# Three paths to the rank metric

Linearized polynomials

M. Ceria
Politecnico di Bari

# Textbooks

Wu, Baofeng, and Zhuojun Liu. Linearized polynomials over finite fields revisited. Finite Fields and Their Applications 22 (2013): 79-100.

Polverino, O., Zullo, F. (2020). Connections between scattered linear sets and MRD-codes, Bulletin of the ICA Volume 89 (2020), 46–74

# LINEARIZED POLYNOMIALS

Polynomials of the form

$$L(x) := \sum_{i=0}^{r} a_i x^{q^i},\ r \in \mathbb{N}, a_i \in \mathbb{F}_{q^n}$$

$$\mathcal{L}(\mathbb{F}_{q^n}) = \{\sum_{i=0}^{r} a_i x^{q^i},\ r \in \mathbb{N}, a_i \in \mathbb{F}_{q^n}\}$$

# AND THE *modular* VERSION

Linearized polynomials induce $\mathbb{F}_q$-linear endomorphisms of $\mathbb{F}_{q^n}$

As maps between finite fields we consider them as

$$L(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_{q^n}[x]/(x^{q^n} - x)$$

$$\mathcal{L}_n(\mathbb{F}_{q^n}) = \{all \sum_{i=0}^{n-1} a_i x^{q^i}\}$$

# Multiplication (Ore)

$$L_1(x) := \sum_{i=0}^{r} a_i x^{q^i} \quad L_2(x) := \sum_{i=0}^{s} b_i x^{q^i}$$

Not closed for multiplication: symbolic multiplication is composition which makes the set a ring:

$$L_1(x) \circ L_2(x) = L_1(L_2(x))$$
$$L_2(x) \circ L_1(x) = L_2(L_1(x))$$

# THE STRUCTURE OF $\mathcal{L}(\mathbb{F}_{q^n}), \mathcal{L}_n(\mathbb{F}_{q^n})$

## VECTOR SPACE OVER $\mathbb{F}_{q^n}$

sum and multiplication by elements in $\mathbb{F}_{q^n}$

## ALGEBRA OVER $\mathbb{F}_q$

Addition - composition - scalar multiplication by elements of $\mathbb{F}_q$

$\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$ subfield ($m \mid n$); $\mathcal{L}_n(\mathbb{F}_{q^m}) \subseteq \mathcal{L}_n(\mathbb{F}_{q^n})$, $\mathbb{F}_q$-subalgebra.

# Ore polynomials

$R[y]$, $R$ domain (non-necessarily commutative).

## Conjugate

$$\alpha : R \to R$$

## Derivative

$$\delta : R \to R$$

$$y \cdot r = \alpha(r)y + \delta(r)$$

# Ore polynomials

$$y \cdot r = \alpha(r)y + \delta(r)$$

## Ore extension $R[y; \alpha, \delta]$

- $\forall r \in R \; \alpha(r) = 0 \Rightarrow r = 0$ ($\alpha$ injective);
- $\alpha$ ring endomorphism;
- $\delta$ is an $\alpha$-derivation
    - **additive**;
    - $\forall r, r' \in R : \delta(rr') = \alpha(r)\delta(r') + \delta(r)r'$

# Skew polynomials over $\mathbb{F}_{q^n}$

## Our $\alpha$

$$\begin{aligned}\sigma :& \mathbb{F}_{q^n} \to \mathbb{F}_{q^n} \\ & y \mapsto y^q\end{aligned}$$

## Our $\delta$

$\delta = 0$

## $\mathbb{F}_{q^n}[y; \sigma]$

$$y \cdot a = \sigma(a)y = a^q y$$

It is a PID.

## On the Ore polynomials

We will need Ore polynomials of the form $\mathbb{F}_{q^n}[y;\sigma]$.

