On KM-arcs in Small Desarguesian Planes

Peter Vandendriessche*
Department of Mathematics
Ghent University
Gent, Belgium
peter.vandendriessche@ugent.be

Submitted: Apr 6, 2016; Accepted: Mar 3, 2017; Published: Mar 17, 2017
Mathematics Subject Classifications: 51E20, 51E21

Abstract

In this paper we study the existence problem for KM-arcs in small Desarguesian planes. We establish a full classification of $\mathrm{KM}_{q,t}$-arcs for $q \leqslant 32$, up to projective equivalence. We also construct a $\mathrm{KM}_{64,4}$-arc; as $t = 4$ was the only value for which the existence of a $\mathrm{KM}_{64,t}$-arc was unknown, this fully settles the existence problem for $q \leqslant 64$.

Keywords: Desarguesian projective plane, KM-arcs, $(q+t,t)$-arcs of type $(0,2,t)$

1 Introduction and Preliminaries

Definition 1. An *incidence structure* $\mathcal{I}$ is a triple $(\mathcal{P}, \mathcal{L}, *_{\mathcal{I}})$, where $\mathcal{P}, \mathcal{L}$ are sets and $*_{\mathcal{I}} \subseteq \mathcal{P} \times \mathcal{L}$. More often than not, $\mathcal{L}$ is a collection of subsets of $\mathcal{P}$ (called *lines*) and $*$ is the inclusion relation: $p *_{\mathcal{I}} L \Leftrightarrow p \in L$ for any $p \in \mathcal{P}, L \in \mathcal{L}$. In such the elements of $\mathcal{P}$ are called *points*.

Definition 2. The *dual* of $\mathcal{I}$, denoted by $\mathcal{I}^D$, is the incidence structure $(\mathcal{L}, \mathcal{P}, *_{\mathcal{I}^D})$ where the incidence is preserved (i.e. $(L,p) \in *_{\mathcal{I}^D} \Leftrightarrow (p,L) \in *_{\mathcal{I}}$). The set $\mathcal{L}$ is now the set of points, and $\mathcal{P}$ the set of lines.

The most commonly studied point-line incidence structures are by no doubt $\mathrm{PG}(2,q)$ and $\mathrm{AG}(2,q)$. It is well-known that $\mathrm{PG}(2,q)$ is isomorphic to $PG(2,q)^D$, while for $\mathrm{AG}(2,q)$ this is not the case: $AG(2,q)$ has q^2 points and q^2+q lines (i.e. $|\mathcal{P}| = q^2$ and $|\mathcal{L}| = q^2+q$), whereas $\mathrm{AG}(2,q)^D$ has q^2+q points and q^2 lines (i.e. $|\mathcal{P}| = q^2+q$ and $|\mathcal{L}| = q^2$).

A large area of research is devoted to studying substructure of $\mathrm{PG}(2,q)$ and $\mathrm{AG}(2,q)$ with certain combinatorial properties. One substructure that has gotten a lot of attention in $\mathrm{PG}(2,q)$ is the following one.

*The research of the author is supported by a postdoctoral grant of the FWO-Flanders.

Definition 3. A hyperoval in $\mathrm{PG}(2,q)$ is a nonempty set S of points, such that every line is incident with 0 or 2 of points of S. One readily computes that a hyperoval has $q+2$ points.

In this paper, we study a slight relaxation of this definition, to the following concept.

Definition 4 ([7])**.** A $\mathrm{KM}_{q,t}$-arc in $\mathrm{PG}(2,q)$, also known as a $(q+t,t)$-arc of type $(0,2,t)$, is a set S of $q+t$ points in $\mathrm{PG}(2,q)$ for which every projective line ℓ meets S in either 0, 2 or t points.

The case $t=1$ is a degenerate case where S is just any arc. Hence, $t>1$ will almost always be assumed. The case $t=q$ is fully classified; here the only example is the symmetric difference of two lines. Hence, for most purposes it is sufficient to study the the case $1<t<q$.

Definition 4 was introduced in [7] and there are several reasons why these structures are of interest. The first reason is that strong structural properties can be derived from this combinatorial definition.

Theorem 5 ([7])**.** *$KM_{q,t}$-arcs of type $(0,2,t)$ with $1<t<q$ can only exist if q is even. Moreover, t needs to be a divisor of q, i.e. $t=2^r$ with $r\leqslant h$.*

Theorem 6 ([4])**.** *All t-secants of a $KM_{q,t}$-arc with $t>2$ are concurrent in a point outside the set, which is called the* nucleus.

