Universitat d'Alacant
Universidad de Alicante

EDEM
Escuela de Empresarios

Coding theory and cryptography
A conference in the honor of Joachim Rosenthal's 60th birthday

Cyclic Orbit Flag Codes

Miguel Ángel Navarro-Pérez

Joint work with Clementa Alonso-González

July 15, 2022

mnavarro@edem.es

Outline

Notation

Let...

- q be a prime power,
- $\mathbb{F}_q$ denote the finite field with q elements,
- n be a positive integer,
- $\mathbb{F}_{q^n}$ is the extension field with q^n elements.

Outline

1. Cyclic orbit subspace codes
2. Cyclic orbit flag codes and their best friend
3. Flag codes with prescribed best friend

Subspace codes

Metric space

Given two $\mathbb{F}_q$-subspaces $\mathcal{U}, \mathcal{V}$ of $\mathbb{F}_{q^n}$, their subspace distance is

$$d_S(\mathcal{U}, \mathcal{V}) = \dim_q(\mathcal{U} + \mathcal{V}) - \dim_q(\mathcal{U} \cap \mathcal{V}).$$

Definition

A **subspace code** (of length n) is a nonempty collection $\mathcal{C}$ of $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^n}$. Its minimum distance is

$$d_S(\mathcal{C}) = \min\{d_S(\mathcal{U}, \mathcal{V}) \mid \mathcal{U}, \mathcal{V} \in \mathcal{C},\ \mathcal{U} \neq \mathcal{V}\}.$$

If every element in a subspace code has the same dimension

constant dimension code.

Subspace codes

Metric space

Given two $\mathbb{F}_q$-subspaces $\mathcal{U}, \mathcal{V}$ of $\mathbb{F}_{q^n}$, their subspace distance is

$$d_S(\mathcal{U}, \mathcal{V}) = \dim_q(\mathcal{U} + \mathcal{V}) - \dim_q(\mathcal{U} \cap \mathcal{V}).$$

Definition

A **subspace code** (of length n) is a nonempty collection $\mathcal{C}$ of $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^n}$. Its minimum distance is

$$d_S(\mathcal{C}) = \min\{d_S(\mathcal{U}, \mathcal{V}) \mid \mathcal{U}, \mathcal{V} \in \mathcal{C},\ \mathcal{U} \neq \mathcal{V}\}.$$

If every element in a subspace code has the same dimension

constant dimension code.

Subspace codes

Metric space

Given two $\mathbb{F}_q$-subspaces $\mathcal{U}, \mathcal{V}$ of $\mathbb{F}_{q^n}$, their subspace distance is

$$d_S(\mathcal{U}, \mathcal{V}) = \dim_q(\mathcal{U} + \mathcal{V}) - \dim_q(\mathcal{U} \cap \mathcal{V}).$$

Definition

A **subspace code** (of length n) is a nonempty collection $\mathcal{C}$ of $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^n}$. Its minimum distance is

$$d_S(\mathcal{C}) = \min\{d_S(\mathcal{U}, \mathcal{V}) \mid \mathcal{U}, \mathcal{V} \in \mathcal{C},\ \mathcal{U} \neq \mathcal{V}\}.$$

If every element in a subspace code has the same dimension

constant dimension code.

Subspace codes

Metric space

Given two $\mathbb{F}_q$-subspaces $\mathcal{U}, \mathcal{V}$ of $\mathbb{F}_{q^n}$, their subspace distance is

$$d_S(\mathcal{U}, \mathcal{V}) = \dim_q(\mathcal{U} + \mathcal{V}) - \dim_q(\mathcal{U} \cap \mathcal{V}).$$

Definition

A **subspace code** (of length n) is a nonempty collection $\mathcal{C}$ of $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^n}$. Its minimum distance is

$$d_S(\mathcal{C}) = \min\{d_S(\mathcal{U}, \mathcal{V}) \mid \mathcal{U}, \mathcal{V} \in \mathcal{C},\ \mathcal{U} \neq \mathcal{V}\}.$$

If every element in a subspace code has the same dimension

constant dimension code.

Cyclic orbit codes

Group action

Given an $\mathbb{F}_q$-subspace $\mathcal{U}$ of $\mathbb{F}_{q^n}$ with $\dim_q(\mathcal{U}) = k$,

- and $\beta \in \mathbb{F}_{q^n}^*$, then

$$\mathcal{U} \cdot \beta = \{u\beta \mid u \in \mathcal{U}\}$$

is an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$ of dimension $\dim_q(\mathcal{U} \cdot \beta) = \dim_q(\mathcal{U}) = k$.

