New families of KM-arcs

Maarten De Boeck
(joint work with Geertrui Van de Voorde)

Fq13 – June 5, 2017

UNIVERSITEIT GENT

Introduction

2 KM-arcs

Definition

A *KM-arc of type* t in $\mathrm{PG}(2, q)$ is a set of $q + t$ points in $\mathrm{PG}(2, q)$ which is of type $(0, 2, t)$, $t \geq 2$.
A line containing i points of the KM-arc is called an i-secant. So, all lines are 0-, 2- or t-secants with respect to a KM-arc.
Originally a KM-arc of type t was called a $(q + t, t)$*-arc of type* $(0, 2, t)$ *in* $\mathrm{PG}(2, q)$.

Example

$t = 2$: hyperoval
$t = q$: two lines without intersection point

3 Basic properties

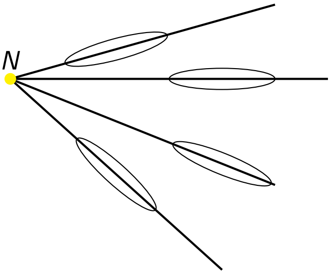
Theorem (Korchmáros-Mazzocca, Gács-Weiner)

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

- *q is even;*
- *t is a divisor of q.*

If moreover $t > 2$, then

- *there are $\frac{q}{t} + 1$ different t-secants to $\mathcal{A}$, and they are concurrent.*



The common point of the t-secants is called the *t-nucleus*.

Construction (Korchmáros-Mazzocca)

- $h - i \mid h$
- L be the relative trace function $\mathbb{F}_{2^h} \to \mathbb{F}_{2^{h-i}}$
- g an o-polynomial in $\mathbb{F}_{2^{h-i}}$

The set $\mathcal{A}_{km} = \{(1, g(L(x)), x) \mid x \in \mathbb{F}_{2^h}\}$ in $\mathrm{PG}(2, 2^h)$ is the affine part of a KM-arc of type 2^i.

5 Constructions in $\mathrm{PG}(2, 2^h)$

Construction (Gács-Weiner)

- $h - i \mid h$
- I a direct complement of $\mathbb{F}_{2^{h-i}}$ in $\mathbb{F}_{2^h}$
- KM-arc H of type t with affine part $\{(1, x_k, y_k)\} \subseteq \mathrm{PG}(2, 2^{h-i})$

We define in $\mathrm{PG}(2, 2^h)$:

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

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

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

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

6 KM-arcs of type q/4

First construction by Vandendriessche.

Theorem (De Boeck-Van de Voorde)

Let Tr *be the absolute trace function* $\mathbb{F}_q \to \mathbb{F}_2$. *Let* $\alpha, \beta \in \mathbb{F}_q \setminus \{0,1\}$ *such that* $\alpha\beta \neq 1$ *and denote* $\gamma = \frac{\beta+1}{\alpha\beta+1}$, $\xi = \alpha\beta\gamma$. *Define the following sets*

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

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

Overview

- For every q hyperovals (KM-arcs of type 2) in $\mathrm{PG}(2,q)$ are known to exist. Classification for $q \leq 64$.
- For every q KM-arcs of type $q/2$ in $\mathrm{PG}(2,q)$ are classified: one example up to PGL-equivalence.

q	$t=4$	$t=8$	$t=16$	$t=32$
16	KM			
32	**KMM, V**	V, DB-VdV		
64	**V**	KM	KM, GW, DB-VdV	
128	?	?	?	V, DB-VdV

Elation KM-arcs

9 A conjecture

Theorem (Gács-Weiner)

A KM-arc of type t in $\mathrm{PG}(2, q)$ determines a Vandermonde set on each of its t-secants.

Definition

$T = \{y_1, \ldots, y_n\} \subseteq \mathbb{F}_q$ is a Vandermonde set if $\sum_{i=0}^{n} y_i^k = 0$ for all $k = 0, \ldots, n-2$.

9 A conjecture

Theorem (Gács-Weiner)

A KM-arc of type t in $\mathrm{PG}(2, q)$ determines a Vandermonde set on each of its t-secants.

Definition

$T = \{y_1, \dots, y_n\} \subseteq \mathbb{F}_q$ is a Vandermonde set if $\sum_{i=0}^{n} y_i^k = 0$ for all $k = 0, \dots, n-2$.

Conjecture (Vandendriessche)

A KM-arc of type t in $\mathrm{PG}(2, q)$ together with its nucleus determines $\mathbb{F}_2$-linear sets on each of its t-secants.

