Strong t mod q arcs in PG$(k-1,q)$

Sascha Kurz
sascha.kurz@uni-bayreuth.de, University of Bayreuth

joint work with

Ivan Landjev
i.landjev@nbu.bg, New Bulgarian University

and

Assia Rousseva
assia@fmi.uni-sofia.bg, Sofia University

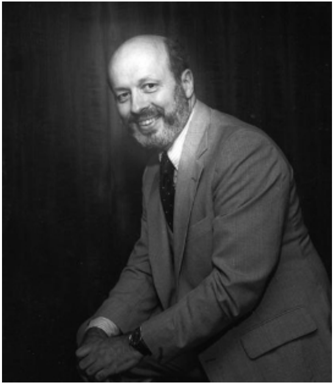
Finite Geometries 2022 – Sixth Irsee Conference, Irsee, 28.08-03.09.2022

Assia and Ivan

Some literature

- I. Landjev and A. Rousseva. On the extendability of Griesmer arcs. Annual of Sofia University “St. Kliment Ohridski” – Faculty of Mathematics and Informatics, 101:183–192, 2013.
- I. Landjev and A. Rousseva. The non-existence of $(104, 22; 3, 5)$-arcs. Advances in Mathematics of Communications, 10(3):601–611, 2016.
- I. Landjev and A. Rousseva. On the characterization of $(3 \mod 5)$ arcs. Electronic Notes in Discrete Mathematics, 57:187–192, 2017.
- I. Landjev and A. Rousseva. Divisible arcs, divisible codes, and the extension problem for arcs and codes. Problems of Information Transmission, 55(3):226–240, 2019.
- I. Landjev, A. Rousseva, and L. Storme. On the extendability of quasidivisible Griesmer arcs. Designs, Codes and Cryptography, 79(3):535–547, 2016.
- A. Rousseva. On the structure of $(t \mod q)$-arcs in finite projective geometries. Annuaire de l’Univ. de Sofia, 102:16pp., 2015.

The Griesmer bound for linear codes



$[n,k,d]_q$ code: $\quad n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil =: g_q(k,d)$ tight for sufficiently large d

Known results

The minimum possible length $n_q(k, d)$ of an $[n, k, d]_q$ code is known for:

- $k \leq 8$ if $q = 2$;
- $k \leq 5$ if $q = 3$;
- $k \leq 4$ if $q = 4$;
- $k \leq 3$ if $q \leq 9$;
- $k = 4$ if $q = 5$ except $d \in \{81, 161, 162\}$.

The talk reports techniques used to determine $n_5(4, 82) = 105$.

Extendability results

- adding a parity check bit to an $[n, k, d]_2$ code of odd minimum distance d yields an even $[n+1, k, d+1]_2$ code
- Theorem of Hill–Lizak: if all weights of codewords in an $[n, k, d]_q$ code are $\equiv 0$ or d modulo q, where $\gcd(d, q) = 1$, then the code is extendable to an $[n+1, k, d+1]_q$ code
  - Hill R.: An extension theorem for linear codes. Des. Codes Cryptogr. 17, 151–157 (1999).
  - Hill R., Lizak P.: Extensions of linear codes. In: Proceedings of International Symposium on Information Theory, Whistler (1995).

Extendability results (cont.)

- further generalized by Tatsuya Maruta
  - Maruta T.: On the extendability of linear codes. Finite Fields Appl. 7, 350–354 (2001).
  - Maruta T.: Extendability of linear codes over GF(q). Discret. Math. 266, 377–385 (2003).
  - Maruta T.: A new extension theorem for linear codes. Finite Fields Appl. 10, 674–685 (2004).
  - Maruta T.: Extension theorems for linear codes over finite fields. J. Geom. 101, 173–183 (2011).
  - Yoshida Y., Maruta T.: An extension theorem for $[n, k, d]_q$. Australas. J. Comb. 48, 117–131 (2010).

