Linear codes from arcs and quadrics

Kanat Abdukhalikov

(Joint work with Duy Ho)

.

Dept of Mathematical Sciences, UAEU

Finite Geometries 2022
Sixth Irsee Conference
August 29 - September 2, 2022
Irsee, Germany

Outline

- Hyperovals and extended cyclic codes
- Maximal arcs and codes
- Ovoids and codes
- Vandermonde sets and LCD codes
- KM-arcs and codes

Ovals

$q = 2^m$

An oval in a projective plane $PG(2, q)$ is a set of $q + 1$ points, no three of which are collinear.

Hyperoval: set of $q + 2$ points, no three of which are collinear.

For any oval there is a unique point (called nucleus) that completes oval to hyperoval

Linear Codes and Sets of Points in Projective Spaces

Consider multi-set of n points $\mathcal{P} = \{\{P_1, P_2, \ldots, P_n\}\}$ from $PG(2, q)$.

Construct $(3 \times n)$-matrix G whose columns are points P_i.

Then one can consider a linear $[n, 3]$-code C with a generator matrix G.

If $\mathcal{P}$ is a hyperoval then C is an MDS code with parameters $[q + 2, 3, q]$.

MDS: $d = n - k + 1$

Extended Cyclic Codes and Sets of Hyperovals

Ding (2019) gave a construction extended cyclic code with parameters $[q+2, 3, q]$.
It is an MDS code. Therefore, it defines a hyperoval.

Theorem

Any extended cyclic code over $\mathbb{F}_q$ with parameters $[q+2, 3, q]$ is equivalent to an MDS code obtained from a regular hyperoval.

(Two codes are equivalent if one can be obtained from the other by a permutation of the coordinates)

Maximal Arcs

A $\{k; t\}$-arc in $PG(2, q)$ is a set $\mathcal{K}$ of k points such that t is the maximum number of points in $\mathcal{K}$ that are collinear.

$$k \leq (q+1)(t-1)+1$$

A $\{k; t\}$-arc in $PG(2, q)$ with $k = (q+1)(t-1)+1$ is called a *maximal arc*.

If $\mathcal{K}$ is a maximal $\{k; t\}$-arc in $PG(2, q)$ and $1 < t < q$ then q is even, t is a divisor of q, and every line in $PG(2, q)$ intersects $\mathcal{K}$ in 0 or t points.

The $\{q+2; 2\}$-arcs in $PG(2, q)$ are hyperovals.

Denniston Maximal Arcs

Choose $\delta \in F = \mathbb{F}_q$ such that the polynomial $X^2 + \delta X + 1$ is irreducible over F. For each $\lambda \in F$ consider the quadratic curve D_λ in $AG(2, q)$ defined by the equation $X^2 + \delta XY + Y^2 = \lambda$.

If $\lambda \neq 0$ then D_λ is a conic and its nucleus is the point $(0, 0)$. If $\lambda = 0$ then D_λ consists of the single point $(0, 0)$.

Let $\Delta \subseteq F$. Then the set

$$D = \bigcup_{\lambda \in \Delta} D_\lambda \tag{1}$$

is a maximal arc in $AG(2, q)$ (and therefore in $PG(2, q)$) if and only if Δ is a subgroup of the additive group of F. In this case D is a maximal $\{qt - q + t; t\}$-arc with $t = |\Delta|$.

Polar coordinate presentation

K/F field extension of degree 2, $K = \mathbb{F}_{2^n}$, $F = \mathbb{F}_{2^m}$, $n = 2m$.

Consider K as $AG(2, q)$, $q = 2^m$.
The *conjugate* of $x \in K$ over F is

$$\bar{x} = x^q.$$

Norm and *Trace* maps from K to F are

$$N(x) = x\bar{x}, \quad T = x + \bar{x}.$$

The unit circle of K is the set of elements of norm 1:

$$S = \{u \in K : N(x) = 1\}.$$

Each element $x \in K^*$ has a unique presentation

$$x = \lambda u$$

with $\lambda \in F^*$ and $u \in S$ (polar coordinate presentation).

The next theorem shows that in terms of polar coordinates the Denniston maximal arcs can be expressed in a very simple way.

