 4.10. This proves the theorem. □

Remark 5.15. The previous theorem also shows that when applying Theorem 5.2 for $q = 16$ we get a set of 17 points which forms a hyperoval together with $(0, 0, 1)$. This hyperoval is the Lunelli-Sce hyperoval.

We end this section with a discussion on the existence of KM-arcs of type $q/16$.

Remark 5.16. Previously KM-arcs of type $q/16$ in $\mathrm{PG}(2, q)$, $q = 2^h$ were known to exist for $4 \mid h$, $5 \mid h$ and $6 \mid h$ through Constructions 1 and 2 (A), Construction 2 (B) and Construction 2 (C) applied on the example of a KM-arc of type 4 in $\mathrm{PG}(2, 64)$ [16], respectively.

By Theorem 5.11 the construction from Theorem 5.2 can only be applied for $4 \mid h$, $6 \mid h$ and $7 \mid h$ and given admissible tuples. The KM-arcs of type 2^{h-4} in $\mathrm{PG}(2, 2^h)$ with $4 \mid h$, constructed through Theorem 5.2 using an admissible tuple $(\alpha_1, \alpha_2, \alpha_3, 1)$ with $\langle \alpha_1, \alpha_2, \alpha_3, 1\rangle = \mathbb{F}_{16} \subset \mathbb{F}_q$ were already known to exist since they are by Theorem 5.14 PΓL-equivalent to the KM-arcs of type $q/16$ obtained by applying Construction 2 (A) on a Lunelli-Sce hyperoval. Note that Construction 2 (A) can also be applied on a regular hyperoval. In this case we find a translation KM-arc of type $q/16$, which cannot arise from the construction in Theorem 5.2 by Theorem 5.9.

The KM-arcs of type 2^{h-4} in $\mathrm{PG}(2, 2^h)$ with $6 \mid h$, constructed through Theorem 5.2 using an admissible tuple $(\alpha_1, \alpha_2, \alpha_3, 1)$ with $\langle \alpha_1, \alpha_2, \alpha_3, 1\rangle = \langle \mathbb{F}_4, \mathbb{F}_8\rangle \subset \mathbb{F}_q$ were already known to exist since they are by Theorem 5.10 and Remark 5.13 PΓL-equivalent to the KM-arcs of type $q/16$ obtained by applying Construction 2 (C) on the KM-arc of type 4 in $\mathrm{PG}(2, 64)$ described in [16]. Note that no other KM-arcs of type 2^{h-4} in $\mathrm{PG}(2, 2^h)$ with $6 \mid h$, are known (unless h is also a multiple of 4, 5 or 7).

The KM-arcs of type 2^{h-4} in $\mathrm{PG}(2, 2^h)$ with $7 \mid h$, constructed through Theorem 5.2 using an admissible tuple $(\alpha_1, \alpha_2, \alpha_3, 1)$ with $\langle \alpha_1, \alpha_2, \alpha_3, 1\rangle = \langle z, z^2, z^4, 1\rangle \subset \mathbb{F}_q$ or $\langle \alpha_1, \alpha_2, \alpha_3, 1\rangle = \langle z^{11}, z^{22}, z^{44}, 1\rangle \subset \mathbb{F}_q$ were not described before, so are two new families of examples (the KM-arcs of both families are inequivalent by Remark 5.12).

References

[1] J. Bamberg, A. Betten, Ph. Cara, J. De Beule, M. Lavrauw and M. Neunhöffer. *Finite Incidence Geometry.* FinInG – a GAP package, version 1.3.3, 2016.

[2] M. De Boeck and G. Van de Voorde. A linear set view on KM-arcs. *J. Algebraic Combin.* **44 (1)** (2016), 131–164.

[3] A. Gács and Zs. Weiner. On $(q+t)$-arcs of type $(0,2,t)$. *Des. Codes Cryptogr.*, **29 (1-3)** (2003), 131–139.

[4] M. Hall. Ovals in the Desarguesian plane of order 16. *Ann. Mat. Pura Appl.*, **102** (1975), 159–176.

[5] J.D. Key, T.P. McDonough and V.C. Mavron. An upper bound for the minimum weight of the dual codes of Desarguesian planes. *European J. Combin.*, **30** (2009), 220–229.

[6] G. Korchmáros and F. Mazzocca. On $(q+t)$-arcs of type $(0,2,t)$ in a desarguesian plane of order q. *Math. Proc. Cambridge Philos. Soc.*, **108 (3)** (1990), 445–459.

[7] M. Lavrauw and G. Van de Voorde. Field reduction in finite geometry. *Topics in finite fields.* Contemp. Math., 632, Amer. Math. Soc., Providence, RI, 2010.

[8] R. Lidl and H. Niederreiter. *Finite Fields*, second ed., Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, Cambridge, 1997.

[9] G. Migliori. Insiemi di tipo $(0,2,q/2)$ in un piano proiettivo e sistemi di terne di Steiner. *Rend. Mat. Appl.*, **7** (1987), 77–82.

[10] O. Polverino. Linear sets in finite projective spaces. *Discrete Math.* **310 (22)**(2010), 3096–3107.

[11] C.M. O'Keefe and T. Penttila. Hyperovals in PG$(2,16)$. *European J. Combin.*, **12** (1991), 51–59.

[12] S.E. Payne and J.E. Conklin. An unusual generalized quadrangle of order sixteen. *J. Combin. Theory Ser. A*, **24** (1978), 50–74.

[13] B. Segre. Sui k-archi nei piani finiti di caratteristica due. *Rev. Math. Pures Appl.* **2** (1957), 289–300.

[14] P. Vandendriessche. Codes of Desarguesian projective planes of even order, projective triads and $(q+t,t)$-arcs of type $(0,2,t)$. *Finite Fields Appl.*, **17 (6)** (2011), 521–531.

[15] P. Vandendriessche. A new class of $(q+t,t)$-arcs of type $(0,2,t)$. Talk at *Giornate di geometria*, Vicenza, 13–14 February 2012.

[16] P. Vandendriessche. On KM-arcs in small Desarguesian planes. *Electronic J. Comb.* **24 (1)** (2017), P 1.51.