Arcs – geometric view on linear codes

- A multiset in $\mathrm{PG}(k-1, q)$ is a mapping $\mathcal{K}\colon \mathcal{P} \to \mathbb{N}_0$, $P \mapsto \mathcal{K}(P)$.
- $\mathcal{K}(P)$ – multiplicity of the point P.
- $\mathcal{Q} \subseteq \mathcal{P}$: $\mathcal{K}(\mathcal{Q}) = \sum_{P \in \mathcal{Q}} \mathcal{K}(P)$ – multiplicity of the set $\mathcal{Q}$.
- $\mathcal{K}(\mathcal{P})$ – the cardinality of $\mathcal{K}$.
- a_i – the number of hyperplanes H with $\mathcal{K}(H) = i$.
- $(a_i)_{i \geq 0}$ – the spectrum of $\mathcal{K}$.
- (n, s)-arc in $\mathrm{PG}(k-1, q)$: a multiset $\mathcal{K}$ with
  - $\mathcal{K}(\mathcal{P}) = n$;
  - for every hyperplane H: $\mathcal{K}(H) \leq s$;
  - there exists a hyperplane H_0: $\mathcal{K}(H_0) = s$.
- An (n, s)-arc in $\mathrm{PG}(k-1, q)$ $\mathcal{K}$ is called t-extendable if there exists an $(n+t, s)$-arc $\mathcal{K}'$ in $\mathrm{PG}(k-1, q)$ with $\mathcal{K}'(P) \geq \mathcal{K}(P)$ for all $P \in \mathcal{P}$. An arc is called extendable if it is 1-extendable.

Quasidivisible arcs

Definition

An (n, s)-arc in $\mathrm{PG}(k-1, q)$ is called *t-quasidivisible* with divisor $\Delta \in \mathbb{N}$ if $a_i = 0$ for all $i \not\equiv n, n+1, \ldots, n+t \pmod{\Delta}$, $1 \leq t \leq q-1$. If we speak of a *t-quasidivisible* arc, then $\Delta := q$.

Definition

Let $\mathcal{K}$ be a t-quasidivisible (n, s)-arc with divisor q in $\mathrm{PG}(k-1, q)$, where $1 \leq t < q$. By $\widetilde{\mathcal{K}}$ we denote the σ-dual

$$\widetilde{\mathcal{K}}\colon \begin{cases} \mathcal{H} \to \{0, 1, \ldots, t\} \\ H \mapsto \widetilde{\mathcal{K}}(H) \equiv n + t - \mathcal{K}(H) \pmod{q} \end{cases} \tag{1}$$

Hyperplanes of multiplicity congruent to $n + a \pmod{q}$ become $(t-a)$-points in the dual geometry; s-hyperplanes become 0-points with respect to $\widetilde{\mathcal{K}}$.

The link to extendability

Theorem Landjev/Rousseva

Let $\mathcal{K}$ be an (n, s)-arc in $\mathrm{PG}(k-1, q)$, which is t-quasidivisible modulo q with $1 \le t < q$. Let $\widetilde{\mathcal{K}}$ defined by Equation (1). If

$$\widetilde{\mathcal{K}} = \sum_{i=1}^{c} \chi_{\widetilde{P}_i} + \mathcal{K}' \tag{2}$$

for some multiset $\mathcal{K}'$ in $\mathrm{PG}^{\perp}(k-1, q)$ and c not necessarily different hyperplanes $\widetilde{P}_1, \ldots, \widetilde{P}_c$ in $\mathrm{PG}^{\perp}(k-1, q)$, then $\mathcal{K}$ is c-extendable. In particular, if $\widetilde{\mathcal{K}}$ contains a hyperplane in its support, then $\mathcal{K}$ is extendable.