Hence, every $\mathrm{KM}_{q,t}$-arc S with $t>2$ has the following structure:

- there are $q/t+1$ concurrent lines, each containing t points of S;
- all other lines contain 0 or 2 points of S.

It is interesting that such a strong structure follows from a combinatorial definition based on three intersection possibilities (0, 2 and t). Usually, such strong properties are only found for sets with two possible intersection numbers. One reason for this - which at the same time is our second motivation - is that they only have two possible intersection numbers when embedded in $\mathrm{AG}(2,q)^D$.

Proposition 7. *A set S in $\mathrm{PG}(2,q)$, $\mathrm{PG}(2,q)^D$ or $\mathrm{AG}(2,q)$ is a set of type $(0,2)$ if and only if it consists of $q+2$ points, no three collinear (i.e. it is a hyperoval).*

Proposition 8. *A set S in $\mathrm{AG}(2,q)^D$ is a set of type $(0,2)$ if and only if, when embedding $\mathrm{AG}(2,q)^D$ in $\mathrm{PG}(2,q)$, S is either a hyperoval or a KM-arc with the point at infinity as its nucleus.*

Proof. Let S be KM-arc. If $t=2$, the statement is trivial. For $t>2$, it follows from Theorem 6 that S is a hyperoval in $\mathrm{AG}(2,q)^D$, where the point of concurrency in the KM-arc is the point at infinity of $\mathrm{AG}(2,q)^D$.

For the reverse implication, let S be a hyperoval in $\mathrm{AG}(2,q)^D$ and let p be any affine point not in S and let L be its line at infinity. Every affine line through p needs at least

	t=2	t=4	t=8	t=16	t=32
$q=4$	1 [10]				
$q=8$	1 [10]	1 [7]			
$q=16$	2 [5]	$\geqslant 3$ [7]	1 [7]		
$q=32$	6 [9]	$\geqslant 1$ [6]	$\geqslant 2$ [2]	1 [12]	
$q=64$	$\geqslant 4$ [3]	?	$\geqslant 1$ [7]	$\geqslant 2$ [2]	1 [12]

Table 1: Number of projective equivalence classes of $\mathrm{KM}_{q,t}$-arcs in $\mathrm{PG}(2,q)$, $q \leqslant 64$.

one other point of S through it, meaning that the total number of points of S is $q+t$, where $t \geqslant 2$ is the number of points of S on L. Since L was arbitrary, and the total number of points of S is fixed, that means the number t is independent of the choices of p and L, and every line through the point at infinity has either no points of S on it, or has exactly t points of S through it. Hence, S is a KM-arc. □

While the above is largely a reformulation of Theorem 6, it does highlight better why these KM-arcs are special and have stronger structural properties than other sets with three intersection numbers.

The third reason is that they have been shown [1, 12, 11] to be crucial in the structure of the dual projective plane code, and of LDPC codes derived from certain partial geometries, where (non)existence of certain KM-arcs is relevant for their dimension and minimum distance, respectively.

The main challenge regarding these KM-arcs is construction and classification. We know that nontrivial examples only exist when $q=2^h$ and $t=2^r$ with $1 \leqslant r \leqslant h$, but the converse is not known. Classification is known only up to $q=8$ [7] and existence is known only by a few (families of) constructions[1], which together settle the existence problem for $q \leqslant 32$.

- In [7], a $\mathrm{KM}_{2^h,2^r}$ was constructed when $h-r|h$.
- In [4], a $\mathrm{KM}_{2^h,2^{r+1}}$ was constructed when $h-r|h$. The same paper also provides a construction for $\mathrm{KM}_{2^h,2^{r+m}}$ when $h-r|h$ and a $\mathrm{KM}_{2^{h-r},2^m}$ exists.
- In [8], a $\mathrm{KM}_{32,8}$ was constructed via random search as part of Limbupasiriporn's PhD thesis.
- In [6], the authors describe a clever random search to construct a $KM_{32,4}$ as a union of subsets of conics, and succeeded in finding such an example.
- In [12], a $\mathrm{KM}_{q,q/4}$ was constructed for every q. In [2], more (nonequivalent) $\mathrm{KM}_{q,q/4}$ were constructed for $q \geqslant 16$.

The reason the random searches in [6, 8] are so important, is because they show that for $q=32$, all proper divisors t yield $\mathrm{KM}_{q,t}$-arcs. Table 1 lists the number of known

[1]We only mention constructions which settle at least one new pair (q,t) of parameter compared to previous publications.

projective equivalence classes of $\mathrm{KM}_{q,t}$-arcs. Only the most recent paper changing the bounds on each number is listed.

