On additive MDS codes with linear projections

Sam Adriaensen
(Joint work with Simeon Ball)

Irsee 6

VRIJE
UNIVERSITEIT
BRUSSEL

Central question

Linear MDS codes have been well studied. It is widely believed that the longest linear MDS codes are extended Reed-Solomon codes, aside from some known exceptions.

Central question

Linear MDS codes have been well studied. It is widely believed that the longest linear MDS codes are extended Reed-Solomon codes, aside from some known exceptions.

What if we relax linearity to additivity? Are there long additive MDS codes over finite fields, which are not equivalent to linear codes?

Linear codes and their geometry

From a linear code to projective point sets

Let C be a linear $[n, k, d]_q$ code over $\mathbb{F}_q$.

From a linear code to projective point sets

Let C be a linear $[n, k, d]_q$ code over $\mathbb{F}_q$.
Choose a generator matrix G for C.

$$G = k\left[\underbrace{\begin{pmatrix} \cdot & \cdot & & \cdot & \cdot \\ \vdots & \vdots & \dots & \vdots & \vdots \\ \cdot & \cdot & & \cdot & \cdot \end{pmatrix}}_{n}\right.$$

From a linear code to projective point sets

Let C be a linear $[n, k, d]_q$ code over $\mathbb{F}_q$.
Choose a generator matrix G for C. $\text{RowSp}(G) = C$.

$$G = k \left[\underbrace{\begin{pmatrix} \cdot & \cdot & & \cdot & \cdot \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ \cdot & \cdot & & \cdot & \cdot \end{pmatrix}}_{n} \right.$$

From a linear code to projective point sets

Let C be a linear $[n, k, d]_q$ code over $\mathbb{F}_q$.
Choose a generator matrix G for C. $\mathrm{RowSp}(G) = C$.

$$G = k\left[\vphantom{\begin{pmatrix} \cdot \\ \vdots \\ \cdot \end{pmatrix}}\right. \underbrace{\begin{pmatrix} \boxed{\begin{matrix} \cdot \\ \vdots \\ \cdot \end{matrix}} & \boxed{\begin{matrix} \cdot \\ \vdots \\ \cdot \end{matrix}} & \cdots & \boxed{\begin{matrix} \cdot \\ \vdots \\ \cdot \end{matrix}} & \boxed{\begin{matrix} \cdot \\ \vdots \\ \cdot \end{matrix}} \end{pmatrix}}_{n}$$

Every column of G represents a point of $\mathrm{PG}(k-1, q)$. This gives us a (mutli)set of n points in $\mathrm{PG}(k-1, q)$.

Equivalence classes

Different generator matrices G of C may yield different point sets in $\mathrm{PG}(k-1, q)$. The different point sets form an orbit of $\mathrm{PGL}(k, q)$.

Equivalence classes

Different generator matrices G of C may yield different point sets in $\mathrm{PG}(k-1, q)$. The different point sets form an orbit of $\mathrm{PGL}(k, q)$.

Vice versa, from a point set we can construct a code (by reversing the previous process). This can yield different point sets, which are an orbit under code equivalence.

The parameters of the code

	Linear code	Point set
n	length	size
k	dimension	(vector) dimension of the ambient projective space
d	minimum Hamming distance	minimum number of points outside any hyperplane

Additive codes and their geometry

Additive codes

Definition

A code C over $\mathbb{F}_q$ is *additive* if

$$(\forall \mathbf{x}, \mathbf{y} \in C)(\mathbf{x} + \mathbf{y} \in C).$$

Additive codes

Definition

A code C over $\mathbb{F}_q$ is *additive* if

$$(\forall\, \mathbf{x}, \mathbf{y} \in C)(\mathbf{x} + \mathbf{y} \in C).$$

Equivalently, C is linear over $\mathbb{F}_p$ (with p the prime number dividing q).

Additive codes

Definition

A code C over $\mathbb{F}_q$ is *additive* if

$$(\forall\, \mathbf{x}, \mathbf{y} \in C)(\mathbf{x} + \mathbf{y} \in C).$$

Equivalently, C is linear over $\mathbb{F}_p$ (with p the prime number dividing q).