### Some facts

- $\mathbb{F}_{q^n}[y;\sigma]$ is a noncommutative integral domain;
- $\mathbb{F}_{q^n}[y;\sigma]$ is **not** a UFD;
- $\mathbb{F}_{q^n}[y;\sigma]$ is right and left Euclidean domain (standard degree);
- The centre of $\mathbb{F}_{q^n}[y;\sigma]$ is $\mathbb{F}_q[y^n;\sigma] \simeq \mathbb{F}_q[z]$ (commutative polynomial ring) and $n$ the order of $\sigma$;
- $\mathbb{F}_{q^n}[y;\sigma]$ is a PID and its prime bilateral ideals are generated by elements of the form $f(y^n)$, with $n$ the order of $\sigma$ and $f \in \mathbb{F}_q[z]$ irreducible.

(See for example N. Jacobson, Finite-dimensional division algebras over fields, Springer, Berlin, 1996).

# Division, GCDs, lcms...

We can do right and left Euclidean division, so, let $f, g \in \mathbb{F}_{q^n}[y;\sigma]$

### *gcrd*$(f, g)$

unique monic $d \in \mathbb{F}_{q^n}[y;\sigma]$ of maximal degree s.t. there are $u, u' \in \mathbb{F}_{q^n}[y;\sigma]$ s.t. $f = ud$, $g = u'd$

### *lclm*$(f, g)$

unique monic $m \in \mathbb{F}_{q^n}[y;\sigma]$ of minimal degree s.t. there are $u, u' \in \mathbb{F}_{q^n}[y;\sigma]$ s.t. $m = uf = u'g$.

### Minimal central left multiple of $f$

unique monic $F(y^n) \in \mathbb{F}_{q^n}[y;\sigma]$ of minimal degree in $Z(\mathbb{F}_{q^n}[y;\sigma])$ s.t. $F(y^n) = gf$ for some $g \in \mathbb{F}_{q^n}[y;\sigma]$.

# Some properties

Let us consider $\mathbb{F}_{q^n}[y;\sigma]$

If $f$ factorizes as $f = g_1 \cdots g_k = h_1 \cdots h_m$ then $k = m$ and there is a permutation $\pi \in S_k$: $\deg(g_{\pi(i)}) = \deg(h_i)$ for each $i$;

If $F$ irreducible polynomial in $\mathbb{F}_q[z]$ then every irreducible right divisor of $F(y^n)$ in $\mathbb{F}_{q^n}[y;\sigma]$ has degree equal to $\deg(F)$ and every right divisor of $F(y^n)$ in $\mathbb{F}_{q^n}[y;\sigma]$ has degree equal to $k\deg(F)$ for some $k \in \{1, ..., n\}$

$f \in \mathbb{F}_{q^n}[y;\sigma]$ irreducible, then its minimal central left multiple $F(y^n)$ is s.t. $F$ is an irreducible polynomial in $\mathbb{F}_q[z]$ of degree $\deg(f)$.

# Ore and linearized polynomials

## Idea

$1 \mapsto x$
$y \mapsto x^q$
$y^a \mapsto x^{q^a}$
$y^{a+b} = y^a y^b \mapsto x^{q^a} \circ x^{q^b} = x^{(q^{a+b})}$.

$$\phi : \mathbb{F}_{q^n}[y;\sigma] \to \mathcal{L}(\mathbb{F}_{q^n})$$
$$\sum_{i=0}^{r} a_i y^i \mapsto \sum_{i=0}^{r} a_i x^{q^i}$$

# Ore and linearized polynomials

$$\begin{aligned} \phi : & \mathbb{F}_{q^n}[y;\sigma] \to \mathcal{L}(\mathbb{F}_{q^n}) \\ & \sum_{i=0}^{r} a_i y^i \mapsto \sum_{i=0}^{r} a_i x^{q^i} \end{aligned}$$

Algebra isomorphism, so...