In Section 2, we will describe our method to obtain a full classification of $\mathrm{KM}_{q,t}$-arcs for $q \leqslant 32$, as well as the results. In Section 3 we discuss the new findings, as well as several observations and pattens. In Section 4, we use one of these patterns to perform a targeted search that has lead to the construction of a $\mathrm{KM}_{64,4}$-arc, solving the last remaining open case in Table 1.

2 Classifying the KM-arcs in PG$(2, q)$ for $q \leqslant 32$

To settle the notation, we recall the concept of *associated polynomial* from [7].

Theorem 9 ([7])**.** *A set S in $PG(2, q)$ is a $KM_{q,t}$-arc if and only if it can be written in the following form:*

$$S = \{(1, f(c), c) | c \in \mathbb{F}_q)\} \cup \{(0, 1, w_i) | w_i \in W\},$$

where $W = \mathbb{F}_q \setminus \left\{ \frac{x+y}{f(x)+f(y)} \middle| x, y \in \mathbb{F}_q \wedge f(x) \neq f(y) \right\}$, $|W| = t$ and where f a polynomial with the following properties:

- *f reaches every value in $\mathbb{F}_q$ either 0 or t times;*
- *f is monic and has $f(0) = 0$;*
- *$F_a(z) = \frac{f(z)+f(a)}{z+a}$ acts injectively on its set of non-roots in $\mathbb{F}_q$;*
- *for $w \in W \setminus \{0\}$, $w^{-1} + F_a(z)$ has no roots in $\mathbb{F}_q \setminus \{a\}$.*

We can now describe KM-arcs by their associated polynomial. Note however that multiple associated polynomials can describe equivalent KM-arcs. It is also worth remarking that the properties of an associated polynomial from 9 look very similar to those of o-polynomials of hyperovals.

Remark 10. In [7, Theorem 2], the conditions on the second bullet are optional, and in the original version from [7] also contained $f(1) = 0$. However, sometimes one can obtain easier polynomials when not requiring this condition. We will always list the easiest associated polynomial with $f(0) = 0$ and $0 \in W$, where *easiest* is defined below.

Notation 11. Define a function $\varphi : \{0, 1, \ldots, q-1\} \to \mathbb{F}_q$ that represents the lexicographical order of the elements in additive notation:

$$\varphi(0) = 0, \varphi(1) = 1, \varphi(2) = \alpha, \varphi(3) = \alpha + 1, \varphi(4) = \alpha^2, \ldots,$$

$$\varphi(q-1) = \alpha^{h-1} + \alpha^{h-2} + \cdots + \alpha + 1.$$

When choosing an associated polynomial to represent the KM-arc, we will always pick the one with smallest degree (and in case of equal degree, the lexicographically smallest one w.r.t. φ) among all possible associated polynomials.

Remark 12. In the case $t = 2$, the definition of associated polynomial is slightly different from the classical definition for hyperovals (the difference is a term $+z$), because of a slightly different coordinate system.

Now, we will discuss all cases that need to be considered. Some cases have already been dealt with.

Proposition 13. *A $KM_{q,q}$-arc is always projectively equivalent to*

$$S = \{(0, 1, x) | x \in \mathbb{F}_q\} \cup \{(1, 0, x) | x \in \mathbb{F}_q\},$$

which has associated polynomial $f(z) = 0$.

The group $\left\langle x \mapsto \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \alpha \end{smallmatrix}\right) x, x \mapsto \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \alpha^{h-1} & 1 \end{smallmatrix}\right) x, x \mapsto \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha^{h-1} & 0 & 1 \end{smallmatrix}\right) x \right\rangle$ acts transitively on the set of KM-arcs found in [12] (as they are cosets of hyperplanes), resulting in the following proposition.

Proposition 14 ([12])**.** *A $KM_{q,q/2}$ is always projectively equivalent to*

$$S = \left\{(0, 1, \varphi(i)) \middle| 0 \leqslant i < \frac{q}{2}\right\} \cup \left\{(1, 0, \varphi(i)) \middle| 0 \leqslant i < \frac{q}{2}\right\} \cup \left\{(1, 1, \varphi(i)) \middle| \frac{q}{2} \leqslant i < q\right\}.$$

Corollary 15. *There is one projective equivalence class of $KM_{q,q/2}$-arcs in* $\mathrm{PG}(2, q)$*:*

- $f(z) = Tr(z) = z^{q/2} + z^{q/4} + \cdots + z^4 + z^2 + z$.