In this talk we will consider codes over $\mathbb{F}_{q^h}$ which are linear over $\mathbb{F}_q$.

Additive codes

Definition

A code C over $\mathbb{F}_q$ is *additive* if

$$(\forall\, \mathbf{x}, \mathbf{y} \in C)(\mathbf{x} + \mathbf{y} \in C).$$

Equivalently, C is linear over $\mathbb{F}_p$ (with p the prime number dividing q).

In this talk we will consider codes over $\mathbb{F}_{q^h}$ which are linear over $\mathbb{F}_q$.
$q = q^h \rightarrow$ linear code
q prime $\rightarrow$ additive code

From an additive code to a set of subspaces

Let C be an $\mathbb{F}_q$-linear $(n, q^k, d)_{q^h}$ code over $\mathbb{F}_{q^h}$.

From an additive code to a set of subspaces

Let C be an $\mathbb{F}_q$-linear $(n, q^k, d)_{q^h}$ code over $\mathbb{F}_{q^h}$.
Let G be a generator matrix for C over $\mathbb{F}_q$. This means that $G \in \mathbb{F}_{q^h}^{k \times n}$, and the rows of G are an $\mathbb{F}_q$-basis for C.

$$G = k \left[\begin{pmatrix} \boxed{\cdot \quad \cdot \qquad\qquad \cdot \quad \cdot} \\ \underbrace{\vdots \quad \vdots \quad \cdots \quad \vdots \quad \vdots}_{} \\ \boxed{\cdot \quad \cdot \qquad\qquad \cdot \quad \cdot} \end{pmatrix} \right.$$

$$\underbrace{\qquad\qquad\qquad\qquad}_{n}$$

From an additive code to a set of subspaces

Let C be an $\mathbb{F}_q$-linear $(n, q^k, d)_{q^h}$ code over $\mathbb{F}_{q^h}$.
Let G be a generator matrix for C over $\mathbb{F}_q$. This means that $G \in \mathbb{F}_{q^h}^{k \times n}$, and the rows of G are an $\mathbb{F}_q$-basis for C.

$$G = k \underbrace{\begin{pmatrix} \boxed{\vdots} & \boxed{\vdots} & \cdots & \boxed{\vdots} & \boxed{\vdots} \end{pmatrix}}_{n}$$

Take an $\mathbb{F}_q$-basis $\alpha_1, \dots, \alpha_h$ of $\mathbb{F}_{q^h}$ and write $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_h)$. The j^{th} column of G is of the form $\boldsymbol{\alpha} G_j$ for some unique $G_j \in \mathbb{F}_q^{h \times k}$.

From an additive code to a set of subspaces

Let C be an $\mathbb{F}_q$-linear $(n, q^k, d)_{q^h}$ code over $\mathbb{F}_{q^h}$.
Let G be a generator matrix for C over $\mathbb{F}_q$.

Take an $\mathbb{F}_q$-basis $\alpha_1, \dots, \alpha_h$ of $\mathbb{F}_{q^h}$ and write $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_h)$. The j^{th} column of G is of the form $\boldsymbol{\alpha} G_j$ for some unique $G_j \in \mathbb{F}_q^{h \times k}$.

$$\begin{pmatrix} g_{1j} \\ \vdots \\ g_{kj} \end{pmatrix} = \begin{pmatrix} \alpha_1 g_{1j}^{(1)} + \dots + \alpha_h g_{1j}^{(h)} \\ \vdots \\ \alpha_1 g_{kj}^{(1)} + \dots + \alpha_h g_{kj}^{(h)} \end{pmatrix} = \boldsymbol{\alpha} \begin{pmatrix} g_{1j}^{(1)} & \dots & g_{1j}^{(h)} \\ & \vdots & \\ g_{kj}^{(1)} & \dots & g_{kj}^{(h)} \end{pmatrix}$$

From an additive code to a set of subspaces

Let C be an $\mathbb{F}_q$-linear $(n, q^k, d)_{q^h}$ code over $\mathbb{F}_{q^h}$.
Let G be a generator matrix for C over $\mathbb{F}_q$.