10 Translation KM-arcs

Definition

A KM-arc $\mathcal{A}$ in $\mathrm{PG}(2, q)$ is a called a *translation KM-arc* with respect to the line ℓ if the group of elations (translations) with axis ℓ fixing $\mathcal{A}$ acts transitively on the points of $\mathcal{A} \setminus \ell$; the line ℓ is called the *translation line*.

Theorem (De Boeck-Van de Voorde)

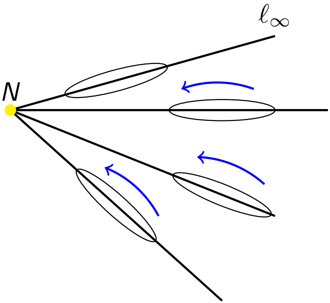
Translation KM-arcs and i-clubs are equivalent objects.

11 Elation KM-arcs

Definition

A KM-arc $\mathcal{A}$ of type $t > 2$ in $\mathrm{PG}(2, q)$ 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 $\mathcal{A}$ (setwise) acts transitively on the points of ℓ.

A hyperoval $\mathcal{H}$ 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.



If $t > 2$, the t-nucleus is the centre of the elations.

12 Observations

Theorem

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

Observations

Theorem

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

Lemma

If $\mathcal{A}$ is an elation KM-arc of type $t > 2$ in $\mathrm{PG}(2,q)$, with elation line $L_\infty : X = 0$ 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; and vice versa.

13 The known arcs

Theorem

- *Korchmáros-Mazzocca (Gács-Weiner (A)): all elation.*
- *Gács-Weiner (B), (C): elation if starting from elation KM-arc or elation hyperoval*
- *Vandendriessche, eight KM-arcs of type* 4 *in* $\mathrm{PG}(2,32)$*: one elation.*

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

Theorem

Let $\mathcal{A}$ be an elation KM-arc of type $q/4$, then $\mathcal{A}$ is PGL*-equivalent to the KM-arc constructed by the DB-VdB construction with $\alpha = \frac{1}{\beta^2}$. Hence, $\mathcal{A}$ is a translation KM-arc iff it is an elation KM-arc.*

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

16 Construction

Theorem

- $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_q^*$ *are* $\mathbb{F}_2$*-independent,* $q = 2^h \geq 16$
- $S = \{x \in \mathbb{F}_q \mid \forall i : \mathrm{Tr}(\alpha_i x) = 0\}$
- $\beta_1, \beta_2, \beta_3 \in \mathbb{F}_q^*$ *such that* $\mathrm{Tr}(\alpha_i \beta_j) = \delta_{i,j}$
- f_1, f_2, f_3 *functions* $\mathbb{F}_2^3 \to \mathbb{F}_2$
  - $f_1 : (x, y, z) \mapsto x + y + z + yz$
  - $f_2 : (x, y, z) \mapsto y + z + xz$
  - $f_3 : (x, y, z) \mapsto z + xy$
- $\mathcal{S}_0 = \{(0, 1, x) \mid \forall i : \mathrm{Tr}(\alpha_i^2 x) = 0\}$

$$\mathcal{S}_{(\lambda_1,\lambda_2,\lambda_3)} = \left\{ \left(1, \sum_{i=1}^{3} \lambda_i \alpha_i, \sum_{i=1}^{3} f_i(\lambda_1, \lambda_2, \lambda_3)\beta_i + s \right) \middle| \; s \in S \right\}, \; (\lambda_1, \lambda_2, \lambda_3) \in \mathbb{F}_2^3$$

The point set $\mathcal{A} = \mathcal{S}_0 \cup \bigcup_{v \in \mathbb{F}_2^3} \mathcal{S}_v$ *is an elation KM-arc of type* $q/8$ *in* $\mathrm{PG}(2, q)$ *with elation line* $Z = 0$ *and* $q/8$*-nucleus* $(0, 0, 1)$.

Why does it work?