Proposition 16 ([10])**.** *There is one projective equivalence class of $KM_{q,2}$-arcs for $q \leqslant 8$:*

- $f(z) = z^2 + z$.

Proposition 17 ([5])**.** *There are two projective equivalence classes of $KM_{16,2}$-arcs in* $\mathrm{PG}(2, 16)$*:*

- $f(z) = z^2 + z$,
- $f(z) = z^{12} + z^{10} + \alpha^3 z^8 + z^6 + \alpha^8 z^4 + \alpha^{13} z^2 + z$.

Here, α is a primitive element of $\mathbb{F}_{16}$ with $\alpha^4 + \alpha + 1 = 0$.

Proposition 18 ([9])**.** *There are six projective equivalence classes of $KM_{32,2}$-arcs in* $\mathrm{PG}(2, 32)$*:*

- $f(z) = z^2 + z$,
- $f(z) = z^4 + z$,
- $f(z) = z^6 + z$,
- $f(z) = z^{26} + z^{16} + z^6 + z$,
- $f(z) = z^{28} + z^{10} + z^8 + z$,

- $f(z) = z^{28} + z^{26} + \alpha^{18}z^{22} + \alpha^3 z^{20} + \alpha^{18}z^{18} + \alpha^{14}z^{16} + \alpha^{23}z^{14} + \alpha^6 z^{12} + \alpha^{16}z^{10} + \alpha^{26}z^8 + \alpha^{23}z^6 + \alpha^4 z^4 + \alpha^{24}z^2 + \alpha^{13}z$.

Here, α is a primitive element of $\mathbb{F}_{32}$ with $\alpha^5 + \alpha^2 + 1 = 0$.

For planes of order up to 32, the remaining cases to classify are hence $(q,t) \in \{(16,4),(32,4),(32,8)\}$. Since the classification will be computational, one needs to fix the primitive polynomials of the fields for the coordinates to make sense. For $\mathbb{F}_{16}$ we pick $X^4 + X + 1$ as primitive polynomial, for $\mathbb{F}_{32}$ we pick $X^5 + X^2 + 1$.

We will now outline the algorithm used for our classification result. First we fix the nucleus $N = (0,0,1)$. Let L_N be the set of lines through N. Consider the set $\mathcal{P}(L_N)_{\frac{q}{t}+1}$ of all subsets of L_N of size $\frac{q}{t}+1$. Now, we will partition this set into orbits under the $\mathrm{P\Gamma L}(3,q)_N$, the stabilizer of N in the collineation group of $\mathrm{PG}(2,q)$. To make this computationally feasible, we used a breadth-first backtracking search to find a representative for each $\mathrm{P\Gamma L}(3,q)_N$-orbit of subsets of $\mathcal{P}(L_N)$ of size $1,2,3,\ldots,\frac{q}{t}+1$ in that order, where each size is obtained by considering all possibilities to extend the previous size, and only keeping a unique canonical representative per orbit.

We denote by $\mathcal{L}_N$ the set of representatives obtained, i.e. a set of sets of $\frac{q}{t}+1$ lines. Since N must be a fixed point of every collineation in the automorphism group of any KM-arc, different elements $S_1, S_2 \in \mathcal{L}_N$ represent different orbits under $\mathrm{P\Gamma L}(3,q)_N$, and hence a KM-arc having S_1 as its set of t-secants (with $t > 2$) is always projectively inequivalent to a KM-arc having S_2 as its set of t-secants. Hence, this splits the problem in disjoint subproblems.

Now, for any given such line set $\mathcal{L} \in \mathcal{L}_N$, let $\mathcal{S}_\mathcal{L} = \emptyset$ and pick an arbitrary line $L \in \mathcal{L}$ (computationally, it is wise to pick one with the smallest orbit size under $\mathrm{P\Gamma L}(3,q)_\mathcal{L}$, but that is not mandatory). Now consider the set $\mathcal{T}_L$ of all $\mathrm{P\Gamma L}_{\mathcal{L},L}$-inequivalent t-sets on L. For each $T \in \mathcal{T}_L$ we use a backtracking-based constraint solver to find the possible placings of the remaining q points on the lines of $\mathcal{L}$, such that the KM-arc properties are satisfied. In the vast majority of the cases this solver only requires milliseconds to determine that there will be no solutions for this T. When a solution S is found, it is tested explicitly for projective equivalence with every element in $\mathcal{S}_\mathcal{L}$, and if no equivalent element is found, S is added to $\mathcal{S}_\mathcal{L}$.