Take an $\mathbb{F}_q$-basis $\alpha_1, \dots, \alpha_h$ of $\mathbb{F}_{q^h}$ and write $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_h)$. The j^{th} column of G is of the form $\boldsymbol{\alpha} G_j$ for some unique $G_j \in \mathbb{F}_q^{h \times k}$.

$$\begin{pmatrix} g_{1j} \\ \vdots \\ g_{kj} \end{pmatrix} = \begin{pmatrix} \alpha_1 g_{1j}^{(1)} + \dots + \alpha_h g_{1j}^{(h)} \\ \vdots \\ \alpha_1 g_{kj}^{(1)} + \dots + \alpha_h g_{kj}^{(h)} \end{pmatrix} = \boldsymbol{\alpha} \begin{pmatrix} g_{1j}^{(1)} & \dots & g_{1j}^{(h)} \\ & \vdots & \\ g_{kj}^{(1)} & \dots & g_{kj}^{(h)} \end{pmatrix}$$

Consider the subspaces $\mathrm{ColSp}(G_1), \dots, \mathrm{ColSp}(G_n)$ of $\mathrm{PG}(k-1, q)$.

Equivalence

Definition

Call two $\mathbb{F}_q$-linear codes C and D over $\mathbb{F}_{q^h}$ *$\mathbb{F}_q$-equivalent* if C can be transformed into D by

1. permuting the coordinate positions,
2. in each coordinate, apply an $\mathbb{F}_q$-linear bijection. This bijection can be different for different coordinates.

Equivalence

Definition

Call two $\mathbb{F}_q$-linear codes C and D over $\mathbb{F}_{q^h}$ *$\mathbb{F}_q$-equivalent* if C can be transformed into D by

1. permuting the coordinate positions,
2. in each coordinate, apply an $\mathbb{F}_q$-linear bijection.

There exist an equivalence between:

1. equivalence classes of $\mathbb{F}_q$-linear $(n, q^k, d)_{q^h}$ codes,
2. $\mathrm{PGL}(k, q)$-orbits of multisets of n subspaces in $\mathrm{PG}(k-1, q)$ of dimension at most $h-1$.

Parameters of the code

	$\mathbb{F}_q$-linear code over $\mathbb{F}_{q^h}$	Set of subspaces of dimension $< h$
n	length	size
k	$\mathbb{F}_q$-dimension	(vector) dimension of the ambient projective space
d	minimum Hamming distance	minimum number of subspaces not contained in a hyperplane

Recognising linear codes

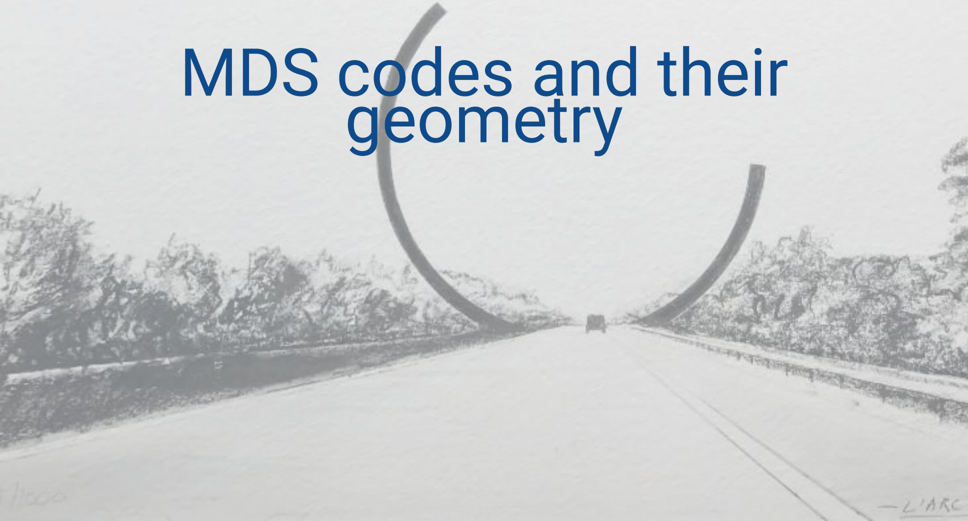
Theorem

An $\mathbb{F}_q$-linear $(n, q^k, d)_{q^h}$ code is $\mathbb{F}_q$-equivalent to a linear code

$$\Longleftrightarrow$$

its associated set of subspaces is a subset of a Desarguesian $(h-1)$-spread of $\mathrm{PG}(k-1, q)$.