Strong ($t \mod q$)-arcs

Theorem Landjev/Rousseva

Let $\mathcal{K}$ be an (n, s)-arc in $\mathrm{PG}(k-1, q)$ which is t-quasidivisible modulo q with $1 \le t < q$. For every subspace $\widetilde{S}$, with $\dim\left(\widetilde{S}\right) \ge 2$, in the dual geometry $\mathrm{PG}^{\perp}(k-1, q)$ we have

$$\widetilde{\mathcal{K}}\left(\widetilde{S}\right) \equiv t \pmod{q}. \quad (3)$$

Definition

An arc $\mathcal{K}$ in $\mathrm{PG}(k-1, q)$ is called a ($t \mod q$)-arc, where $t \in \mathbb{N}$, if we have $\mathcal{K}(S) \equiv t \pmod{q}$ for all subspaces S with $\dim(S) \ge 2$ and $\mathcal{K}(P) < q$ for all points $P \in \mathcal{P}$. We speak of a strong ($t \mod q$)-arc if the maximum point multiplicity is at most t.

Strong ($t \mod q$)-arcs (cont.)

Remark

An equivalent version of the previous definition is to require the condition $\mathcal{K}(S) \equiv t \pmod{q}$ just for all lines S in $\mathrm{PG}(k-1, q)$.

The importance of ($t \mod q$)-arcs is due to the fact that every t-quasidivisible arc $\mathcal{K}$ gives a unique strong ($t \mod q$)-arc $\widetilde{\mathcal{K}}$.

Corollary

If $\mathcal{K}$ is a t-quasidivisible arc in $\mathrm{PG}(k-1, q)$, then $\widetilde{\mathcal{K}}$, defined by Equation (1), is a strong ($t \mod q$)-arc.

- different t-quasidivisible arcs can produce the same strong ($t \mod q$)-arc;
- strong ($t \mod q$)-arcs without 0-points and $1 \leq t < q$ cannot be obtained by (1) from t-quasidivisible arcs;

Constructions for strong ($t \mod q$)-arcs

Theorem Landjev/Rousseva

Let $t_1 < q$ and $t_2 < q$ be positive integers. The sum of a strong ($t_1 \mod q$)-arc and a ($t_2 \mod q$)-arc in $\mathrm{PG}(k-1, q)$ is a ($t \mod q$)-arc with $t = t_1 + t_2 \pmod q$ provided the multiplicities of all points do not exceed t. In particular, the sum of t hyperplanes in $\mathrm{PG}(k-1, q)$ is a ($t \mod q$)-arc.

Constructions for strong ($t \mod q$)-arcs (cont.)

Theorem Landjev/Rousseva

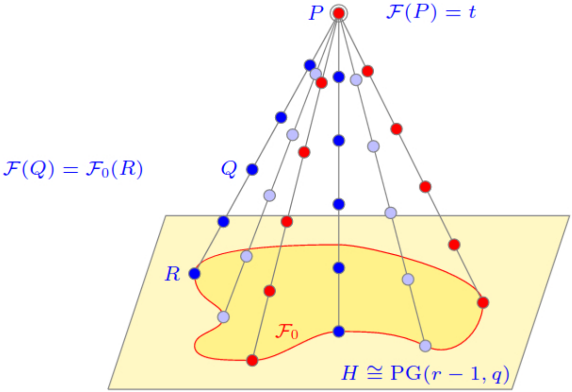
Let $\mathcal{F}_0$ be a strong ($t \mod q$)-arc in a hyperplane $H \simeq \mathrm{PG}(k-2,q)$ of $\Sigma = \mathrm{PG}(k-1,q)$. For a fixed point $P \in \Sigma \backslash H$, define an arc $\mathcal{F}$ in Σ as follows:

- $\mathcal{F}(P) = t$;
- for each point $Q \neq P$: $\mathcal{F}(Q) = \mathcal{F}_0(R)$ where $R = \langle P, Q \rangle \cap H$.

Then the arc $\mathcal{F}$ is a strong ($t \mod q$)-arc in $\mathrm{PG}(k-1,q)$ of size $q|\mathcal{F}_0| + t$.

Strong ($t \mod q$)-arcs obtained by this theorem are called lifted arcs.