Then, at the end,

$$U := \bigcup_{\mathcal{L} \in \mathcal{M}} \mathcal{S}_\mathcal{L}$$

is the set of all $\mathrm{KM}_{q,t}$-arcs up to projective equivalence.

For $q = 16$, nothing surprising was found. The three projective equivalence classes of $\mathrm{KM}_{16,4}$-arcs found in [7] are the only existing classes of $\mathrm{KM}_{16,4}$-arcs, which could be expected given that no new constructions had been found despite the very small order of the plane.

Result 19. *There are exactly* 3 *projective equivalence classes of $KM_{16,4}$-arcs. One representative of each class is given below (where $\alpha^4 = \alpha + 1$).*

- $f(z) = z^8 + z^4 + \alpha z^2 + \alpha^7 z$, *its automorphism group has order* 32 *and partitions its points in orbits of sizes* $16, 4$ *(the four points correspond to one* t*-secant).*

- $f(z) = z^{12} + z^{10} + z^6 + \alpha z^4 + z^2 + \alpha z$, *its automorphism group has order* 64 *and partitions its points in orbits of sizes* $16, 4$ *(the four points correspond to one* t*-secant).*

- $f(z) = z^8 + z^2$, *its automorphism group has order* 3840 *and acts transitively on its points.*

Here, α *is a primitive element of* $\mathbb{F}_{16}$ *with* $\alpha^4 + \alpha + 1 = 0$.

For $q = 32$, $t = 8$ the search found one class of translation arcs (the first one below) and two classes of non-translation arcs. All three can be constructed from [2, Theorem 4.6].

Result 20. *There are exactly* 3 *projective equivalence classes of* $KM_{32,8}$*-arcs. One representative of each class is given below.*

- $f(z) = z^{16} + z^8 + \alpha^{11} z^4 + \alpha^{16} z^2 + \alpha^{13} z$, *its automorphism group has order* 128 *and partitions its points in orbits of sizes* $32, 4, 4$ *(the* $4 + 4$ *points correspond to one* t*-secant).*

- $f(z) = z^{24} + z^{20} + \alpha^{18} z^{18} + \alpha^2 z^{12} + \alpha^{18} z^{10} + \alpha z^8 + \alpha^{23} z^6 + \alpha^6 z^4 + \alpha^{18} z^2 + \alpha^7 z$, *its automorphism group has order* 160 *and acts transitively on its points.*

- $f(z) = z^{24} + z^{20} + \alpha^{18} z^{18} + z^{16} + \alpha^2 z^{12} + \alpha^{18} z^{10} + \alpha^{11} z^8 + \alpha^{23} z^6 + \alpha^2 z^4 + \alpha^{28} z$, *its automorphism group has order* 32 *and partitions its points in five orbits size* 8 *(one for each* t*-secant).*

Here, α *is a primitive element of* $\mathbb{F}_{32}$ *with* $\alpha^5 + \alpha^2 + 1 = 0$.

For $q = 32$, $t = 4$ the search did find new results results. Despite $t = 4$ being the case that has been the hardest to find examples for (only one example known for $q = 32$, constructed by random search, and no examples known for $q = 64$), we found no less than eight projective equivalence classes of $\mathrm{KM}_{32,4}$-arcs, and none of them are translation KM-arcs.

Result 21. *There are exactly* 8 *projective equivalence classes of* $KM_{32,4}$*-arcs. One representative of each class is given below (where* $\alpha^5 = \alpha^2 + 1$*).*

- $f(z) = z^{24} + z^{20} + \alpha^{18} z^{18} + \alpha^5 z^{16} + \alpha^2 z^{12} + \alpha^{18} z^{10} + \alpha^{18} z^8 + \alpha^{23} z^6 + \alpha^5 z^4 + \alpha^{22} z^2 + \alpha^{26} z$, *its automorphism group has order* 16 *and partitions its points in orbits of sizes* $16, 16, 4$ *(corresponding to two sets of four* t*-secants and one set of one* t*-secant).*

- $f(z) = z^{26} + z^{22} + \alpha^{18} z^{20} + \alpha^8 z^{18} + \alpha^{13} z^{16} + \alpha^{28} z^{14} + \alpha^{12} z^{12} + \alpha^{17} z^{10} + \alpha^{20} z^8 + \alpha^{19} z^6 + \alpha^{21} z^4 + \alpha^{11} z^2 + \alpha^{21} z$, *its automorphism group has order* 2 *and partitions its points in sixteen orbits of size* 2 *and four orbits of size* 1 *(all on the same* t*-secant).*

- $f(z) = z^{24}+z^{20}+\alpha^{18}z^{18}+\alpha^2z^{12}+\alpha^{18}z^{10}+\alpha^{19}z^8+\alpha^{23}z^6+\alpha^{27}z^4+\alpha^{18}z^2+z$, *its automorphism group has order* 8 *and partitions its points in orbits of sizes* $8, 8, 8, 4, 4, 2, 2$.