MDS codes and their geometry



Linear MDS codes and arcs

Theorem (Singleton bound)

If an $(n, M, d)_q$ code exists, then

$$M \leq q^{n-d+1}.$$

Linear MDS codes and arcs

Theorem (Singleton bound)

If an $(n, M, d)_q$ code exists, then

$$M \leq q^{n-d+1}.$$

Codes meeting this bound are called MDS (maximum distance separable) codes.

Linear MDS codes and arcs

Theorem (Singleton bound)

If an $(n, M, d)_q$ *code exists, then*

$$M \leq q^{n-d+1}.$$

Codes meeting this bound are called MDS codes.

Proposition

A linear code is MDS

$$\iff$$

its associated point set is an arc, i.e. a set of points in $\mathrm{PG}(k-1, q)$ *of which any* k *span the space.*

Additive MDS codes and generalised arcs

Definition

A set of $(h-1)$-spaces in $\mathrm{PG}(kh-1,q)$ is a called a *generalised arc* if any k of them span the space.

Additive MDS codes and generalised arcs

Definition

A set of $(h-1)$-spaces in $\mathrm{PG}(kh-1,q)$ is a called a *generalised arc* if any k of them span the space.

Proposition (Ball, Lavrauw, Gamboa; 2021)

An $\mathbb{F}_q$-linear $(n, q^{kh}, d)_{q^h}$ code is MDS

$$\iff$$

its associated set of subspaces is a generalised arc of $(h-1)$-spaces in $\mathrm{PG}(kh-1,q)$.

Question

Can we make long additive MDS codes over finite fields, which aren't equivalent to linear codes?

Can we make large generalised arcs which aren't contained in a Desarguesian spread?

Generalised arcs and translation generalised quadrangles

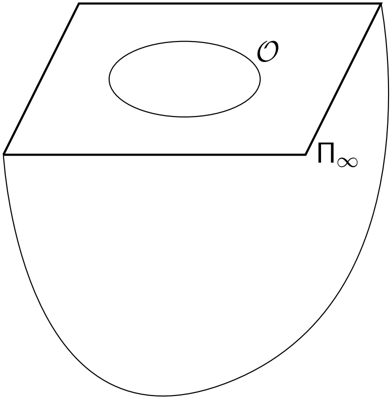
Generalised quadrangles

Definition

A *generalised quadrangle (GQ)* is a point- and block-regular incidence geometry such that given any point P and a line/block $\ell \not\ni P$, there is a unique point $Q \in \ell$ collinear to P.

The $\mathcal{T}_2(\mathcal{O})$ construction by Tits

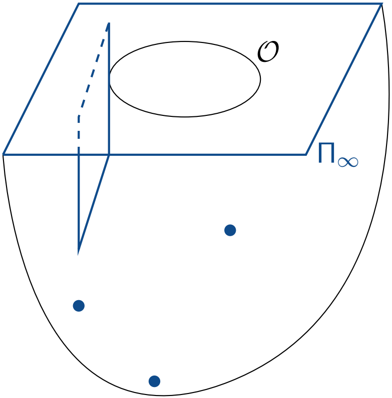
In PG$(3, q)$, take a plane Π_∞ and an oval $\mathcal{O} \subset \Pi_\infty$. We can construct a GQ



The $\mathcal{T}_2(\mathcal{O})$ construction by Tits

In $\mathrm{PG}(3, q)$, take a plane Π_∞ and an oval $\mathcal{O} \subset \Pi_\infty$. We can construct a GQ with

Points:
- affine points,
- planes intersecting Π_∞ in a tangent line to $\mathcal{O}$,
- Π_∞.

