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

1. Cyclic orbit subspace codes
2. Cyclic orbit flag codes and their best friend
3. Flag codes with prescribed best friend
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, it is a constant dimension code.
Subspace codes

Metric space

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

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

Definition

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

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

If every element in a subspace code has the same dimension the code is called a **constant dimension code**.
Subspace codes

Metric space

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

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

Definition

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

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

If every element in a subspace code has the same dimension, it is a **constant dimension code**.
Subspace codes

Metric space

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

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

Definition

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

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

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 $\text{dim}_q(\mathcal{U}) = k$,

- and $\beta \in \mathbb{F}_q^*$, 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 $\text{dim}_q(\mathcal{U} \cdot \beta) = \text{dim}_q(\mathcal{U}) = k$.

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

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

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

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 $\beta$-cyclic orbit code generated by $\mathcal{U}$ is

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

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

Miguel Ángel Navarro-Pérez
Parameters of a cyclic orbit code

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

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

and it holds

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

- The minimum distance is

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

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

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

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

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

and it holds

$$|\text{Orb}_\beta(U)| = \frac{|\beta|}{|\text{Stab}_\beta(U)|}.$$
Best friend of a subspace

Definition

Let $U$ 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 $U$ if $U$ is an $\mathbb{F}_{q^m}$-vector space. The largest friend of $U$ is called its best friend.

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

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

Cyclic orbit flag codes and their best friend

Flag codes with prescribed best friend
A **flag** of length $r$ on $\mathbb{F}_{q^n}$ is a sequence

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

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

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

The increasing sequence of dimensions

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

is called the **type** of $\mathcal{F}$.
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 $C$ of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_q^n$. For every $1 \leq i \leq r$, its $i$-th projected code is the constant dimension code of dimension $t_i$:

$$C_i = \{ \mathcal{F}_i \mid \mathcal{F} \in C \}.$$
Cyclic orbit codes

Group action
Given a flag $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_{q^n}$
- If $\beta \in \mathbb{F}_{q^n}^*$, then
  $$\mathcal{F} \cdot \beta = (\mathcal{F}_1 \cdot \beta, \ldots, \mathcal{F}_r \cdot \beta)$$
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 $\beta$-cyclic orbit flag code generated by $\mathcal{F}$ is
$$\text{Orb}_\beta(\mathcal{F}) = \{ \mathcal{F} \cdot \beta^i \mid 0 \leq i \leq |\beta| - 1 \}.$$In case $\langle \beta \rangle = \mathbb{F}_{q^n}^* \rightarrow$ cyclic orbit flag code $\text{Orb}(\mathcal{F})$. 
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

$$(\text{Orb}_\beta(\mathcal{F}))[i] = \text{Orb}_\beta(\mathcal{F}_i).$$

Information about cyclic orbit flag codes in terms of cyclic orbit (subspace) codes.
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 $\text{Orb}_\beta(\mathcal{F})$ has associated:

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

and it holds

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

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

In particular,

$$2m \leq d_f(\text{Orb}_\beta(\mathcal{F})) \leq 2 \left( \sum_{t_i \leq n/2} t_i + \sum_{t_i > n/2} (n - t_i) \right).$$
Cyclic orbit subspace codes

Cyclic orbit flag codes and their best friend

Flag codes with prescribed best friend
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 $\text{Orb}(\mathcal{F})$ is an ODFC if, and only if, its type vector is one of the following ones:

- $(m)$,
- $(n-m)$ or
- $(m, n-m)$.
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 $\ell$ of $q^n - 1$. If $\text{Orb}_\beta(\mathcal{F})$ is an ODFC, then for every dimension $t$ in the type vector, it is satisfied:

$$\frac{\text{lcm}(\ell, q^n - 1)}{\ell} \leq \begin{cases} 
\left\lfloor \frac{q^n - 1}{q^t - 1} \right\rfloor & \text{if } 2t \leq n, \\
\left\lfloor \frac{q^n - 1}{q^{n-t} - 1} \right\rfloor & \text{if } 2t > n.
\end{cases}$$
On $\mathbb{F}_{2^{12}}$ and with $\mathbb{F}_{2^2}$ as best friend...

| $\beta$ | $|\beta|$ | $\langle\beta\rangle \cap \mathbb{F}^*_m$ | $|\text{Orb}_\beta(\mathcal{F})|$ | Allowed dimensions | Max. distance |
|---------|-----------|-----------------|-----------------|-------------------|--------------|
| $\alpha$ | 4095 | $\mathbb{F}^*_{2^2}$ | 1365 | 2, 10 | 8 |
| $\alpha^5$ | 819 | $\mathbb{F}^*_{2^2}$ | 273 | 2, 4, 8, 10 | 24 |
| $\alpha^9$ | 455 | $\{1\}$ | 455 | 2, 10 | 8 |
| $\alpha^{13}$ | 315 | $\mathbb{F}^*_2$ | 105 | 2, 4, 8, 10 | 24 |
| $\alpha^{39}$ | 105 | $\mathbb{F}^*_2$ | 35 | 2, 4, 6, 8, 10 | 36 |
| $\alpha^{45}$ | 91 | $\{1\}$ | 91 | 2, 4, 8, 10 | 24 |
| $\alpha^{63}$ | 65 | $\{1\}$ | 65 | 2, 4, 6, 8, 10 | 36 |

Table: Values for $q = 2$, $n = 12$, $m = 2$. 
Cyclic orbit subspace codes

Cyclic orbit flag codes and their best friend

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 $1 \leq i \leq r - 1$. 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 $\beta \in \mathbb{F}_q^*$, the code

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

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

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

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

is the Galois $\beta$-cyclic flag code of type $(t_1, \ldots, t_r)$. 
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 $\text{Orb}_\beta(\mathcal{F})$ is the (partial) $t_i$-spread $\text{Orb}_\beta(\mathbb{F}_{q^{t_i}})$.

Moreover:

$$\text{Stab}_\beta(\mathcal{F}) = \text{Stab}_\beta(\mathbb{F}_{q^{t_1}}) \subseteq \text{Stab}_\beta(\mathbb{F}_{q^{t_2}}) \subseteq \cdots \subseteq \text{Stab}_\beta(\mathbb{F}_{q^{t_r}}) \subseteq \langle \beta \rangle.$$
Theorem (Alonso-González, Navarro-Pérez, 2021)

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

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

Moreover,

Subgroups of $\mathbb{F}_{q^n}^*$ $\leftrightarrow$ 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:

| $\beta$   | $|\beta|$ | $|\text{Orb}_\beta(\mathcal{F})|$ | $d_\beta$ |
|-----------|-----------|-------------------------------|-----------|
| $\alpha$  | 65535     | 21845                         | 4         |
| $\alpha^5$| 13107     | 4369                          | 12        |
| $\alpha^{17}$ | 3855     | 1285                          | 4         |
| $\alpha^{85}$ | 771       | 257                           | 28        |
| $\alpha^{257}$ | 255      | 85                            | 4         |
| $\alpha^{1285}$ | 51       | 17                            | 12        |
| $\alpha^{4369}$ | 15       | 5                             | 4         |

where $\langle \alpha \rangle = \mathbb{F}_2^{*16}$. 
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 $\mathbb{F}_q$. 

Miguel Ángel Navarro-Pérez
The presence of subfields (partial spreads)

set of potential values for the distance

Open question

subgroups of $\mathbb{F}_{q^n}^*$ $\leftrightarrow$ distance values
Cyclic Orbit Flag Codes

Miguel Ángel Navarro-Pérez

Joint work with Clementa Alonso-González

July 15, 2022