- $f(z) = z^{28} + z^{26} + z^{22} + \alpha^{18}z^{20} + \alpha^{17}z^{18} + \alpha z^{16} + \alpha^{20}z^{14} + \alpha^3z^{12} + \alpha^9z^{10} + \alpha^{26}z^8 + \alpha^2z^6 + \alpha^6z^4 + \alpha^{10}z^2 + \alpha^{29}z$, *its automorphism group has order* 2 *and partitions its points in sixteen orbits of size* 2 *and four orbits of size* 1 *(all on the same* t*-secant).*

- $f(z) = z^{28} + z^{26} + z^{22} + \alpha z^{20} + \alpha^{18}z^{18} + \alpha^{25}z^{16} + z^{14} + \alpha^{23}z^{12} + \alpha^{12}z^{10} + \alpha^{29}z^8 + \alpha^{20}z^6 + \alpha^7z^4 + \alpha z^2 + \alpha^6z$, *its automorphism group has order* 4 *and partitions its points in seven orbits of size* 4 *and four orbits of size* 2.

- $f(z) = z^{28}+z^{26}+z^{22}+\alpha^{11}z^{20}+\alpha^{19}z^{18}+\alpha^8z^{16}+z^{14}+\alpha^{11}z^{12}+\alpha^{19}z^{10}+\alpha^{23}z^8+z^6+\alpha^{22}z^4+\alpha^{24}z^2+\alpha^3z$, *its automorphism group has order* 2 *and partitions its points in sixteen orbits of size* 2 *and four orbits of size* 1 *(all on the same* t*-secant).*

- $f(z) = z^{24}+z^{20}+\alpha^{18}z^{18}+\alpha^2z^{12}+\alpha^{18}z^{10}+\alpha^{11}z^8+\alpha^{23}z^6+\alpha^2z^4+\alpha^{18}z^2+\alpha^6z$, *its automorphism group has order* 24 *and partitions its points in orbits of sizes* $24, 6, 6$.

- $f(z) = z^{24}+z^{20}+\alpha^{18}z^{18}+z^{16}+\alpha^2z^{12}+\alpha^{18}z^{10}+\alpha^{25}z^8+\alpha^{23}z^6+\alpha^{17}z^4+\alpha^{19}z$, *its automorphism group has order* 8 *and partitions its points in orbits of sizes* $8, 8, 8, 4, 4, 2, 2$.

Here, α *is a primitive element of* $\mathbb{F}_{32}$ *with* $\alpha^5 + \alpha^2 + 1 = 0$.

3 Observations

Remark 22. It is remarkable that while (for the same value of q) examples for smaller t are remarkably harder to construct, the number of examples is definitely not smaller. The examples indeed get less symmetrical, but their number increases.

Remark 23. In [12], the author observes that all t-secants in his example stem from (affine) linear sets, and expresses belief that this could hold in general. In the coordinates used in Section 2, that means if we partition the arc in $\frac{q}{t} + 1$ sets of size t based on which t-secant they belong to, and replace each point by its last coordinate (since the first two coordinates are identical for all points in the partition class), each class is now a coset of an additive subgroup of $\mathbb{F}_q$. We verified this property and now confirm that this holds for all $\mathrm{KM}_{q,t}$-arcs with $q \leqslant 32$.

Unfortunately, we did not manage to find a similar pattern in the coordinates of the secant lines. A criterion (even conjectured) that would eliminate a large portion of the possible sets of t-secants, or a pattern that all of the sets of t-secants fulfill, would be extremely helpful in constructing larger new KM-arcs.