- For every $\beta \in \mathbb{F}_{q^n}^*$, the β-cyclic orbit code generated by $\mathcal{U}$ is

$$\mathrm{Orb}_\beta(\mathcal{U}) = \{\mathcal{U} \cdot \beta^i \mid 0 \leqslant i \leqslant |\beta| - 1\}.$$

- If $\langle \beta \rangle = \mathbb{F}_{q^n}^*$: cyclic orbit code generated by $\mathcal{U}$, $\mathrm{Orb}(\mathcal{U})$.

Cyclic orbit codes

Group action

Given an $\mathbb{F}_q$-subspace $\mathcal{U}$ of $\mathbb{F}_{q^n}$ with $\dim_q(\mathcal{U}) = k$,

- and $\beta \in \mathbb{F}_{q^n}^*$, then

$$\mathcal{U} \cdot \beta = \{u\beta \mid u \in \mathcal{U}\}$$

is an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$ of dimension $\dim_q(\mathcal{U} \cdot \beta) = \dim_q(\mathcal{U}) = k$.

- For every $\beta \in \mathbb{F}_{q^n}^*$, the β-cyclic orbit code generated by $\mathcal{U}$ is

$$\mathrm{Orb}_\beta(\mathcal{U}) = \{\mathcal{U} \cdot \beta^i \mid 0 \leqslant i \leqslant |\beta| - 1\}.$$

- If $\langle \beta \rangle = \mathbb{F}_{q^n}^*$: cyclic orbit code generated by $\mathcal{U}$, $\mathrm{Orb}(\mathcal{U})$.

Parameters of a cyclic orbit code

- The orbit $\mathrm{Orb}_\beta(\mathcal{U})$ has associated:

$$\mathrm{Stab}_\beta(\mathcal{U}) = \{\beta^i \mid \mathcal{U}\cdot\beta^i = \mathcal{U}\} \subseteq \langle\beta\rangle$$

and it holds

$$|\mathrm{Orb}_\beta(\mathcal{U})| = \frac{|\beta|}{|\mathrm{Stab}_\beta(\mathcal{U})|}.$$

- The minimum distance is

$$d_S(\mathrm{Orb}_\beta(\mathcal{U})) = \min\{d_S(\mathcal{U}, \mathcal{U}\cdot\beta^i) \mid \beta^i \notin \mathrm{Stab}_\beta(\mathcal{U})\}$$

is an even integer between 0 and $\min\{2k, 2(n-k)\}$.

For every divisor k of n, the code $\mathrm{Orb}(\mathbb{F}_{q^k})$ is a k-spread of $\mathbb{F}_{q^n}$.

Best friend of a subspace

Definition

Let $\mathcal{U}$ be an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$. A subfield $\mathbb{F}_{q^m}$ of $\mathbb{F}_{q^n}$ is a friend of $\mathcal{U}$ if $\mathcal{U}$ is an $\mathbb{F}_{q^m}$-vector space. The largest friend of $\mathcal{U}$ is called its best friend.

Let $\mathcal{U}$ be a subspace of $\mathbb{F}_{q^n}$ with $\mathbb{F}_{q^m}$ as its best friend, then:

- m divides $k = \dim_q(\mathcal{U}) = m \dim_{q^m}(\mathcal{U})$.
- $\mathrm{Stab}_\beta(\mathcal{U}) = \langle\beta\rangle \cap \mathbb{F}_{q^m}^*$
- and $2m$ divides $d_S(\mathrm{Orb}_\beta(\mathcal{U}))$, $\forall \beta \in \mathbb{F}_{q^n}^*$.

Best friend of a subspace

Definition

Let $\mathcal{U}$ be an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$. A subfield $\mathbb{F}_{q^m}$ of $\mathbb{F}_{q^n}$ is a friend of $\mathcal{U}$ if $\mathcal{U}$ is an $\mathbb{F}_{q^m}$-vector space. The largest friend of $\mathcal{U}$ is called its best friend.

Let $\mathcal{U}$ be a subspace of $\mathbb{F}_{q^n}$ with $\mathbb{F}_{q^m}$ as its best friend, then:

- m divides $k = \dim_q(\mathcal{U}) = m \dim_{q^m}(\mathcal{U})$.
- $\mathrm{Stab}_\beta(\mathcal{U}) = \langle\beta\rangle \cap \mathbb{F}_{q^m}^*$
- and $2m$ divides $d_S(\mathrm{Orb}_\beta(\mathcal{U}))$, $\forall \beta \in \mathbb{F}_{q^n}^*$.