Lifted arcs



P
$\mathcal{F}(P) = t$
$\mathcal{F}(Q) = \mathcal{F}_0(R)$
Q
R
$\mathcal{F}_0$
$H \cong \mathrm{PG}(r-1, q)$

Classification of strong $(1 \mod q)$-arcs

A plane $(1 \mod q)$-arc is easily seen to be either a line, or the complete plane for all q. In higher dimensions such an arc is either a hyperplane or the complete space. Therefore every 1-quasidivisible arc $\mathcal{K}$ is extendable $\rightsquigarrow$ Hill–Lizak Theorem

Class. of plane strong $(2 \mod q)$-arcs

Proposition

Let $q \geq 5$ be odd. For a strong $(2 \mod q)$-arc $\mathcal{K}$ in PG$(2, q)$ we have the following possibilities:

(I) A lifted arc from a 2-line with $\#\mathcal{K} = 2q + 2$. There exist two possibilities:

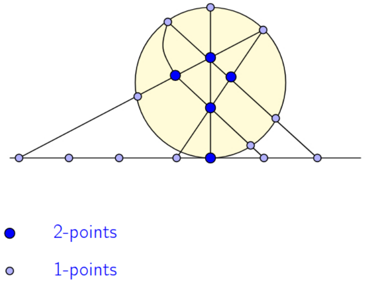
- (I-1) a double line; or
- (I-2) a sum of two different lines.

(II) A lifted arc from a $(q + 2)$-line L with $\#\mathcal{K} = q^2 + 2q + 2$ points. The line L has i double points, $q - 2i + 2$ single points, and $i - 1$ 0-points, where $1 \leq i \leq \frac{q+1}{2}$. We say that such an arc is of type (II-i) if it is lifted from a line with i double points.

(III) A lifted arc from a $(2q + 2)$-line, which is the same as two copies of the plane. Such an arc has $2(q^2 + q + 1)$ points.

(IV) An exceptional $(2 \mod q)$-arc for q odd. It consists of the points of an oval, a fixed tangent to this oval, and two copies of each internal point of the oval.

The exceptional strong (2 mod q)-arc



Proof

Follows from the standard equations (a.k.a. first three MacWilliams identities).

Classification of strong $(2 \mod q)$-arcs

Theorem Landjev/Rousseva

Let $\mathcal{K}$ be a strong $(2 \mod q)$-arc in $\mathrm{PG}(k-1, q)$, where $k \geq 4$ and q is odd. Then, $\mathcal{K}$ is a lifted arc. In particular, for $k \geq 3$ every $(2 \mod q)$-arc in $\mathrm{PG}(k-1, q)$ has a hyperplane in its support.

Corollary

For $k \geq 4$ each 2-quasidivisible arc in $\mathrm{PG}(k-1, q)$ is extendable.

$\rightsquigarrow$ Theorem of Maruta

Class. of plane strong (3 mod 5)-arcs

$\#\mathcal{K}$	line mult.	# isomorphism types
18	0, 1, 2, 3	4
23	1, 2, 3, 4	1
28	2, 3, 4, 5	1
33	3, 4, 5, 6	10
38	4, 5, 6, 7	23
43	5, 6, 7, 8	53
48	6, 7, 8, 9	49
53	7, 8, 9, 10	17
58	8, 9, 10, 11	11
63	9, 10, 11, 12	9
68	10, 11, 12, 13	6
73	11, 12, 13, 14	0
78	12, 13, 14, 15	0
83	13, 14, 15, 16	0
88	14, 15, 16, 17	0
93	15, 16, 17, 18	1

Classification of strong ($3 \mod 5$)-arcs in $\mathrm{PG}(3,5)$

Conjecture Landjev/Rousseva

A ($t \mod q$)-arc in $\mathrm{PG}(r,q)$, $r \geq 3$, is a lifted arc or the sum of lifted arcs.

Theorem Landjev/Rousseva

Every ($3 \mod 5$)-arc $\mathcal{F}$ in $\mathrm{PG}(3,5)$ with $\#\mathcal{F} \leq 168$ is a lifted arc.