$$\mathcal{L}(\mathbb{F}_{q^n}) \cong \mathbb{F}_{q^n}[y;\sigma]$$

Two-side ideals

$$(y^n - 1) \triangleleft \mathbb{F}_{q^n}[y;\sigma]$$
$$(x^{q^n} - x) \triangleleft \mathcal{L}(\mathbb{F}_{q^n})$$

$$\phi(y^n - 1) = x^{q^n} - x$$

$$\mathcal{L}_n(\mathbb{F}_{q^n}) = \mathcal{L}(\mathbb{F}_{q^n})/(x^{q^n} - x) \cong \mathbb{F}_{q^n}[y;\sigma]/(y^n - 1)$$

# Semi-linear group algebra

B. McDonald, Finite Rings with Identity, Dekker, New York, 1974.

Let $G = Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle \sigma \rangle$

$\mathbb{F}_{q^n}[G]$: $\mathbb{F}_{q^n}$-vector space generated by $G$'s elements.

$$(a\sigma^i)(b\sigma^j) = a\sigma^i(b)\sigma^{i+j} = ab^{q^i}\sigma^{i+j},\ a, b \in \mathbb{F}_{q^n}$$

Semilinear group ring with this kind of multiplication.
Scalar multiplication with elements in $\mathbb{F}_q$: $\mathbb{F}_q$-algebra.

# And another isomorphism

$$\mathbb{F}_{q^n}[G] \to \mathcal{L}_n(\mathbb{F}_{q^n})$$
$$\sum_{i=0}^{n-1} a_i \sigma^i \mapsto \sum_{i=0}^{n-1} a_i x^{q^i}$$

$$\mathcal{L}_n(\mathbb{F}_{q^n}) \cong \mathbb{F}_{q^n}[G]$$

# Matrix Algebra

B. McDonald, Finite Rings with Identity, Dekker, New York, 1974.

$M_n(\mathbb{F}_q)$: matrix algebra over $\mathbb{F}_q$
$End(\mathbb{F}_{q^n})$: endomorphisms of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.
The transformations can be induced by a linearized polynomial over $\mathbb{F}_{q^n}$.

### $\mathbb{F}_q$-algebra isomorphism

$$End(\mathbb{F}_{q^n}) \to \mathcal{L}_n(\mathbb{F}_{q^n})$$
$$\sum_{i=0}^{n-1} a_i\sigma^i \mapsto \sum_{i=0}^{n-1} a_i x^{q^i}$$

$$\mathcal{L}_n(\mathbb{F}_{q^n}) \cong End(\mathbb{F}_{q^n}) \cong M_n(\mathbb{F}_q)$$

Suppose $E$ is a $K$-vector space.

$$E^* = Hom_k(E, K)$$

**Tensor space**: $E^* \otimes_K E$: consider the multiplication, $\forall l_1, l_2 \in E^*$, $\forall x_1, x_2 \in E$

$$(l_1 \otimes x_1)(l_2 \otimes x_2) = l_1(x_2) l_2 \otimes x_1$$

and the expand via linearity.

# Composition algebra

Associative non-commutative algebra.

$$\Lambda : E^* \otimes_K E \to End_K(E)$$

$$(l \otimes x)(y) \mapsto l(y)x$$

Isomorphism when $\dim_K(E)$ is finite giving

$$E^* \otimes_K E \cong End_K(E)$$

# In our case

$E = \mathbb{F}_{q^n}$; $\dim_{\mathbb{F}_q}(E) = n$

We know

$$L_n(\mathbb{F}_{q^n}) \cong End(\mathbb{F}_{q^n})$$

So...

$$L_n(\mathbb{F}_{q^n}) \cong \mathbb{F}^*_{q^n} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$$