Theorem

The Denniston maximal arcs (1) *can be expressed as*

$$D = \bigcup_{\lambda \in \Lambda} \lambda S \subset K, \tag{2}$$

where Λ *is a subgroup of the additive group of the field* F *and* S *is the unit circle of* K*.*

Codes from Denniston Arcs

De Winter, Ding & Tonchev (2019) gave a constuction of an extended cyclic code obtained from a Denniston arc.

They showed that this code has parameters $[qt - q + t, 3, qt - q]$ and nonzero weights $qt - q$ and $qt - q + t$. Furthermore, the dual minimum distance $d^{\perp}$ of the code C is 3 when $t > 2$ and 4 when $t = 2$ (hyperoval case).

We consider now the reverse process.

Theorem

Any extended cyclic code over $\mathbb{F}_q$ with parameters $[qt - q + t, 3, qt - q]$, $1 < t < q$, q is a power of t, is equivalent to a code obtained from a cyclic Denniston maximal arc.

Cyclic codes and ovoids

In $PG(n, q)$, $n \geq 3$, a set $\mathcal{K}$ of k points no three of which are collinear is called a *k-cap*.

For any k-cap $\mathcal{K}$ in $PG(3, q)$ with $q \neq 2$:

$$k \leq q^2 + 1.$$

A $(q^2 + 1)$-cap of $PG(3, q)$, $q \neq 2$, is called an *ovoid*.

A linear $[q^2 + 1, 4]$-code is called an *ovoid code* if the columns of its generator matrix G constitute an ovoid in $PG(3, q)$.

Cyclic codes and ovoids

Let Q be a non-degenerate quadratic form on 4-dimensional vector space V over F.

The set of singular points of Q defines either *hyperbolic* or *elliptic* quadric in $PG(3, q)$.

The elliptic quadric in $PG(3, q)$ is an ovoid and contains $q^2 + 1$ points.

Cyclic codes and ovoids

Ding (2019) introduced a family of cyclic codes with parameters $[q^2 + 1, 4, q^2 - q]$ and stated without proof that they can be obtained from elliptic quadrics. The next theorem proves this statement and shows a very natural connection between these cyclic codes and elliptic quadrics.

Theorem

A cyclic code over $\mathbb{F}_q$ with parameters $[q^2 + 1, 4, q^2 - q]$ is equivalent to an ovoid code obtained from an elliptic quadric in $PG(3, q)$.

Cyclic codes and ovoids

The next theorem provides a coordinate-free presentation of the elliptic quadric in $PG(3, q)$.

Theorem

Let $E \supset K \supset F$ be a chain of finite fields, $|E| = q^4$, $|K| = q^2$, $|F| = q$, $q = 2^m$. Then

$$Q(x) = Tr_{K/F}(N_{E/K}(x))$$

is a non-degenerate quadratic form on 4-dimensional vector space E over F. Moreover, the set

$$\mathcal{O} = \{u \in E \mid N_{E/K}(u) = 1\} = \{u \in E \mid u^{q^2+1} = 1\}$$

determines an elliptic quadric in $PG(3, q)$.

Vandermonde sets

(Gács, Weiner, Sziklai, Takáts, ...)
Let $1 < t < q^2$. A set $T = \{y_1, \cdots, y_t\} \subseteq K$ is called a *Vandermonde set* if

$$\pi_k(T) := \sum_{y \in T} y^k = 0,$$

for all $1 \leq k \leq t-2$.

The set T is a *super-Vandermonde set* if it is a Vandermonde set and $\pi_{t-1}(T) = 0$.

Vandermonde sets

We showed that if $\mathcal{O}$ is an oval with points in $AG(2, q) = K$ and nucleus 0, then $\mathcal{O}$ is a super-Vandermonde set.

Also, a hyperoval with points in $AG(2, q) = K$ is a Vandermonde set.

LCD codes

A linear code C over $\mathbb{F}_q$ is called a *Euclidean linear complementary dual code* (Euclidean LCD code) if $C \cap C^{\perp} = \{0\}$.

A linear code C over $\mathbb{F}_{q^2}$ is called a *Hermitian linear complementary dual code* (Hermitian LCD code) if $C \cap C^{\perp_H} = \{0\}$.