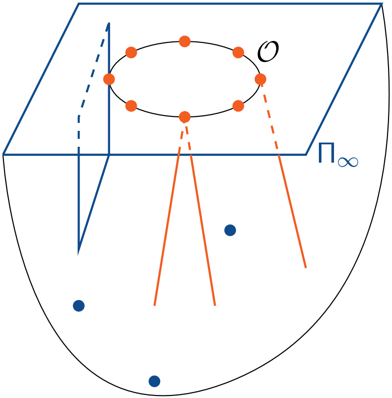


The $\mathcal{T}_2(\mathcal{O})$ construction by Tits

In PG$(3, q)$, take a plane Π_∞ and an oval $\mathcal{O} \subset \Pi_\infty$. We can construct a GQ with

Points:
- affine points,
- planes intersecting Π_∞ in a tangent line to $\mathcal{O}$,
- Π_∞.

Lines:
- lines intersecting Π_∞ in a point of $\mathcal{O}$,
- points of $\mathcal{O}$.



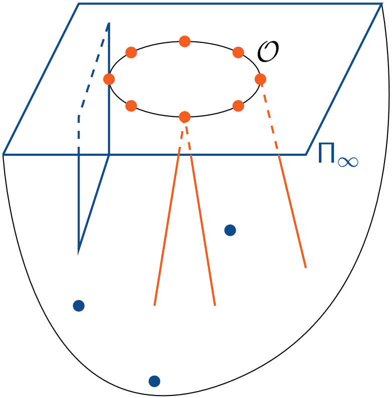
The $\mathcal{T}_2(\mathcal{O})$ construction by Tits

In PG$(3, q)$, take a plane Π_∞ and an oval $\mathcal{O} \subset \Pi_\infty$. We can construct a GQ with

Points:
- affine points,
- planes intersecting Π_∞ in a tangent line to $\mathcal{O}$,
- Π_∞.

Lines:
- lines intersecting Π_∞ in a point of $\mathcal{O}$,
- points of $\mathcal{O}$.

and the natural incidence inherited from PG$(3, q)$.



Translation generalised quadrangles

An oval is an arc of $q+1$ points in $\mathrm{PG}(2,q)$.

Translation generalised quadrangles

An oval is an arc of $q+1$ points in $\mathrm{PG}(2,q)$. The previous construction can be generalised using a generalised arc of q^h+1 $(h-1)$-spaces in $\mathrm{PG}(3h-1,q)$.

Translation generalised quadrangles

An oval is an arc of $q+1$ points in $\mathrm{PG}(2,q)$. The previous construction can be generalised using a generalised arc of q^h+1 $(h-1)$-spaces in $\mathrm{PG}(3h-1,q)$. These GQs can be characterised by certain properties of their automorphism group, and are called *translation GQs*.

Translation generalised quadrangles

An oval is an arc of $q+1$ points in $\mathrm{PG}(2,q)$. The previous construction can be generalised using a generalised arc of q^h+1 $(h-1)$-spaces in $\mathrm{PG}(3h-1,q)$. These GQs can be characterised by certain properties of their automorphism group, and are called *translation GQs*. The only known construction of such generalised arcs is through field reduction (i.e. they are contained in a Desarguesian spread).

Translation generalised quadrangles

An oval is an arc of $q+1$ points in $\mathrm{PG}(2,q)$. The previous construction can be generalised using a generalised arc of q^h+1 $(h-1)$-spaces in $\mathrm{PG}(3h-1,q)$. These GQs can be characterised by certain properties of their automorphism group, and are called *translation GQs*. The only known construction of such generalised arcs is through field reduction (i.e. they are contained in a Desarguesian spread). There have been efforts to prove that there are no other examples.

Projections of a generalised arc

Definition

Let $\mathcal{A} = \{\pi_1, \ldots, \pi_n\}$ be a generalised arc of $(h-1)$-spaces in $\mathrm{PG}(kh-1, q)$. The *projection* of $\mathcal{A}$ from π_j is constructed as follows.

Projections of a generalised arc

Definition

Let $\mathcal{A} = \{\pi_1, \ldots, \pi_n\}$ be a generalised arc of $(h-1)$-spaces in $\mathrm{PG}(kh-1, q)$. The *projection* of $\mathcal{A}$ from π_j is constructed as follows.