Outline

Flags

Definition

A **flag** of length r on $\mathbb{F}_{q^n}$ is a sequence

$$\mathcal{F} = (\mathcal{F}_1, \dots, \mathcal{F}_r)$$

of $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^n}$ satisfying

$$\{0\} \subsetneq \mathcal{F}_1 \subsetneq \mathcal{F}_2 \subsetneq \cdots \subsetneq \mathcal{F}_r \subsetneq \mathbb{F}_{q^n}.$$

The increasing sequence of dimensions

$$(\dim_q(\mathcal{F}_1), \dots, \dim_q(\mathcal{F}_r))$$

is called the type of $\mathcal{F}$.

Flags

Let $\mathcal{F}, \mathcal{F}'$ be flags of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_{q^n}$. Their flag distance is

$$d_f(\mathcal{F}, \mathcal{F}') = \sum_{i=1}^{r} d_S(\mathcal{F}_i, \mathcal{F}'_i).$$

Definition

A flag code of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_{q^n}$ is a nonempty set of flags of this type and its minimum (flag) distance is

$$d_f(\mathcal{C}) = \min\{d_f(\mathcal{F}, \mathcal{F}') \mid \mathcal{F}, \mathcal{F}' \in \mathcal{C},\ \mathcal{F} \neq \mathcal{F}'\}.$$

Projected codes

Definition

Given a flag code $\mathcal{C}$ of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_{q^n}$. For every $1 \leqslant i \leqslant r$, its i-th projected code is the constant dimension code of dimension t_i:

$$\mathcal{C}_i = \{\mathcal{F}_i \mid \mathcal{F} \in \mathcal{C}\}.$$

Cyclic orbit codes

Group action

Given a flag $\mathcal{F} = (\mathcal{F}_1, \dots, \mathcal{F}_r)$ of type $(t_1, \dots, t_r)$ on $\mathbb{F}_{q^n}$

- If $\beta \in \mathbb{F}_{q^n}^*$, then

$$\mathcal{F} \cdot \beta = (\mathcal{F}_1 \cdot \beta, \dots, \mathcal{F}_r \cdot \beta)$$

is a flag of the same type.

Definition

Given a flag $\mathcal{F}$ on $\mathbb{F}_{q^n}$ and $\beta \in \mathbb{F}_{q^n}^*$, the β-cyclic orbit **flag** code generated by $\mathcal{F}$ is

$$\mathrm{Orb}_\beta(\mathcal{F}) = \{\mathcal{F} \cdot \beta^i \mid 0 \leqslant i \leqslant |\beta| - 1\}.$$

In case $\langle \beta \rangle = \mathbb{F}_{q^n}^* \rightarrow$ cyclic orbit flag code $\mathrm{Orb}(\mathcal{F})$.

Projected codes

Remark:

Let $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ be a flag on $\mathbb{F}_{q^n}$ and $\beta \in \mathbb{F}_{q^n}^*$, then

$$(\mathrm{Orb}_\beta(\mathcal{F}))_i = \mathrm{Orb}_\beta(\mathcal{F}_i).$$

$$\Downarrow$$

Information about cyclic orbit flag codes in terms of cyclic orbit (subspace) codes.

Parameters of a cyclic orbit flag code

Let $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ be a flag of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_q^n$:

- The code $\mathrm{Orb}_\beta(\mathcal{F})$ has associated:

$$\mathrm{Stab}_\beta(\mathcal{F}) = \{\beta^i \mid \mathcal{F} \cdot \beta^i = \mathcal{F}\} \subseteq \langle \beta \rangle$$

and it holds

$$\mathrm{Stab}_\beta(\mathcal{F}) = \bigcap_{i=1}^{r} \mathrm{Stab}_\beta(\mathcal{F}_i).$$

The best friend of a flag

Definition

A subfield $\mathbb{F}_{q^m}$ of $\mathbb{F}_{q^n}$ is said to be a friend of $\mathcal{F}$ if it is a friend of all its subspaces. The largest friend of $\mathcal{F}$ is called its best friend.