Remark 24. In [2], the authors observe the property that the $\mathrm{KM}_{q,q/4}$-arcs they studied, had the following property. Label the t-secants of $\mathcal{S}$ as L_0, L_1, L_2, L_3, L_4. Then for any such labeling,

$$S_1 := \{\langle p, p'\rangle \cap L_0 | p \in \mathcal{S} \cap L_1, p' \in \mathcal{S} \cap L_2\} = \{\langle p, p'\rangle \cap L_0 | p \in \mathcal{S} \cap L_3, p' \in \mathcal{S} \cap L_4\},$$

$$S_2 := \{\langle p, p'\rangle \cap L_0 | p \in \mathcal{S} \cap L_1, p' \in \mathcal{S} \cap L_3\} = \{\langle p, p'\rangle \cap L_0 | p \in \mathcal{S} \cap L_2, p' \in \mathcal{S} \cap L_4\},$$
$$S_3 := \{\langle p, p'\rangle \cap L_0 | p \in \mathcal{S} \cap L_1, p' \in \mathcal{S} \cap L_4\} = \{\langle p, p'\rangle \cap L_0 | p \in \mathcal{S} \cap L_2, p' \in \mathcal{S} \cap L_3\}$$

are well defined (the equality holds), and either

$$|S_1| = |S_2| = |S_3| = q/2, |S_1 \cap S_2| = |S_1 \cap S_3| = |S_2 \cap S_3| = q/4, |S_1 \cap S_2 \cap S_3| = 0$$

in which case they say L_0 has Property II, or

$$|S_1| = |S_2| = |S_3| = q/4, |S_1 \cap S_2| = |S_1 \cap S_3| = |S_2 \cap S_3| = 0$$

in which case they say L_0 has Property I. Our search found the following.

- For the first class in $(16, 4)$ and the first class in $(32, 8)$, the line $\langle (0, 0, 1), (0, 1, 0)\rangle$ has Property I, while the remaining four t-secants have Property II.
- For the second and third class in $(32, 8)$ and for the second class in $(16, 4)$, all t-secants have Property II.
- For the third class in $(16, 4)$, all t-secants have property I.

Moreover, we discovered that a stronger result holds. Remark 22 states that the non-nucleus points on each line have a natural correspondence to the additive group $(\mathbb{F}_q, +)$ by the last coordinate of the points. In this group, it turns out that for all $\mathrm{KM}_{16,4}$-arcs and all $\mathrm{KM}_{32,8}$-arcs, the subsets corresponding to

- S_1, S_2, S_3 (for t-secants L of type I)
- $S_1 \cap S_2, S_1 \cap S_3, S_2 \cap S_3$ (for t-secants L of type II)

are exactly the three cosets of the additive subgroup corresponding to $\mathcal{S} \cap L_0$. Food for thought.

Remark 25. When we consider the subgroup of the automorphism group which stabilizes every single t-secant, all $\mathrm{KM}_{q,t}$-arcs with $q \leqslant 32$ yield an elementary abelian 2-group, i.e. $C_2 \times C_2 \times \cdots \times C_2$. The action of this group within each t-secant is closely linked to the linearity property above, but is not a requirement for it: even for the $\mathrm{KM}_{32,4}$-arcs with automorphism group order 2 the linearity property still holds, despite the absence of a subgroup of order 4 to act on the points within each t-secant.

Remark 26. Let $f(z) - \sum_{i=0}^{q-1} a_i z^i$ be the associated polynomial of a KM-arc. Let $\nu(i)$ be the number of 1s in the base 2 representation of the integer i. Denote by $f_k(z) = \sum_{i \in I_k} a_i z^i$, with $I_k = \{i \in \{0, 1, \ldots, q-1\} | \nu(i) = k\}$. Clearly, $f(z) = f_1(z) + f_2(z) + \cdots + f_h(z)$, where $q = 2^h$ (as $f(0) = 0$, we have $f_0(z) = 0$).

Then, [7, Proposition 6.3] states that a KM-arc with associated polynomial f is a translation KM-arc if and only if $f = f_1$ (i.e. it is a linearized polynomial). Non-translation KM-arcs with $t = q/4$, as well as some $\mathrm{KM}_{32,4}$ arcs with relatively large automorphism group, have $f = f_1 + f_2$. Hence, the limited data we have suggests that it may be interesting to study KM-arcs with $f = f_1 + f_2$, as we may be able to find such a $\mathrm{KM}_{q,t}$-arc for any q, t with t a proper divisor of $q = 2^h$.

Remark 27. The first example for $(16, 4)$ and $(32, 4)$ share a peculiar property. The set of values obtained by the associated polynomial f is respectively $\{\varphi(i)|i \in \{0, \ldots, 3\}\}$ and $\{\varphi(i)|i \in \{0, \ldots, 7\}\}$. This is the key observation for the construction in Section 4.

4 Construction of a $\mathrm{KM}_{64,4}$-arc

Since we have no clear requirements on which line sets $\mathcal{L}$ can yield KM-arcs (or equivalently, what sets can be the image of the associated polynomial of a KM-arc), and since iterating over all possible $\binom{65}{17}$ line sets of size 17 through the nucleus is not feasible on today's computer hardware (even up to isomorphism), a full classification is not possible for $q = 64$ with our techniques. However, in this section we will present a partial search, solving the last open case in Table 1.