# Dickson matrices

## Dickson matrix / $\sigma$−circulant

$$D_L = (a_{j-i}^{q^i}) \in M_n(\mathbb{F}_{q^n})$$

ASSOCIATED TO

$$L(x) := \sum_{i=0}^{n-1} a_i x^{q^i}$$

# Dickson matrices

The linear transformation associated to $L$, if $B = \{\beta_0, ..., \beta_{n-1}\}$, can be described as

$$M_L = (\beta_j^{q^i})^{-1} D_L (\beta_j^{q^i})$$

AN $\mathbb{F}_q$ – *algebra*

$$\mathcal{D}_n(\mathbb{F}_{q^n}) = (\beta_j^{q^i})M_n(\mathbb{F}_{q^n})(\beta_j^{q^i})^{-1}$$

$$\mathcal{D}_n(\mathbb{F}_{q^n}) \cong M_n(\mathbb{F}_q) \cong \mathcal{L}_n(\mathbb{F}_{q^n})$$

# Recall on MRMC

$C \leq M_{n,m}(\mathbb{F}_q)$, we can see it as a subspace of $Hom(\mathbb{F}_q^m, \mathbb{F}_q^n)$.

*$m \geq n$*

We can see $\mathbb{F}_q^n$ as a subspace of $\mathbb{F}_q^m$ considering $Hom(\mathbb{F}_q^m, \mathbb{F}_q^n)$ as the subspace of $Hom(\mathbb{F}_q^m, \mathbb{F}_q^m)$ whose image is indeed contained in $\mathbb{F}_q^n$. We recall also that $\mathbb{F}_q^m \cong \mathbb{F}_{q^m}$ and that $End(\mathbb{F}_{q^m}) \cong \mathcal{L}_m(\mathbb{F}_{q^m})$

# LINEARIZED POLYNOMIALS AND RMC

We can see a RMC as $\mathbb{F}_q$-subspace of $\mathcal{L}_m(\mathbb{F}_{q^m})$

We can then restate definitions in terms of linearized polynomials.

# Example: Duality

$f, g \in \mathcal{L}_m(\mathbb{F}_{q^m})$

## Bilinear form

$$b : \mathcal{L}_m(\mathbb{F}_{q^m}) \times \mathcal{L}_m(\mathbb{F}_{q^m}) \to \mathbb{F}_q$$
$$(f, g) \mapsto Tr_{q^m/q}\left(\sum_{i=0}^{m-1} f_i g_i\right)$$

## Duality

$\mathcal{C}^{\perp} = \{f \in \mathcal{L}_m(\mathbb{F}_{q^m}) : b(f, g) = 0,\ \forall g \in \mathcal{C}\}$

# Adjoint code

Adjoint of $L(x) = \sum_{i=0}^{m-1} a_i x^{q^i}$ w.r.t.

## Bilinear form

$$b : \mathcal{L}_m(\mathbb{F}_{q^m}) \times \mathcal{L}_m(\mathbb{F}_{q^m}) \to \mathbb{F}_q$$
$$(f, g) \mapsto Tr_{q^m/q}\left(\sum_{i=0}^{m-1} f_i g_i\right)$$

$$\hat{L}(x) = \sum_{i=0}^{m-1} a_i^{q^{m-i}} x^{q^{m-i}}$$

# Adjoint code

Adjoint of $L(x) = \sum_{i=0}^{m-1} a_i x^{q^i}$ w.r.t. $b$

$\hat{L}(x) = \sum_{i=0}^{m-1} a_i^{q^{m-i}} x^{q^{m-i}}$

## Adjoint code

$$\mathcal{C}_T = \{\hat{L} : L \in \mathcal{C}\} \subseteq \mathcal{L}_m(\mathbb{F}_{q^m}).$$

# The equivalence issue

$\mathcal{C} \subset M_{n,m}(\mathbb{F}_q)$ non-necessarily linear.

