Equidistant Single-Orbit Cyclic Subspace Codes

by

Mahak

Ph.D. student

Department of Mathematics
Indian Institute of Technology Roorkee, India

work done with Maheshanand Bhaintwal

June 20, 2024

Outline

- Subspace codes
- Orbit codes
- Equidistant single-orbit cyclic subspace Codes
- Sunflower single-orbit cyclic subspace codes

Definition (Subspace code)

Let $\mathcal{P}_q(n)$ denote the set of all the subspaces of $\mathbb{F}_q^n$. A *subspace code* is a non-empty collection $C \subseteq \mathcal{P}_q(n)$ with minimum distance

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

- The distance d_s used here is the subspace distance and is defined by

$$d_s(U, V) = \dim(U) + \dim(V) - 2\dim(U \cap V) .$$

- If every subspace in code C is of the same dimension, say k, then

$$d(C) = 2k - \max_{U,V \in C, U \neq V} \dim(U \cap V) .$$

- It is well-known that $\mathbb{F}_{q^n}$ is isomorphic to $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$. Due to rich algebraic structure of $\mathbb{F}_{q^n}$ compared to $\mathbb{F}_q^n$, we identify the subspaces of $\mathbb{F}_q^n$ with that of $\mathbb{F}_{q^n}$.
- For $\alpha \in \mathbb{F}_{q^n}^*$ and $U \in \mathcal{P}_q(n)$, the *cyclic shift* of U is defined as

$$\alpha U = \{\alpha u \mid u \in U\} .$$

Orbit Codes

- We can define a group action $\mathbb{F}_{q^n}^* \times \mathcal{P}_q(n) \to \mathcal{P}_q(n)$ of $\mathbb{F}_{q^n}^*$ on $\mathcal{P}_q(n)$ as

$$(\alpha, U) \quad \to \quad \alpha U \,.$$

For any $\mathbb{F}_q$-subspace $U \subseteq \mathbb{F}_q^n$, the *orbit of U*, denoted by $\mathrm{Orb}(U)$, is defined by

$$\mathrm{Orb}(U) = \{\alpha U \mid \alpha \in \mathbb{F}_{q^n}^*\} \,.$$

- The *stabilizer* of U, denoted by $\mathrm{Stab}(U)$, is defined by

$$\mathrm{Stab}(U) = \{\alpha \in \mathbb{F}_{q^n}^* \mid \alpha U = U\} \,.$$

$\mathrm{Stab}(U) \cup \{0\} = \mathbb{F}_{q^t}$ for some t which is a divisor of $\gcd(\dim_{\mathbb{F}_q}(U), n)$.

Orbit Codes

- We can define a group action $\mathbb{F}_{q^n}^* \times \mathcal{P}_q(n) \to \mathcal{P}_q(n)$ of $\mathbb{F}_{q^n}^*$ on $\mathcal{P}_q(n)$ as

$$(\alpha, U) \quad \to \quad \alpha U \, .$$

For any $\mathbb{F}_q$-subspace $U \subseteq \mathbb{F}_q^n$, the *orbit of U*, denoted by $\mathrm{Orb}(U)$, is defined by

$$\mathrm{Orb}(U) = \{\alpha U \mid \alpha \in \mathbb{F}_{q^n}^*\} \, .$$

- The *stabilizer* of U, denoted by $\mathrm{Stab}(U)$, is defined by

$$\mathrm{Stab}(U) = \{\alpha \in \mathbb{F}_{q^n}^* \mid \alpha U = U\} \, .$$

$\mathrm{Stab}(U) \cup \{0\} = \mathbb{F}_{q^t}$ for some t which is a divisor of $\gcd(\dim_{\mathbb{F}_q}(U), n)$.

- Using the orbit-stabilizer theorem, for any subspace U of $\mathbb{F}_q^n$, we have

$$|\mathrm{Orb}(U)| = \frac{q^n - 1}{|\mathrm{Stab}(U)|} = \frac{q^n - 1}{q^t - 1} \, .$$

- If $\mathrm{Stab}(U) = \mathbb{F}_q^*$, i.e., $|\mathrm{Orb}(U)| = \frac{q^n-1}{q-1}$, then $\mathrm{Orb}(U)$ is called a *full-length orbit code* and we say that U generates a full-length orbit. Otherwise, $\mathrm{Orb}(U)$ is a degenerate orbit.