1. Take a $((k-1)h-1)$-space Σ skew to π_j,

Projections of a generalised arc

Definition

Let $\mathcal{A} = \{\pi_1, \ldots, \pi_n\}$ be a generalised arc of $(h-1)$-spaces in $\mathrm{PG}(kh-1, q)$. The *projection* of $\mathcal{A}$ from π_j is constructed as follows.

1. Take a $((k-1)h-1)$-space Σ skew to π_j,
2. construct $$\mathcal{A}' = \{\langle \pi_i, \pi_j \rangle \cap \Sigma \,\|\, i \neq j\},$$

Projections of a generalised arc

Definition

Let $\mathcal{A} = \{\pi_1, \ldots, \pi_n\}$ be a generalised arc of $(h-1)$-spaces in $\mathrm{PG}(kh-1, q)$. The *projection* of $\mathcal{A}$ from π_j is constructed as follows.

1. Take a $((k-1)h-1)$-space Σ skew to π_j,
2. construct $\mathcal{A}' = \{\langle \pi_i, \pi_j \rangle \cap \Sigma \parallel i \neq j\}$,
3. $\mathcal{A}'$ is a generalised arc of $(h-1)$-spaces in Σ and the choice of Σ irrelevant (up to isomorphism).

Projections of a generalised arc

Definition

Let $\mathcal{A} = \{\pi_1, \dots, \pi_n\}$ be a generalised arc of $(h-1)$-spaces in $\mathrm{PG}(kh-1, q)$. The *projection* of $\mathcal{A}$ from π_j is constructed as follows.

1. Take a $((k-1)h-1)$-space Σ skew to π_j,
2. construct $\mathcal{A}' = \{\langle \pi_i, \pi_j \rangle \cap \Sigma \,\|\, i \neq j\}$,
3. $\mathcal{A}'$ is a generalised arc of $(h-1)$-spaces in Σ and the choice of Σ irrelevant (up to isomorphism).

If $\mathcal{A}$ is associated to the $\mathbb{F}_q$-linear MDS code over $\mathbb{F}_{q^h}$, then $\mathcal{A}'$ is associated to

$$\{(c_1, \dots, c_{j-1}, c_{j+1}, \dots, c_n) \,\|\, (c_1, \dots, c_{j-1}, 0, c_{j+1}, \dots, c_n) \in C\}.$$

Generalised arcs through projections

Let $\mathcal{A}$ be a generalised arc of n $(h-1)$-spaces in PG$(3h-1, q)$. Call a generalised arc *linear* if it is contained in a Desarguesian spread.