$m \neq n$

$\mathcal{C} \sim \mathcal{C}'$ iff there are $X \in GL_n(q)$, $Y \in GL_m(q)$, $Z \in M_{n,m}(\mathbb{F}_q)$ and $\sigma \in Aut(\mathbb{F}_q)$:

$$\mathcal{C}' = \{X\sigma(C)Y + Z : \ C \in \mathcal{C}\}$$

$m = n$: equivalent

$\mathcal{C} \sim \mathcal{C}'$ iff there are $X, Y \in GL_n(q)$, $Z \in M_n(\mathbb{F}_q)$ and $\sigma \in Aut(\mathbb{F}_q)$:

$$\mathcal{C}' = \{X\sigma(C)Y + Z : \ C \in \mathcal{C}\}$$

# THE EQUIVALENCE ISSUE

$m = n$: WEAKLY EQUIVALENT

$\mathcal{C} \sim' \mathcal{C}'$ iff there are $X, Y \in GL_n(q)$, $Z \in M_n(\mathbb{F}_q)$ and $\sigma \in Aut(\mathbb{F}_q)$:

$$\mathcal{C}' = \{X\sigma(C)Y + Z : \ C \in \mathcal{C}\}$$

or

$$\mathcal{C}' = \{X\sigma(C_T)Y + Z : \ C \in \mathcal{C}\}$$

Equivalent to the code $\mathcal{C}$ or $\mathcal{C}_T$.

# The equivalence issue

If linear we can suppose $Z = 0$.

Difficult to decide on equivalence.

Liebhold and Nebe – Lunardon, Trombetti and Zhou

Let $\mathcal{C} \subset M_{n,m}(\mathbb{F}_q)$

**Left – middle nucleus**

$$L(\mathcal{C}) := \{Y \in M_n(\mathbb{F}_q) : \; YA \in \mathcal{C} \, \forall A \in \mathcal{C}\}$$

**Right – right nucleus**

$$R(\mathcal{C}) := \{Z \in M_m(\mathbb{F}_q) : \; AZ \in \mathcal{C} \, \forall A \in \mathcal{C}\}$$

LUNARDON, TROMBETTI ZHOU

$\mathcal{C}, \mathcal{C}' \leq M_{n,m}(\mathbb{F}_q)$ linear MRMC. Suppose $\mathcal{C} \sim \mathcal{C}'$.
Then their left (right) idealizers are equivalent.

$\mathcal{C} \leq M_{n,m}(\mathbb{F}_q)$ linear MRMC.

$$L(\mathcal{C}_T) = R(\mathcal{C})_T \text{ and } R(\mathcal{C}_T) = L(\mathcal{C})_T$$
$$L(\mathcal{C}^\perp) = L(\mathcal{C})_T \text{ and } R(\mathcal{C}^\perp) = R(\mathcal{C})_T$$

# IDEALIZERS

LUNARDON, TROMBETTI ZHOU

$\mathcal{C} \leq M_{n,m}(\mathbb{F}_q)$ linear MRMC. Let $d_{min}(\mathcal{C}) = d > 1$.

$n \leq m$

$L(\mathcal{C})$ is a finite field whose size does not exceed $q^n$

$n \geq m$

$R(\mathcal{C})$ is a finite field whose size does not exceed $q^m$

For $n = m$ they are both finite fields.

# Idealizers in terms of linearized polynomials

$$L(\mathcal{C}) = \{\phi \in \mathcal{L}_m(\mathbb{F}_{q^m}) : \phi \circ f \in \mathcal{C}\, \forall f \in \mathcal{C}\}$$

$$R(\mathcal{C}) = \{\phi \in \mathcal{L}_m(\mathbb{F}_{q^m}) : f \circ \phi \in \mathcal{C}\, \forall f \in \mathcal{C}\}$$

# $\mathbb{F}_{q^m}$-LINEARITY

$$F_m = \{\alpha x : \alpha \in \mathbb{F}_{q^m}\}$$

**LEFT**

$L(\mathcal{C}) = F_m$

**RIGHT**

$R(\mathcal{C}) = F_m$

## Csajbók-Marino-Polverino-Zanella-Zhou

$\mathcal{C}$ $\mathbb{F}_q$-linear MRD-code, $\dim(\mathcal{C}) = mk$ with parameters $[m, m, q; m - k + 1]$. Then $L(\mathcal{C})$ has maximum order $q^{mk}$ if and only if there exists another MRD code, $\mathcal{C}' \sim \mathcal{C}$ that is $\mathbb{F}_{q^m}$-linear on the left.