Orbit Codes

A subspace code C is said to be a *cyclic subspace code* if $\alpha U \in C$ for all $\alpha \in \mathbb{F}_{q^n}^*$ and $U \in C$.

Definition

Fix an element $\beta \in \mathbb{F}_{q^n}^* \backslash \{1\}$. Let U be an $\mathbb{F}_q$-subspace in $\mathbb{F}_{q^n}$. The *β-cyclic orbit code* generated by U is defined as the set

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

If β is a primitive element of $\mathbb{F}_{q^n}$, we write $\mathrm{Orb}_\beta(U)$ simply as $\mathrm{Orb}(U)$ and call it a *single-orbit cyclic subspace code.* Otherwise, it is termed a *single-orbit quasi-cyclic subspace code.*

A subspace code C is said to be a *cyclic subspace code* if $\alpha U \in C$ for all $\alpha \in \mathbb{F}_{q^n}^*$ and $U \in C$.

Definition

Fix an element $\beta \in \mathbb{F}_{q^n}^* \backslash \{1\}$. Let U be an $\mathbb{F}_q$-subspace in $\mathbb{F}_{q^n}$. The *β-cyclic orbit code* generated by U is defined as the set

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

If β is a primitive element of $\mathbb{F}_{q^n}$, we write $\mathrm{Orb}_\beta(U)$ simply as $\mathrm{Orb}(U)$ and call it a *single-orbit cyclic subspace code.* Otherwise, it is termed a *single-orbit quasi-cyclic subspace code.*

Definition (Equidistant code)

A β-cyclic orbit code $\mathrm{Orb}_\beta(U)$ is an equidistant code if for all $\beta^i U$, $\beta^j U \in \mathrm{Orb}_\beta(U)$, $\beta^i U \neq \beta^j U$

$$d_s(\beta^i U, \beta^j U) = d(\mathrm{Orb}_\beta(U)) .$$

Equidistant Codes

- Since, $\dim(\beta^i U \cap \beta^j U) = \dim(U \cap \beta^{j-i} U)$, the minimum distance of an orbit code is given by

  $$d_s(\mathrm{Orb}(U)) = 2\dim(U) - \max\{\dim(U \cap \beta^i U) \mid 0 \le i \le |\beta| - 1,\ U \ne \beta^i U\}\ .$$

- If for all i, $1 \le i \le |\beta| - 1$, $U \ne \beta^i U$, $\dim(U \cap \beta^i U) = c$, for some non-negative integer c then $\mathrm{Orb}_\beta(U)$ is said to be a *c-intersecting equidistant code*.

- Since, $\dim(\beta^i U \cap \beta^j U) = \dim(U \cap \beta^{j-i} U)$, the minimum distance of an orbit code is given by

$$d_s(\mathrm{Orb}(U)) = 2\dim(U) - \max\{\dim(U \cap \beta^i U) \mid 0 \leq i \leq |\beta|-1,\ U \neq \beta^i U\}\ .$$

- If for all i, $1 \leq i \leq |\beta| - 1$, $U \neq \beta^i U$, $\dim(U \cap \beta^i U) = c$, for some non-negative integer c then $\mathrm{Orb}_\beta(U)$ is said to be a *c-intersecting equidistant code*.

Definition (Sunflower)

A β-cyclic orbit code $\mathrm{Orb}_\beta(U)$ is a *sunflower* if there exists a subspace T in $\mathbb{F}_{q^n}$ such that for all $\beta^i U, \beta^j U \in \mathrm{Orb}_\beta(U)$, $\beta^i U \neq \beta^j U$ we have $\beta^i U \cap \beta^j U = T$.

- The subspace T is called the center of the sunflower $\mathrm{Orb}_\beta(U)$.
- Note that for an equidistant code $\mathrm{Orb}_\beta(U)$ if there exists a subspace S in $\mathbb{F}_{q^n}$ such that $U \cap \beta^i U = S$ for all $\beta^i U \in \mathrm{Orb}_\beta(U)$ with $\beta^i U \neq U$ then $\mathrm{Orb}_\beta(U)$ is a sunflower.