Theorem (Alonso-González, Navarro-Pérez, 2021)

Let $\mathcal{F}$ be a flag on $\mathbb{F}_{q^n}$. Its best friend is the intersection of the best friends of its subspaces. Moreover, if $\mathbb{F}_{q^m}$ is the best friend of $\mathcal{F}$, then

$$|\mathrm{Orb}_\beta(\mathcal{F})| = \frac{|\beta|}{|\langle\beta\rangle \cap \mathbb{F}_{q^m}^*|}.$$

The best friend of a flag

Let $\mathcal{F}$ be a flag of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_{q^n}$ with $\mathbb{F}_{q^m}$ as its best friend, then:

- m divides $\gcd(t_1, \ldots, t_r, n)$.
- $2m$ divides the minimum distance of $\mathrm{Orb}_\beta(\mathcal{F})$.

In particular,

$$2m \leqslant d_f(\mathrm{Orb}_\beta(\mathcal{F})) \leqslant 2 \left(\sum_{t_i \leqslant n/2} t_i + \sum_{t_i > n/2} (n - t_i) \right).$$

Outline

Optimum distance flag codes

Theorem (Alonso-González, Navarro-Pérez, 2021)

Let $\mathcal{F}$ be a flag on $\mathbb{F}_{q^n}$ with $\mathbb{F}_{q^m}$ as its best friend. The orbit $\mathrm{Orb}(\mathcal{F})$ is an ODFC if, and only if, its type vector is one of the following ones:

- (m),
- $(n-m)$ or
- $(m, n-m)$.

Optimum distance flag codes

Theorem (Alonso-González, Navarro-Pérez, 2021)

Let $\mathcal{F}$ be a flag on $\mathbb{F}_{q^n}$ with $\mathbb{F}_{q^m}$ as its best friend and consider $\beta \in \mathbb{F}_{q^n}^* = \langle \alpha \rangle$. Write $\langle \beta \rangle = \langle \alpha^\ell \rangle$, for some divisor ℓ of $q^n - 1$. If $\mathrm{Orb}_\beta(\mathcal{F})$ is and ODFC, then for every dimension t in the type vector, it is satisfied:

$$\frac{\mathrm{lcm}\left(\ell, \frac{q^n-1}{q^m-1}\right)}{\ell} \leqslant \begin{cases} \left\lfloor \frac{q^n-1}{q^t-1} \right\rfloor & \text{if} \quad 2t \leqslant n, \\ \left\lfloor \frac{q^n-1}{q^{n-t}-1} \right\rfloor & \text{if} \quad 2t > n. \end{cases}$$

Optimum distance flag codes

On $\mathbb{F}_{2^{12}}$ and with $\mathbb{F}_{2^2}$ as best friend...

β	$\lvert\beta\rvert$	$\langle\beta\rangle \cap \mathbb{F}_{q^m}^*$	$\lvert\mathrm{Orb}_\beta(\mathcal{F})\rvert$	Allowed dimensions	Max. distance
α	4095	$\mathbb{F}_{2^2}^*$	1365	2, 10	8
α^5	819	$\mathbb{F}_{2^2}^*$	273	2, 4, 8, 10	24
α^9	455	$\{1\}$	455	2, 10	8
α^{13}	315	$\mathbb{F}_{2^2}^*$	105	2, 4, 8, 10	24
α^{39}	105	$\mathbb{F}_{2^2}^*$	35	2, 4, 6, 8, 10	36
α^{45}	91	$\{1\}$	91	2, 4, 8, 10	24
α^{63}	65	$\{1\}$	65	2, 4, 6, 8, 10	36

Table: Values for $q = 2$, $n = 12$, $m = 2$.

Galois cyclic orbit flag codes

Definition

Let $t_1, \ldots, t_r$ be a sequence of divisors of n such that t_i divides t_{i+1}, for $1 \leqslant i \leqslant r-1$. The sequence of nested subfields

$$\mathcal{F} = (\mathbb{F}_{q^{t_1}}, \ldots, \mathbb{F}_{q^{t_r}})$$

is the Galois flag of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_{q^n}$.
For every $\beta \in \mathbb{F}_{q^n}^*$, the code

$$\mathrm{Orb}_\beta((\mathbb{F}_{q^{t_1}}, \ldots, \mathbb{F}_{q^{t_r}}))$$

is the Galois β-cyclic flag code of type $(t_1, \ldots, t_r)$.