Remark

- used in the non-existence proof of a $[104,4,82]_5$ code;
- unfortunately wrong

Classification of strong (3 mod 5)-arcs in PG(3, 5)

Theorem K./Landjev/Rousseva

Let $\mathcal{K}$ be a strong (3 mod 5)-arc in PG(3, 5) that is neither lifted nor contains a full hyperplane. Then $\#\mathcal{K} \in \{128, 143, 168\}$ and $\mathcal{K}$ is isomorphic to one of the following three possibilities:

(1) $\#\mathcal{K} = 128$: Generator matrix given by the concatenation of

$$\begin{pmatrix} 00000000000000000000000000000000011111111111111111111111111111111 \\ 00011111111111111111111111111111100000000000000000000011111111111 \\ 11100011111112222222223333333344400011111111122233344400011122233 \\ 11401301122333112333440111222322240221112344400113311123333302300 \end{pmatrix}$$

and

$$\begin{pmatrix} 111111111111111111111111111111111111111111111111111111111111111 \\ 111111111222222222222222333333333333333333344444444444444444444 \\ 333333444000111222333444000111222333444444400011111111222333444 \\ 111233444124012013244033024444044333011122441220111333400211144 \end{pmatrix}$$

with a corresponding automorphism group of order 7680.

Classification of strong $(3 \mod 5)$-arcs in $\mathrm{PG}(3,5)$

Theorem K./Landjev/Rousseva

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(3,5)$ that is neither lifted nor contains a full hyperplane. Then $\#\mathcal{K} \in \{128, 143, 168\}$ and $\mathcal{K}$ is isomorphic to one of the following three possibilities:

(2) $\#\mathcal{K} = 143$: Generator matrix given by the concatenation of

$$\begin{pmatrix}
0000000000000000000000000000000000011111111111111111111111111111111111111 \\
0000000011111111111111111111111111100000000000000000000011111111111111111 \\
0111111100000001122222222334444444400000001122334444444400000001122333334 \\
1000333401222340201114440301233340001222223030111123330123334043400012341
\end{pmatrix}$$

and

$$\begin{pmatrix}
11111111111111111111111111111111111111111111111111111111111111111111111111 \\
11111122222222222222222222233333333333333333333333333444444444444444444444 \\
44444400000001122222222334400112222222233333334444444001122222222333333344 \\
11222240222333120001113130204340001234111222240123333403011112333000122223
\end{pmatrix}$$

with a corresponding automorphism group of order 62400.

Class. of s. $(3 \mod 5)$-arcs in $\mathrm{PG}(3,5)$

Theorem K./Landjev/Rousseva

Let $\mathcal{K}$ be a strong $(3 \mod 5)$-arc in $\mathrm{PG}(3,5)$ that is neither lifted nor contains a full hyperplane. Then $\#\mathcal{K} \in \{128, 143, 168\}$ and $\mathcal{K}$ is isomorphic to one of the following three possibilities:

(3) $\#\mathcal{K} = 168$: Generator matrix given by the concatenation of

$$\begin{pmatrix}
00000000000000000000000000000000000000000001111111111111111111111111111111111111111111 \\
00000000000000001111111111111111111111111110000000000000000000000000111111111111111111 \\
00011111111111111100000111112222233333444440000011111222223333344444000001111122222333 \\
11100011122233344403444034440344403444034440222412444111340133300023000140344423334122
\end{pmatrix}$$

and

$$\begin{pmatrix}
1111111111111111111111111111111111111111111111111111111111111111111111111111111111 \\
1111111222222222222222222222222223333333333333333333333333444444444444444444444444 \\
3344444222223333333333333334444400000111112222233333444440000011111222223333344444 \\
2301112012340001112223334440123412223233340344400014011120002301333111341244402224
\end{pmatrix}$$

with a corresponding automorphism group of order 57600.