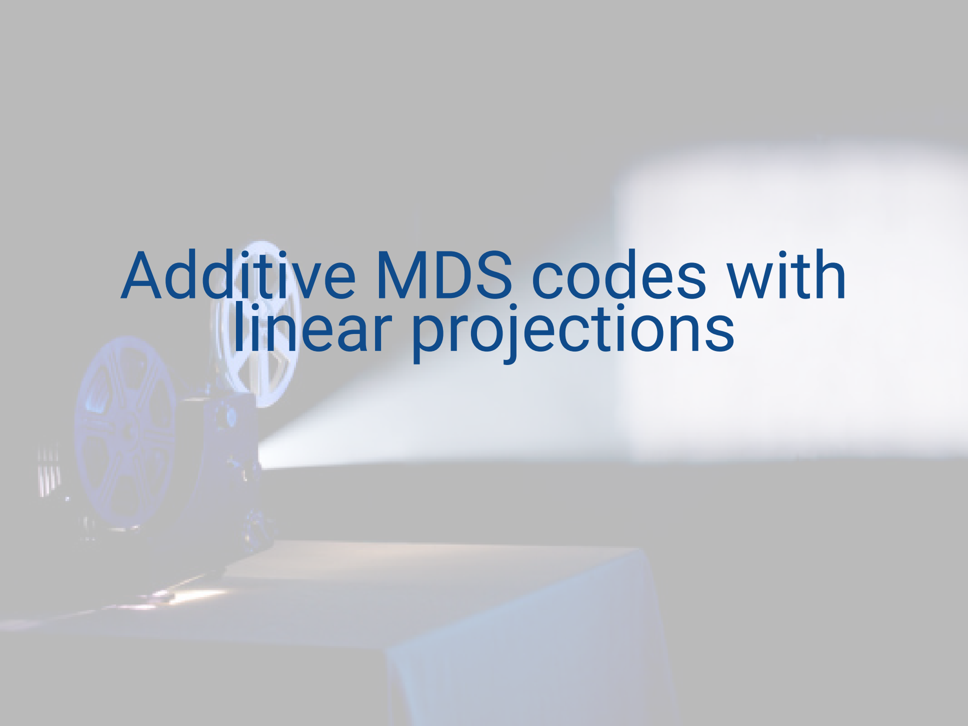
Generalised arcs through projections

Let $\mathcal{A}$ be a generalised arc of n $(h-1)$-spaces in $\mathrm{PG}(3h-1,q)$. Call a generalised arc *linear* if it is contained in a Desarguesian spread.

$\mathcal{A}$ is linear if

- (Penttila, Van de Voorde; 2013) q is odd, $n >$ size of the second largest complete arc in $\mathrm{PG}(2,q^h)$, $\mathcal{A}$ has at least 1 linear projection;
- (Rottey, Van de Voorde; 2015) (Thas; 2019) q is even, h is prime, $n = q^h + 1$, all projections of $\mathcal{A}$ are linear.

Additive MDS codes with linear projections



The projection of a code

Definition

Recall that the projection of a code C from the i^{th} coordinate equals

$$\{(\mathbf{c}_1, \mathbf{c}_2) \mid (\mathbf{c}_1, \underbrace{0}_{i^{\text{th}} \text{ coordinate}}, \mathbf{c}_2) \in C\}$$

The case $k > 3$

Theorem (A., Ball; 2022+)

Let C be an $\mathbb{F}_q$-linear $(n, q^{kh}, n-k+1)_{q^h}$ MDS code over $\mathbb{F}_{q^h}$. Suppose that

- $k > 3$,
- $n \geq q + k$,
- *there are two coordinates from which the projection of C is $\mathbb{F}_q$-equivalent to a linear code.*

Then C is $\mathbb{F}_q$-equivalent to an $\mathbb{F}_{q^s}$-linear code (for some $1 < s | h$).

The case $k > 3$

Theorem (A., Ball; 2022+)

Let C be an $\mathbb{F}_q$-linear $(n, q^{kh}, n-k+1)_{q^h}$ MDS code over $\mathbb{F}_{q^h}$. Suppose that

- $k > 3$,
- $n \geq q + k$,
- *there are two coordinates from which the projection of C is $\mathbb{F}_q$-equivalent to a linear code.*

Then C is $\mathbb{F}_q$-equivalent to an $\mathbb{F}_{q^s}$-linear code (for some $1 < s|h$).

Corollary

If the above conditions hold and $n \geq q^e + k$, with $e = \max\{t < h \mid\mid t|h\}$, then C is equivalent to a linear code.

The case $k = 3$

The case $k = 3$ is harder, since there is too little overlap in different projections.

The case $k = 3$

The case $k = 3$ is harder, since there is too little overlap in different projections.

Theorem (A., Ball; 2022+)

Suppose that C is an $\mathbb{F}_q$-linear $(n, q^{3h}, n-2)_{q^h}$ MDS code over $\mathbb{F}_{q^h}$, and suppose that

- $h \in \{2, 3\}$,
- $n \geq \max\{q^{h-1}, hq - 1\} + 4$,
- *There are 3 coordinates from which the projection of C is $\mathbb{F}_q$-equivalent to a linear code.*

Then C is $\mathbb{F}_q$-equivalent to a linear code.

Conclusion

We supported some evidence that if an additive MDS code over a finite field exists such that

- it is reasonably long,
- it is in a sense close to being (essentially) a linear code,

it must be (essentially) a linear code.

Conclusion

We supported some evidence that if an additive MDS code over a finite field exists such that

- it is reasonably long,
- it is in a sense close to being (essentially) a linear code,

it must be (essentially) a linear code.
Progress in this direction might help reduce the additive MDS conjecture to the linear MDS conjecture.


Summer school
Finite geometry & Friends
2nd edition
18-22 September 2023
Brussels