We applied the following simplifications of the search, to allow the search to finish within a reasonable time. We only look for KM-arcs which satisfy the linearity constraint. This reduces the search space within each lines from $\binom{q}{t}$ to roughly $\binom{q}{\log_2(t)+1}$ sets. Moreover, we will not look at all projectively inequivalent sets of secants, but we will only look at one specific set $\mathcal{L}$ of lines through the nucleus, which we select based on the following observation.

Notation 28. For any $x \in \mathbb{F}_q$, we denote by $L(x)$ the line $\langle(0, 0, 1), (1, x, 0)\rangle$.

Remark 29. For $t = 4$ and $q \leqslant 32$, the line set

$$\{L(\varphi(i))|i \in \{0, \ldots, \frac{q}{4} - 1\}\} \cup \{\langle(0, 0, 1), (0, 1, 0)\rangle\}$$

always yields a KM-arc.

Unfortunately, this pattern does not seem to extend: there is no $\mathrm{KM}_{64,4}$-arc with these properties. However, we can slightly weaken the pattern as follows.

Remark 30. For every $q \leqslant 32$ there is a subgroup A of $(\mathbb{F}_q, +)$, of size $q/4$, for which the line set $\{L(a)|a \in A\} \cup \{\langle(0, 0, 1), (0, 1, 0)\rangle\}$ yields a $\mathrm{KM}_{q,4}$-arc.

Since there are only 4 such line sets up to projective equivalence in $\mathrm{PG}(2, 64)$, it is computationally feasible to try them all, and one of these sets effectively lead to a new KM-arc. We obtained the following result.

Result 31. *The polynomial $f(z) = z^{48} + z^{34} + z^{20} + z^{16} + z^6 + z^4 + z$ is an associated polynomial of a $KM_{64,4}$-arc, whose automorphism group has order 192 and partitions its points in orbits of sizes* $32, 32, 4$.

This result, combined with the results from Section 3, yields the updated results in Table 2.

The set A in this case is

$$A = \{0, \alpha^0, \alpha^9, \alpha^{18}, \alpha^{27}, \alpha^{36}, \alpha^{45}, \alpha^{54}, \alpha^{21}, \alpha^{42}, \alpha^{11}, \alpha^{22}, \alpha^{44}, \alpha^{25}, \alpha^{50}, \alpha^{37}\}.$$

Its α-powers consist of two arithmetic progressions (one with common difference 9 and one with common difference 21); and one geometric progression (with common ratio 2).

	t=2	t=4	t=8	t=16	t=32
$q=4$	1 [10]				
$q=8$	1 [10]	1 [7]			
$q=16$	2 [5]	**3**	1 [7]		
$q=32$	6 [9]	**8**	**3**	1 [12]	
$q=64$	$\geqslant$ 4 [3]	$\geqslant$ **1**	$\geqslant$ 1 [7]	$\geqslant$ 2 [2]	1 [12]

Table 2: Number of projective equivalence classes of $\mathrm{KM}_{q,t}$-arcs in $\mathrm{PG}(2,q)$, $q \leqslant 64$. The four new items from this paper are in bold.

References

[1] M. De Boeck. Small weight codewords in the dual code of points and hyperplanes in $\mathrm{PG}(n,q)$, q even. *Des. Codes Cryptogr.*, 63:171–182, 2012.

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

[3] W.E. Cherowitzo, C.M. O'Keefe, and T. Penttila. A unified construction of finite geometries associated with q-clans in characteristic 2. *Advances in Geometry*, 3:1–21, 2003.

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

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

[6] 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.*, 30:220–229, 2009.

[7] G. Korchmáros and F. Mazzocca. On $(q+t,t)$-arcs of type $(0,2,t)$ in a Desarguesian plane of order q. *Math. Proc. Camb. Phil. Soc.*, 108:445–459, 1990.

[8] J. Limbupasiriporn. Partial Permutation Decoding for Codes from Designs and Finite Geometries. PhD Thesis, Clemson University, 2005.

[9] T. Penttila and G.F. Royle. Classification of hyperovals in PG(2,32). *J. Geom.*, 50:151–158, 1994.

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

[11] P. Vandendriessche. LDPC codes arising from partial and semipartial geometries. *Proceedings of the Workshop on Coding Theory and Cryptography 2011*, 419–428, 2011.

[12] 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.*, 17:521–531, 2011.