Galois cyclic orbit flag codes

Definition

Let $t_1, \ldots, t_r$ be a sequence of divisors of n such that t_i divides t_{i+1}, for $1 \leqslant i \leqslant r-1$. The sequence of nested subfields

$$\mathcal{F} = (\mathbb{F}_{q^{t_1}}, \ldots, \mathbb{F}_{q^{t_r}})$$

is the Galois flag of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_{q^n}$.
For every $\beta \in \mathbb{F}_{q^n}^*$, the code

$$\mathrm{Orb}_\beta((\mathbb{F}_{q^{t_1}}, \ldots, \mathbb{F}_{q^{t_r}}))$$

is the Galois β-cyclic flag code of type $(t_1, \ldots, t_r)$.

Galois cyclic orbit flag codes

Let $\mathcal{F} = (\mathbb{F}_{q^{t_1}}, \ldots, \mathbb{F}_{q^{t_r}})$, then:

- every subspace $\mathcal{F}_i = \mathbb{F}_{q^{t_i}}$ is its own best friend and
- $\mathcal{F}_1 = \mathbb{F}_{q^{t_1}}$ is the best friend of the flag.
- The i-th projected code of $\mathrm{Orb}_\beta(\mathcal{F})$ is the (partial) t_i-spread $\mathrm{Orb}_\beta(\mathbb{F}_{q^{t_i}})$.

Moreover:

$$\mathrm{Stab}_\beta(\mathcal{F}) = \mathrm{Stab}_\beta(\mathbb{F}_{q^{t_1}}) \subseteq \mathrm{Stab}_\beta(\mathbb{F}_{q^{t_2}}) \subseteq \cdots \subseteq \mathrm{Stab}_\beta(\mathbb{F}_{q^{t_r}}) \subseteq \langle \beta \rangle.$$

Galois cyclic orbit flag codes

Theorem (Alonso-González, Navarro-Pérez, 2021)

Let $\mathcal{F}$ be the Galois flag of type $(t_1, \dots, t_r)$ on $\mathbb{F}_{q^n}$ and take $\beta \in \mathbb{F}_{q^n}^*$. Then

$$d_f(\mathrm{Orb}_\beta(\mathcal{F})) \in \{2t_1, 2(t_1 + t_2), \dots, 2(t_1 + \cdots + t_r)\}.$$

Moreover,

$$\text{Subgroups of } \mathbb{F}_{q^n}^* \;\leftrightarrow\; \text{distance values.}$$

Galois cyclic orbit flag codes

- $q = 2$, $n = 16$ and type $(2, 4, 8)$:

$$\mathcal{F} = (\mathbb{F}_{2^2}, \mathbb{F}_{2^4}, \mathbb{F}_{2^8})$$

- Possible values for the distance: $\{4, 12, 28\}$ and:

β	$\lvert\beta\rvert$	$\lvert\mathrm{Orb}_\beta(\mathcal{F})\rvert$	d_β
α	65535	21845	4
α^5	13107	4369	12
α^{17}	3855	1285	4
α^{85}	771	257	28
α^{257}	255	85	4
α^{1285}	51	17	12
α^{4369}	15	5	4

where $\langle \alpha \rangle = \mathbb{F}^*_{2^{16}}$.

Generalized Galois flag codes

Definition

A flag $\mathcal{F}$ on $\mathbb{F}_{q^n}$ is said to be a generalized Galois flag if:

1. it contains subfields among its subspaces,
2. but not all its subspaces are subfields of $\mathbb{F}_{q^n}$.

Example

Consider a flag of type $(2, 3, 4)$ on $\mathbb{F}_{q^8}$ of the form

$$\mathcal{F} = (\mathbb{F}_{q^2}, \mathcal{U}, \mathbb{F}_{q^4}).$$

- The subspace $\mathcal{U}$ cannot be a subfield.
- The sequence of best friends is $(\mathbb{F}_{q^2}, \mathbb{F}_q, \mathbb{F}_{q^4})$.
- The best friend of $\mathcal{F}$ is $\mathbb{F}_q$.

Generalized Galois flag codes

The presence of subfields (partial spreads)

$\Downarrow$

set of potential values for the distance

Open question

subgroups of $\mathbb{F}_{q^n}^*$ $\not\leftrightarrow$ distance values

Universitat d'Alacant
Universidad de Alicante

EDEM
Escuela de Empresarios

Coding theory and cryptography

A conference in the honor of Joachim Rosenthal's 60th birthday

Cyclic Orbit Flag Codes

Miguel Ángel Navarro-Pérez

Joint work with Clementa Alonso-González

July 15, 2022

mnavarro@edem.es