Definition (Difference set)

Suppose $(G, +)$ is a finite group of order v in which the identity element is denoted by "0". Let k and λ be positive integers such that $2 \leq k < v$. A (v, k, λ)-difference set in $(G, +)$ is a subset $D \subseteq G$ that satisfies the following properties:

1. $|D| = k$,
2. the multiset $[x - y : x, y \in D, x \neq y]$ contains every element in $G \backslash \{0\}$ exactly λ times.

- Note that if a (v, k, λ)-difference set exists,

$$\lambda(v - 1) = k(k - 1) ,$$

- Let D be a (v, k, λ)-difference set in a group $(G, +)$. For any $g \in G$, define

$$D + g = \{x + g : x \in D\} .$$

  Any set $D + g$ is called a translate of D.

Difference sets

Lemma

Let G be a group of order v and $D \subseteq G$ with $|D| = k$. If for every $0 \neq g \in G$, $|D \cap (D + g)| = \lambda$ $(\lambda > 0)$ then D is a (v, k, λ)-difference set in G.

Lemma

Let G be a group of order v and $D \subseteq G$ with $|D| = k$. If for every $0 \neq g \in G$, $|D \cap (D + g)| = \lambda$ $(\lambda > 0)$ then D is a (v, k, λ)-difference set in G.

Definition (Relative difference set)

Let $(G, +)$ be a group of order nm and let $(N, +)$ be a subgroup of G of order n. Then a k-subset D of G is called a *relative difference set* with parameters n, m, k, λ_1 and λ_2 (relative to N) or briefly an $(n, m, k, \lambda_1, \lambda_2)$-RDS, provided that the list of differences $\{d_1 - d_2 : d_1, d_2 \in D, d_1 \neq d_2\}$ contain each element of N, except zero, precisely λ_1 times and each element of $G \backslash N$ exactly λ_2 times.

- Let D be an $(n, m, k, \lambda_1, \lambda_2)$-RDS in G. Then

$$k(k-1) = n(m-1)\lambda_2 + (n-1)\lambda_1 \ .$$

Equidistant Codes

The code Orb(U) is trivially an equidistant code in the following cases:-

1. $\dim(U) = 1$ (Orb(U) is a 0-intersecting equidistant code.)
2. $\dim(U) = n - 1$ (($n - 2$)-intersecting)
3. if U is a cyclic shift of a subfield of $\mathbb{F}_{q^n}$, i.e., $U = \gamma\mathbb{F}_{q^t}$, where $\gamma \in \mathbb{F}_{q^n}^*$ and t is a divisor of n (0-intersecting)

For a subspace U of dimension k in $\mathbb{F}_{q^n}$, $d_s(\text{Orb}(U)) = 2k$ if and only if $U = \beta\mathbb{F}_{q^k}$, for some $\beta \in \mathbb{F}_{q^n}^*$.

Equidistant Codes

The code $\mathrm{Orb}(U)$ is trivially an equidistant code in the following cases:-

1. $\dim(U) = 1$ ($\mathrm{Orb}(U)$ is a 0-intersecting equidistant code.)
2. $\dim(U) = n - 1$ ($(n-2)$-intersecting)
3. if U is a cyclic shift of a subfield of $\mathbb{F}_{q^n}$, i.e., $U = \gamma\mathbb{F}_{q^t}$, where $\gamma \in \mathbb{F}_{q^n}^*$ and t is a divisor of n (0-intersecting)

For a subspace U of dimension k in $\mathbb{F}_{q^n}$, $d_s(\mathrm{Orb}(U)) = 2k$ if and only if $U = \beta\mathbb{F}_{q^k}$, for some $\beta \in \mathbb{F}_{q^n}^*$.