$\mathcal{C}$ $\mathbb{F}_q$-linear MRD-code, $\dim(\mathcal{C}) = mk$ with parameters $[m, m, q; m - k + 1]$. Then $R(\mathcal{C})$ has maximum order $q^{mk}$ if and only if there exists another MRD code, $\mathcal{C}' \sim \mathcal{C}$ that is $\mathbb{F}_{q^m}$-linear on the right.

# Some MRD codes

## Gabidulin codes

$k \leq n-1$

$$\mathcal{G}_k = \left\{ \sum_{i=0}^{k-1} a_i x^{q^i},\ a_i \in \mathbb{F}_{q^n} \right\} = \langle x, x^q, \ldots, x^{q^{k-1}} \rangle$$

## Generalized

$k \leq n-1,\ GCD(s,n) = 1$

$$\mathcal{G}_{k,s} = \left\{ \sum_{i=0}^{k-1} a_i x^{q^{si}},\ a_i \in \mathbb{F}_{q^n} \right\} = \langle x, x^{q^s}, \ldots, x^{q^{s(k-1)}} \rangle$$

# Some MRD codes

## Twisted Gabidulin codes - Sheekey

$k \leq n-1$, $\eta \in \mathbb{F}_{q^n}$ with $N_{q^n/q}(\eta) \neq (-1)^{nk}$

$$\mathcal{H}_k(\eta, h) = \left\{ a_0^{q^h} \eta x^{q^k} + \sum_{i=0}^{k-1} a_i x^{q^i},\ a_i \in \mathbb{F}_{q^n} \right\}$$

## Generalized - Sheekey

$k \leq n-1$, $GCD(s, n) = 1$, $\eta \in \mathbb{F}_{q^n}$ with $N_{q^n/q}(\eta) \neq (-1)^{nk}$

$$\mathcal{H}_{k,s}(\eta, h) = \left\{ a_0^{q^h} \eta x^{q^{sk}} + \sum_{i=0}^{k-1} a_i x^{q^{si}},\ a_i \in \mathbb{F}_{q^n} \right\}$$

Thew both have dimension $nk$.

# Some MRD codes

### Additive generalized twisted Gabidulin codes – Otal and Özbudak

$k \leq n-1$, $GCD(s,n)=1$, $q=q_0^u$ $\eta \in \mathbb{F}_{q^n}$ with $N_{q^n/q}(\eta) \neq (-1)^{nku}$

$$\mathcal{A}_{k,s,q_0}(\eta,h)=\left\{a_0^{q_0^h}\eta x^{q^{sk}}+\sum_{i=0}^{k-1}a_i x^{q^{si}},\ a_i \in \mathbb{F}_{q^n}\right\}$$

### Trombetti and Zhou

$n$ even, $GCD(s,n)=1$, $\eta \in \mathbb{F}_{q^n}$ with $N_{q^n/q}(\eta)$ non-square in $\mathbb{F}_q$

$$\mathcal{D}_{k,s}(\eta,h)=\left\{ax+\eta b x^{sk}+\sum_{i=1}^{k-1}c_i x^{q^{si}},\ c_i \in \mathbb{F}_{q^n}, a,b \in \mathbb{F}_{q^{n/2}}\right\}$$

# Some MRD codes

## Csajbók-Marino-Polverino-Zanella

$q > 4$: $\exists \delta \in \mathbb{F}_{q^2}$ s.t.

$$\langle x, \delta x^q + x^{q^4} \rangle_{\mathbb{F}_{q^6}}$$

MRD with parameters $(6, 6, q, 5)$.

## Its dual

equivalent to

$$\langle x^q, x^{q^2}, x^{q^4}, x - \delta^q x^{q^3} \rangle_{\mathbb{F}_{q^6}}$$

MRD with parameters $(6, 6, q, 3)$.

