KM-arcs in small Desarguesian projective planes

Peter Vandendriessche

July 20, 2015

Definition

Definition (Korchmáros and Mazzocca, 1990)

A (dual) $\mathrm{KM}_{(q,t)}$-arc is a set S of points (lines) in $\mathrm{PG}(2,q)$,

- of size $q+t$,
- s.t. every line (point) is incident with 0, 2 or t points (lines) of S,
- $1 < t < q$.

Original notation: $(q+t,t)$-arc of type $(0,2,t)$.

Remark

- A hyperoval ($q+2$ points, no three collinear) is a $\mathrm{KM}_{(q,2)}$-arc.
- A dual hyperoval is a dual $\mathrm{KM}_{(q,2)}$-arc.

Motivation 1: structure

Strong structural properties follow from this combinatorial definition:

Theorem (Korchmáros and Mazzocca, 1990)

$KM_{(q,t)}$-arcs only exist if $q = 2^h$ and $t|q$.

Theorem (Gács and Weiner, 2003)

Every $KM_{(q,t)}$-arc S 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.*

Motivation 2: dual hyperovals

Definition

A (dual) hyperoval in $\mathrm{PG}(2,q)$ or $\mathrm{AG}(2,q)$ is a nonempty set of points (lines) such that every line (point) is incident with 0 or 2 points (lines).

- Hyperovals in $\mathrm{AG}(2,q)$ and $\mathrm{PG}(2,q)$ are roughly the same,
- dual hyperovals in $\mathrm{PG}(2,q)$ are the dual of the above,
- dual hyperovals in $\mathrm{AG}(2,q)$ are a broader class.

Theorem

S is a dual hyperoval in $AG(2,q)$ $\Leftrightarrow$ S is a dual $KM_{(q,t)}$-arc.

Dual KM-arcs can also be called *affine dual hyperovals*.

Motivation 3: coding theory

Related to structure of (dual) $PG(2, q)$ codes, q even

- KM-arcs are code words of these codes
- linear dependencies between columns stem from the existence of KM-arcs
- only geometric code used frequently in engineering applications
- a simple coordinate-based basis (small q) is based on KM-arcs [Vandendriessche; 2011]

Main problem: construction

Open Problem

If $q = 2^h$ and $t|q$, is there always a $\text{KM}_{(q,t)}$-arc in $\text{PG}(2, q)$?

This problem has been open for more than 25 years now.

- No extension of the regular hyperoval is known.
- Only a handful of families and sporadic examples are known.
- Even for q small there are open cases.

Small q: an overview up to PΓL-isomorphism

q \ t	2	4	8	16	32
4	**1**				
8	**1**	?			
16	**2**	?	?		
32	**6**	?	?	?	
64	$\geq$ **4**	?	?	?	?

- **[Penttila and Royle; 1994-1995]** did t=2 for small q

Small q: an overview up to PΓL-isomorphism

q \ t	2	4	8	16	32
4	1				
8	1	**1**			
16	2	$\geq$ **2**	**1**		
32	6	?	?	$\geq$ **1**	
64	≥ 4	?	$\geq$ **1**	$\geq$ **1**	$\geq$ **1**

- [Penttila and Royle; 1994-1995] did t=2 for small q
- **[Korchmáros and Mazzocca; 1990]** did $\log_2(\frac{q}{t}) | \log_2(q)$

Small q: an overview up to PΓL-isomorphism

q \ t	2	4	8	16	32
4	1				
8	1	1			
16	2	≥ 2	1		
32	6	?	?	≥ 1	
64	≥ 4	?	≥ 1	≥ 1	≥ 1

- [Penttila and Royle; 1994-1995] did t=2 for small q
- [Korchmáros and Mazzocca; 1990] did $\log_2(\frac{q}{t}) | \log_2(q)$
- **[Gács and Weiner; 2003]** did several sparse families (no impact)

Small q: an overview up to PΓL-isomorphism

q \ t	2	4	8	16	32
4	1				
8	1	1			
16	2	≥ 2	1		
32	6	?	$\geq \mathbf{1}$	≥ 1	
64	≥ 4	?	≥ 1	≥ 1	≥ 1

- [Penttila and Royle; 1994-1995] did t=2 for small q
- [Korchmáros and Mazzocca; 1990] found $\log_2(\frac{q}{t}) | \log_2(q)$
- [Gács and Weiner; 2003] found several sparse families
- **[Limbupasiriporn; 2005]** found $q = 32$, $t = 8$

Small q: an overview up to PΓL-isomorphism

q \ t	2	4	8	16	32
4	1				
8	1	1			
16	2	≥ 2	1		
32	6	$\geq \mathbf{1}$	≥ 1	≥ 1	
64	≥ 4	?	≥ 1	≥ 1	≥ 1

- [Penttila and Royle; 1994-1995] did t=2 for small q
- [Korchmáros and Mazzocca; 1990] found $\log_2(\frac{q}{t}) | \log_2(q)$
- [Gács and Weiner; 2003] found several sparse families
- [Limbupasiriporn; 2005] found $q = 32,\ t = 8$
- **[Key, McDonough and Mavron; 2009]** found $q = 32,\ t = 4$

Small q: an overview up to PΓL-isomorphism

q \ t	2	4	8	16	32
4	1				
8	1	1			
16	2	≥ 2	1		
32	6	≥ 1	≥ 1	**1**	
64	≥ 4	?	≥ 1	$\mathbf{\geq 2}$	**1**