Classification of strong $(3 \mod 5)$-arcs in $\mathrm{PG}(3,5)$

Conjecture K./Landjev/Rousseva

Every strong $(3 \mod 5)$-arc in $\mathrm{PG}(k-1,5)$ is lifted for $k \geq 5$.

Theorem K./Landjev/Rousseva

No $[104,4,82]_5$ code exists.

S. K., I. Landjev, and A. Rousseva: *Classification of* $(3 \bmod 5)$ *arcs in* $\mathrm{PG}(3,5)$, to appear in *Advances in Mathematics of Communications*.

Open problems

- classify all strong $(3 \mod 5)$ arcs
- give a geometric construction of the three exceptional non-lifted strong $(3 \mod 5)$ arcs in $\mathrm{PG}(3, 5)$ and generalize to other field sizes

- construct more non-lifted strong $(t \mod q)$ arcs
- use non-lifted strong $(t \mod q)$ arcs to find good codes
- classify all strong $(3 \mod 7)$ arcs in $\mathrm{PG}(3, 7)$

Open problems

- classify all strong $(3 \mod 5)$ arcs
- give a geometric construction of the three exceptional non-lifted strong $(3 \mod 5)$ arcs in $\mathrm{PG}(3,5)$ and generalize to other field sizes $\longrightarrow$ Francesco Pavese:

$\#\mathcal{K} = 128$ 2-points are given by the maximal 20-cap in $\mathrm{PG}(3,5)$ with collineation group of size 1920 (see K_1 in Abatangelo, Korchmaros, Larato 1996: Classification of maximal caps in $\mathrm{PG}(3,5)$ different from elliptic quadrics.)

$\#\mathcal{K} = 143$ 3-points are given by the elliptic quadric in $\mathrm{PG}(3,5)$

$\#\mathcal{K} = 168$ 3-points are given by the hyperbolic quadric in $\mathrm{PG}(3,5)$

- construct more non-lifted strong $(t \mod q)$ arcs
- use non-lifted strong $(t \mod q)$ arcs to find good codes
- classify all strong $(3 \mod 7)$ arcs in $\mathrm{PG}(3,7)$

Thank you very much for your attention!

Appendix: Output for $\#\mathcal{K} = 128$

6 line types remain.
16 point-line types remain.
4 residual arcs remain.
Remaining line 0 with cardinality 3: 5 0 0 1
Remaining line 2 with cardinality 3: 4 1 1 0
Remaining line 5 with cardinality 3: 3 3 0 0
Remaining line 6 with cardinality 8: 0 4 2 0
Remaining line 7 with cardinality 8: 2 1 2 1
Remaining line 8 with cardinality 8: 2 2 0 2
Remaining point-line configuration 9: 2 2 2 2 2 6 6
Remaining point-line configuration 10: 1 2 5 5 5 5 6
Remaining point-line configuration 11: 0 2 2 2 5 5 5
Remaining point-line configuration 12: 3 0 0 7 7 8 8
Remaining point-line configuration 13: 2 2 2 2 7 7 7
Remaining point-line configuration 14: 0 0 0 2 2 5 7
Remaining point-line configuration 15: 1 2 2 5 5 7 8
Remaining point-line configuration 16: 0 0 2 2 2 2 8
Remaining point-line configuration 17: 3 0 8 8 8 8 8
Remaining point-line configuration 18: 0 0 0 5 5 8 8
Remaining point-line configuration 19: 1 5 5 5 8 8 8
Remaining point-line configuration 21: 2 2 6 7 7 7 7
Remaining point-line configuration 25: 0 2 2 5 7 7 8
Remaining point-line configuration 35: 1 5 5 6 7 7 8
Remaining point-line configuration 38: 3 7 7 7 8 8 8
Remaining point-line configuration 55: 1 2 2 6 6 8 8
Remaining hyperplane 3 with cardinality 18: 9 10 11
Remaining hyperplane 4 with cardinality 23: 12 13 14 15 16
Remaining hyperplane 5 with cardinality 28: 17 18 19
Remaining hyperplane 9 with cardinality 33: 21 25 38 35 55