# Some MRD codes

### Csajbók-Marino-Polverino-Zanella

$q$ odd, $\delta \in \mathbb{F}_{q^8}$ s.t. $\delta^2 = -1$

$$\langle x, \delta x^q + x^{q^5} \rangle_{\mathbb{F}_{q^8}}$$

MRD with parameters $(8, 8, q, 7)$.

### Its dual

equivalent to

$$\langle x^q, x^{q^2}, x^{q^3}, x^{q^5}, x^{q^6}, x - \delta x^{q^4} \rangle_{\mathbb{F}_{q^8}}$$

MRD with parameters $(8, 8, q, 3)$.

# Some MRD codes

### Csajbók-Marino-Zullo

$q \equiv 0, \pm 1 \mod 5$ odd, $\delta^2 + \delta = 1$

$$\langle x, x^q + x^{q^3} + \delta x^{q^5} \rangle_{\mathbb{F}_{q^6}}$$

MRD with parameters $(6, 6, q, 5)$.
**Marino-Montanucci-Zullo:** for each $q$ odd.

### Its dual

equivalent to

$$\langle x^q, x^{q^3}, -x + x^{q^2}, \delta x - \delta x^{q^4} \rangle_{\mathbb{F}_{q^6}}$$

MRD with parameters $(6, 6, q, 3)$.

# Some MRD codes

### Zanella-Zullo

$q$ odd, $q \equiv 1 \mod 4$, $q \leq 29$

$$\langle x, x^q - x^{q^2} + x^{q^4} + x^{q^5} \rangle_{\mathbb{F}_{q^6}}$$

MRD with parameters $(6, 6, q, 5)$.

### Its dual

equivalent to

$$\langle x^{q^3}, x^q + x^{q^2}, x^q - x^{q^4}, x^q - x^{q^5} \rangle_{\mathbb{F}_{q^6}}$$

MRD with parameters $(6, 6, q, 3)$.

# Some MRD codes

### Bartoli-Zanella-Zullo

$q$ odd, $h \in \mathbb{F}_{q^6}$: $h^{q^3+1} = -1$

$$\langle x, h^{q-1}x^q - h^{q^2-1}x^{q^2} + x^{q^4} + x^{q^5} \rangle_{\mathbb{F}_{q^6}}$$

MRD with parameters $(6, 6, q, 5)$.

### Its dual

equivalent to

$$\langle x^{q^3}, h^{q^2}x^q + h^q x^{q^2}, x^q - h^{q-1}x^{q^4}, x^q - h^{q-1}x^{q^5} \rangle_{\mathbb{F}_{q^6}}$$

MRD with parameters $(6, 6, q, 3)$.

# Some MRD codes

## Csajbók-Marino-Polverino-Zhou

$q$ odd, $GCD(s,7)=1$

$$\langle x, x^{q^s}, x^{q^{3s}} \rangle_{\mathbb{F}_{q^7}}$$

MRD with parameters $(7,7,q,5)$.

## Its dual

equivalent to

$$\langle x, x^{q^{2s}}, x^{q^{3s}}, x^{q^{4s}} \rangle_{\mathbb{F}_{q^7}}$$

MRD with parameters $(7,7,q,4)$.

# Some MRD codes

### Csajbók-Marino-Polverino-Zhou

$q \equiv 1 \mod 3$, $GDC(s, 8) = 1$

$$\langle x, x^{q^s}, x^{q^{3s}} \rangle_{\mathbb{F}_{q^8}}$$

MRD with parameters $(8, 8, q, 6)$.

### Its dual

equivalent to

$$\langle x, x^{q^{2s}}, x^{q^{3s}}, x^{q^{4s}}, x^{q^{5s}} \rangle_{\mathbb{F}_{q^8}}$$

MRD with parameters $(8, 8, q, 4)$.

***Thank you for your attention!***