Definition

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.

$$\Delta = \begin{vmatrix} 1 & \sum_{i=1}^3 \lambda_i\alpha_i & \sum_{i=1}^3 f_i(\overline{\lambda})\beta_i + s \\ 1 & \sum_{i=1}^3 \lambda_i'\alpha_i & \sum_{i=1}^3 f_i(\overline{\lambda}')\beta_i + s' \\ 1 & \sum_{i=1}^3 \lambda_i''\alpha_i & \sum_{i=1}^3 f_i(\overline{\lambda}'')\beta_i + s'' \end{vmatrix}$$

$$\begin{aligned} \mathrm{Tr}(\Delta) &= \sum_{cyc} ((\lambda_1 + \lambda_1' + 1)(\lambda_2 + \lambda_2' + 1)(\lambda_3 + \lambda_3' + 1) + 1) \\ &= M_2^3(\overline{\lambda}, \overline{\lambda}') + M_2^3(\overline{\lambda}', \overline{\lambda}'') + M_2^3(\overline{\lambda}'', \overline{\lambda}) \\ &= M_3^3(\overline{\lambda}, \overline{\lambda}', \overline{\lambda}'') \,. \end{aligned}$$

18 Equivalences

Theorem

Let $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_q^*$ and $\alpha'_1, \alpha'_2, \alpha'_3 \in \mathbb{F}_q^*$ be both $\mathbb{F}_2$-independent sets with $\langle \alpha_1, \alpha_2, \alpha_3 \rangle_2 = \langle \alpha'_1, \alpha'_2, \alpha'_3 \rangle_2$. Let $\mathcal{A}$ and $\mathcal{A}'$ be the KM-arcs constructed using the triples $(\alpha_1, \alpha_2, \alpha_3)$ and $(\alpha'_1, \alpha'_2, \alpha'_3)$, respectively. Then $\mathcal{A}$ and $\mathcal{A}'$ are PGL*-equivalent.*

Equivalences

Theorem

Let $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_q^*$ *and* $\alpha'_1, \alpha'_2, \alpha'_3 \in \mathbb{F}_q^*$ *be both* $\mathbb{F}_2$*-independent sets with* $\langle \alpha_1, \alpha_2, \alpha_3 \rangle_2 = \langle \alpha'_1, \alpha'_2, \alpha'_3 \rangle_2$. *Let* $\mathcal{A}$ *and* $\mathcal{A}'$ *be the KM-arcs constructed using the triples* $(\alpha_1, \alpha_2, \alpha_3)$ *and* $(\alpha'_1, \alpha'_2, \alpha'_3)$, *respectively. Then* $\mathcal{A}$ *and* $\mathcal{A}'$ *are* PGL*-equivalent.*

Theorem

Let $\mathcal{A}$ *and* $\mathcal{A}'$ *be the KM-arcs in* $\mathrm{PG}(2, q)$ *constructed using the admissible triples* $(\alpha_1, \alpha_2, \alpha_3)$ *and* $(k\alpha_1^\varphi, k\alpha_2^\varphi, k\alpha_3^\varphi)$, *respectively, with* $k \in \mathbb{F}_q^*$ *and* φ *a field automorphism of* $\mathbb{F}_q$. *Then* $\mathcal{A}$ *and* $\mathcal{A}'$ *are* PΓL*-equivalent.*

Results

Theorem

Any KM-arc of type $q/8$ in $\mathrm{PG}(2, q)$ constructed using this construction is not a translation KM-arc.

Theorem

- *In $\mathrm{PG}(2, 16)$ all admissible triples give rise to the Lunelli-Sce hyperoval.*
- *In $\mathrm{PG}(2, 32)$ all admissible triples give rise to the same elation KM-arc of type 4 (computer-free proof).*

Overview for $q/8$

Corollary

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

Overview for $q/8$

Corollary

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

Remark

Discussion of the existence results of KM-arcs of type 2^{h-3} in $\mathrm{PG}(2, 2^h)$; the residue class of h modulo 60 is what matters.

- $h \neq 0 \pmod{m}$ for $m = 3, 4, 5$ (24 residue classes): new existence result.
- $3 \mid h$ and $h \neq 0 \pmod{m}$ for $m = 4, 5$ (12 residue classes): no new existence result, first non-translation KM-arcs.
- $4 \mid h$ or $5 \mid h$ (24 residue classes): no new existence result, non-translation KM-arcs were known.

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

A technicality

Lemma

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.*

Construction

Theorem

- $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{F}_q^*$ *are* $\mathbb{F}_2$*-independent,* $q \geq 64$*,*
  such that $\frac{\alpha_i^2}{\alpha_4} \in \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle$
- $S = \{x \in \mathbb{F}_q \mid \forall i : \mathrm{Tr}(\alpha_i x) = 0\}$
- $\beta_1, \beta_2, \beta_3 \in \mathbb{F}_q^*$ *such that* $\mathrm{Tr}(\alpha_i \beta_j) = \delta_{i,j}$
- $\alpha \in \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle$ *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*
- f_1, f_2, f_3 *functions* $\mathbb{F}_2^3 \to \mathbb{F}_2$ *as before*
- $\mathcal{S}_0 = \{(0, 1, x) \mid \mathrm{Tr}(\alpha_i(\alpha_i + \alpha_4)x) = 0,\ i = 1, 2, 3 \ \wedge \ \mathrm{Tr}(\alpha_4 \alpha x) = 1\}$

$$\mathcal{S}_{\overline{\lambda}} = \left\{ \left(1, \sum_{i=1}^{4} \lambda_i \alpha_i, \sum_{i=1}^{3} f_i(\lambda_1, \lambda_2, \lambda_3) \beta_i + s \right) \middle| \ s \in S \right\}, \ \overline{\lambda} = (\lambda_1, \ldots, \lambda_4) \in \mathbb{F}_2^4$$