- [Penttila and Royle; 1994-1995] classified t=2 for small q
- [Korchmáros and Mazzocca; 1990] found $\log_2(\frac{q}{t}) | \log_2(q)$
- [Gács and Weiner; 2003] found several sparse families
- [Key, McDonough and Mavron; 2009] found $q = 32$, $t = 4$
- **[Vandendriessche; 2011]** found $t = q/4$ and classified $t = q/2$

Goal: classify $q \leq 32$ up to PΓL-isomorphism

Technique:

- fix the nucleus $N = (0, 0, 1)$
- compute up to isomorphism all $(q/t + 1)$-sets of lines through N
- nonisomorphic t-secants $\Rightarrow$ non-isomorphic KM-arcs
  $\rightarrow$ we have split the problem in disjoint subproblems
- for any given such line set $\mathcal{L}$:
  - let $\mathcal{S}_{\mathcal{L}} = \emptyset$
  - pick an arbitrary line $L \in \mathcal{L}$ (ideally with minimal $P\Gamma L_{\mathcal{L}}$-orbit size)
  - consider the set $\mathcal{T}$ of all $P\Gamma L_{\mathcal{L},L}$-inequivalent t-sets on L
  - for each $T \in T$, use self-written diophantine solver to find the possible placings of the remaining q points (takes only milliseconds)
  - test any found solution for PΓL-equivalence with $\mathcal{S}_{\mathcal{L}}$ only (and if new add to $\mathcal{S}_{\mathcal{L}}$)

Small q: an overview up to PΓL-isomorphism

q \ t	2	4	8	16	32
4	1				
8	1	1			
16	2	**3**	1		
32	6	**8**	**3**	1	
64	≥ 4	?	≥ 1	≥ 2	1

- [Penttila and Royle; 1994-1995] classified t=2 for small q
- [Korchmáros and Mazzocca; 1990] found $\log_2(\frac{q}{t}) | \log_2(q)$
- [Gács and Weiner; 2003] found several sparse families (no impact)
- [Vandendriessche; 2011] found $t = q/4$ and classified $t = q/2$
- **[Vandendriessche; 2015]** classified $q \leq 32$

Interesting property: linearity

Definition

A KM-arc is *linear* if within each secant, the last coordinate forms a coset of an additive subgroup of $\mathbb{F}_q$.

Recall that we let $N(0,0,1)$ be the concurrency point of the secants, and we let the first nonzero coordinate of each point be 1.

Remark

For $q \leq 32$, all KM-arcs are linear, and the $\mathcal{L}$-fixator subgroup of their stabilizer is $C_2 \times C_2 \times \cdots \times C_2$.

Interesting property: linearity

Conjecture (Vandendriessche; 2011)

All KM-arcs are linear (and hence have the above stabilizer property).

If this is true, this greatly reduces the search space: instead of trying $\binom{q}{t}$ sets, it would then be sufficient to look at $\binom{q}{\log_2(t)+1}$ sets.

Open Problem

Which line sets $\mathcal{L}$ yield KM-arcs? No clear requirements could be found.

Looking at $\binom{65}{17}$ lines sets is not feasible $\Rightarrow$ problem for next open case

Finding $q = 64$, $t = 4$

However one pattern could help with a construction:

Pattern

The line set corresponding to

$$\{\infty, 0, 1, \alpha, \alpha + 1, \alpha^2, \dots, \alpha^{t-1} + \cdots + \alpha + 1\}$$

always yields a KM-arc for $q \leq 32$.

Unfortunately, this did not hold for $q = 64$, $t = 4$.

Finding $q = 64$, $t = 4$

However, if we generalize the pattern a bit

Pattern

For $q \leq 32$, there is always (a coset of) an additive subgoup of $\mathbb{F}_q$, we call it S, so that the line set corresponding to $\{\infty\} \cup S$ yields a KM-arc.

then it does extend to $q = 64, t = 4$. And that solves the existence question for $q \leq 64$.

Small q: an overview up to PΓL-isomorphism

q \ t	2	4	8	16	32
4	1				
8	1	1			
16	2	**3**	1		
32	6	**8**	**3**	1	
64	≥ 4	$\geq$ **1**	≥ 1	≥ 2	1

- [Penttila and Royle; 1994-1995] classified t=2 for small q
- [Korchmáros and Mazzocca; 1990] found $\log_2(\frac{q}{t}) | \log_2(q)$
- [Gács and Weiner; 2003] found several sparse families (no impact)
- [Vandendriessche; 2011] found $t = q/4$ and classified $t = q/2$
- **[Vandendriessche; 2015]** classified $q \leq 32$ and found $q = 64, t = 4$

And beyond: $q = 128$, $t = 4$

Pattern

For $q \leq 64$, there is always (a coset of) an additive subgoup of $\mathbb{F}_q$, we call it S, so that the line set corresponding to $\{\infty\} \cup S$ yields a KM-arc.

The stabilizer of this KM-arc always has a subgroup of the form

$$\left\langle x \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha & 0 & 1 \end{pmatrix} x, x \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \beta & 0 & 1 \end{pmatrix} x \right\rangle.$$

This makes it feasible to try to find a $\mathrm{KM}_{(128,4)}$-arc, since:

- up to isomorphism, only 4 cosets of additive subgroup exists
- there are only 2667 such groups in PΓL
- for each lineset and group choice, the computation takes 1-2 hours

This search is currently running (ETA somewhere next month)

Future Work

- What line sets can occur?
- What is the geometry behind the known examples?
- Can we classify $q = 64$ with assumption on the stabilizer? (pending)
- Prove the linearity of the arcs
- Major goal: find a general family of examples that works for all q, t

Thank you for your attention!