LCD codes

Let $V := \{v_1, \cdots, v_{q+1}\}$ be a super-Vandermonde set of size $q+1$ in K. Write $v_i = x_i + y_i\mathbf{i}$, where $x_i, y_i \in F$.
Let $\mathcal{C}_\psi = \mathcal{C}_\psi(V)$ be the $[q+2, 3]$-linear code over $\mathbb{F}_q$ with generator matrix

$$G = \begin{bmatrix} x_1 & x_2 & x_3 & \dots & x_{q+1} & 0 \\ y_1 & y_2 & y_3 & \dots & y_{q+1} & 0 \\ 1 & 1 & 1 & \dots & 1 & \psi \end{bmatrix}.$$

Theorem

For $\psi \neq 1$, the code $\mathcal{C}_\psi(V)$ is a Euclidean LCD code.

Corollary

Let $\mathcal{O}$ be an oval of $q+1$ points in K with nucleus at 0, $\psi \neq 1$. Then $\mathcal{C}_\psi(\mathcal{O})$ is a Euclidean LCD MDS code with parameters $[q+2, 3, q]$.

LCD codes

Let $V := \{v_1, \cdots, v_{q+1}\}$ be a super-Vandermonde set of size $q+1$ in K. Write $v_i = x_i + y_i\mathbf{i}$, where $x_i, y_i \in F$.
Let $\mathcal{C}_\alpha = \mathcal{C}_\alpha(V)$ be the $[q+2, 3]$-linear code over $\mathbb{F}_{q^2}$ with generator matrix

$$G = \begin{bmatrix} x_1 & x_2 & x_3 & \dots & x_{q+1} & 0 \\ y_1 & y_2 & y_3 & \dots & y_{q+1} & 0 \\ 1 & 1 & 1 & \dots & 1 & \alpha \end{bmatrix}.$$

Theorem

For $\alpha^{q+1} \neq 1$, the code $\mathcal{C}_\alpha(V)$ is a Hermitian LCD code.

Corollary

Let $\mathcal{O}$ be an oval of $q+1$ points in K with nucleus at 0, $\alpha^{q+1} \neq 1$. Then $\mathcal{C}_\alpha(\mathcal{O})$ is a Hermitian LCD MDS code with parameters $[q+2, 3, q]$.

KM-arcs and codes

In the projective plane $PG(2, q)$, a *KM-arc of type t* is a set H of $q + t$ points meeting every line in $0, 2$ or t points.
(Korchmáros & Mazzocca (1990): $(q + t)$-arcs of type $(0, 2, t)$)
(Gács, Weiner, De Boeck, Van de Voorde, ...)

If H is a KM-arc of type t in $PG(2, q)$, $2 < t < q$, then

1. q is even and t is a divisor of q;
2. each point of H is on exactly one t-secant
3. there are $\frac{q}{t} + 1$ different t-secants to H, and they are concurrent at a unique point called the *t-nucleus* of H;

KM-arcs and codes

Definition

Let $t \geq 2$. A set H of $q + t$ points in $K = AG(2, q)$ is called a *star-set* if all points of H belong to a union of $\frac{q}{t} + 1$ lines concurrent at 0, and each line contains t points of H.

$$E := \left\{ \sum_{j=0}^{m-1} 2^j x_j > 0 \mid x_j \in \{0, 1, q\} \right\}.$$

Theorem

Let H be a star-set. Then H is a KM-arc of type t with t-nucleus at 0 if and only if $\pi_e(H) = 0$ for all $e \in E$.

KM-arcs and codes

Theorem

Let H be a KM-arc of type $t > 2$ *with points in* K *and nucleus at* 0. *Then the associated code C is a three-weight* $[q+t, 3, q]$*-code with weight enumerator*

$$A(z) = 1 + Xz^{q} + Yz^{q+t-2} + Zz^{q+t},$$

where

$$X = \frac{(q-1)(q+t)}{t},$$

$$Y = \frac{q(q-1)(q+t)}{2},$$

and

$$Z = \frac{q(q-1)(qt - t^{2} + 2t - 2)}{2t}.$$

The dual distance of C is 3.

Thank you for your attention!