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* $(0, 0, 1)$.

Why does it work? (bis)

Given $\overline{\lambda} = (\lambda_1, \ldots, \lambda_4) \in \mathbb{F}_2^4$, we denote $\widetilde{\lambda} = (\lambda_1, \lambda_2, \lambda_3) \in \mathbb{F}_2^4$, ...

$$\Delta = \begin{vmatrix} 1 & \sum_{i=1}^4 \lambda_i \alpha_i & \sum_{i=1}^3 f_i(\widetilde{\lambda})\beta_i + s \\ 1 & \sum_{i=1}^4 \lambda_i' \alpha_i & \sum_{i=1}^3 f_i(\widetilde{\lambda}')\beta_i + s' \\ 1 & \sum_{i=1}^4 \lambda_i'' \alpha_i & \sum_{i=1}^3 f_i(\widetilde{\lambda}'')\beta_i + s'' \end{vmatrix}$$

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

If $\widetilde{\lambda}' = \widetilde{\lambda}''$ and $\lambda_4' = \lambda_4'' + 1$:

$$\mathrm{Tr}\left(\frac{\sum_{i=1}^4 (\lambda_i + \lambda_i')\alpha_i}{\alpha_4} \Delta \right) = M_2^3(\widetilde{\lambda}, \widetilde{\lambda}') \ .$$

Equivalences

Theorem

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 both* $\mathbb{F}_2$*-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* $\mathcal{A}$ *and* $\mathcal{A}'$ *be the KM-arcs constructed using the tuples* $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ *and* $(\alpha_1', \alpha_2', \alpha_3', \alpha_4)$, *respectively. Then* $\mathcal{A}$ *and* $\mathcal{A}'$ *are* $\mathrm{P\Gamma L}$*-equivalent.*

Theorem

Let $\mathcal{A}$ *and* $\mathcal{A}'$ *be the KM-arcs in* $\mathrm{PG}(2, q)$ *constructed using the admissible tuples* $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ *and* $(k\alpha_1^\varphi, k\alpha_2^\varphi, k\alpha_3^\varphi, k\alpha_4^\varphi)$, *respectively, 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.*

Results

Theorem

A KM-arc $\mathcal{A}$ of type $q/16$ in $\mathrm{PG}(2,q)$ constructed using this construction admits a group of elations of size $q/8$.

Theorem

Any KM-arc in $\mathrm{PG}(2,q)$ constructed using this construction is not a translation KM-arc.

Existence

Theorem

A KM-arc $\mathcal{A}$ of type $q/16$ in $\mathrm{PG}(2,q)$, $q = 2^h$, constructed through the previous construction exists if and only if

- $4 \mid h$ *and* $\mathcal{A}$ *is* $\mathrm{P\Gamma L}$*-equivalent to the KM-arc constructed 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 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 using the admissible tuple* $(z, z^2, z^4, 1)$ *or to the KM-arc constructed 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 $\mathbb{F}_q, +$.

Overview for q/16

Corollary

A KM-arc of type $q/16$ *in* $\mathrm{PG}(2,q)$ *exists for all* $q = 2^h$ *such that* $4 \mid h$, $5 \mid h$, $6 \mid h$ *or* $7 \mid h$.

Overview for q/16

Corollary

A KM-arc of type $q/16$ in $\mathrm{PG}(2, q)$ exists for all $q = 2^h$ such that $4 \mid h$, $5 \mid h$, $6 \mid h$ or $7 \mid h$.

Remark

Discussion of the KM-arcs of type 2^{h-4} in $\mathrm{PG}(2, 2^h)$ obtained through the new construction

- $4 \mid h$: also appears by applying the Gács-Weiner construction (A) on the Lunelli-Sce hyperoval
- $6 \mid h$: also appears by applying the Gács-Weiner construction (C) on a sporadic example by Vandendriessche
- $7 \mid h$: two new families of examples

Thank you for your attention.