- Consider an extension field $\mathbb{F}_{q^n}$. Let α be a primitive element of $\mathbb{F}_{q^n}$. Then $\mathbb{F}_{q^n}^* = \{\alpha^i \mid i = 0, 1, \ldots, q^n - 2\}$.
- Now consider the group $\mathbb{Z}_{q^n-1} = \{0, 1, \ldots, q^n - 2\}$ under the operation addition modulo $q^n - 1$.
- Let $G = \{\alpha^0 = 1, \alpha^{j_1}, \alpha^{j_2}, \ldots, \alpha^{j_m}\}$ be a subgroup of the multiplicative group $(\mathbb{F}_{q^n}^*, \times)$.
- Let $I = \{t \mid \alpha^t \in G\}$. Then I is a subgroup in $(\mathbb{Z}_{q^n-1}, \oplus_{q^n-1})$. Similarly, for a subgroup in $(\mathbb{Z}_{q^n-1}, \oplus_{q^n-1})$ there is a subgroup in $(\mathbb{F}_{q^n}^*, \times)$.

Contd..

Theorem

Let α be a primitive element of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Let $U = \{0, \alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_{2^k-1}}\}$ be a subspace of dimension k in $\mathbb{F}_{2^n}$ such that U generates a full-length orbit. The subspace code Orb(U) is an r-intersecting equidistant code $(r > 0)$ if and only if the set of indices i_j, $1 \leq j \leq 2^k - 1$, is a difference set in $\mathbb{Z}_{2^n-1}$.

Contd..

Theorem

Let α be a primitive element of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Let $U = \{0, \alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_{2^k-1}}\}$ be a subspace of dimension k in $\mathbb{F}_{2^n}$ such that U generates a full-length orbit. The subspace code Orb(U) is an r-intersecting equidistant code $(r > 0)$ if and only if the set of indices i_j, $1 \leq j \leq 2^k - 1$, is a difference set in $\mathbb{Z}_{2^n-1}$.

Proof idea:

- Let Orb(U) be an equidistant code and let $d_s(\text{Orb}(U)) = 2(k - r)$, where $r > 0$.
- As U generates a full-length orbit, for all $\beta \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2$, $\dim(U \cap \beta U) = r$.
- Now consider the set $D = \{i_j \mid \alpha^{i_j} \in U\}$. Clearly $D \subseteq \mathbb{Z}_{2^n-1}$ and $|D| = 2^k - 1$.
- Let $j(\neq 0)$ be an arbitrary element in $\mathbb{Z}_{2^n-1}$. Then $\alpha^j \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2$, and $\dim(U \cap \alpha^j U) = r$, i.e.,

$$|\{0, \alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_{2^k-1}}\} \cap \{0, \alpha^{j+i_1}, \alpha^{j+i_2}, \ldots, \alpha^{j+i_{2^k-1}}\}| = 2^r .$$

  From this we get $|D \cap (j + D)| = 2^r - 1$.

Contd..

Proof of Converse:

- Let $D = \{i_j \mid \alpha^{i_j} \in U\}$ constitutes a $(2^n - 1, 2^k - 1, s)$-difference set in $\mathbb{Z}_{2^n-1}$. Then,
$$s(2^n - 2) = (2^k - 1)(2^k - 2) \; .$$
From this we get $s(2^{n-1} - 1) = (2^k - 1)(2^{k-1} - 1)$.
- As $k < n$, we get $s = (2^{k-1} - 1)$. This implies that the multiset $[x - y : x, y \in D, x \neq y]$ contains every element of $\mathbb{Z}_{2^n-1} \backslash \{0\}$ exactly $2^{k-1} - 1$ times.
- Let $\alpha^m U \neq U$ be an arbitrary element in Orb(U). Then $m \in \mathbb{Z}_{2^n-1} \backslash \{0\}$ and $|D \cap (m + D)| = 2^{k-1} - 1$. Therefore, $|U \cap \alpha^m U| = 2^{k-1}$ and $\dim(U \cap \alpha^m U) = k - 1$. Hence Orb($U$) is an equidistant code.

Remark

Let $q > 2$. For $2 \in \mathbb{F}_q$, there exist a $j \in \mathbb{Z}_{q^n-1} \backslash \{0\}$ such that $2 = \alpha^j$. Now, $|D \cap (j + D)| = q^k - 1$. Thus, D is not a difference set in G.

Contd..

Theorem

Let α be a primitive element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Let $U = \{0, \alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_{q^k-1}}\}$ be a subspace in $\mathbb{F}_{q^n}$ of dimension k such that U generates a full-length orbit. If the subspace code Orb(U) is an r-intersecting equidistant code ($r > 0$) then the indices i_j, $1 \leq j \leq q^k - 1$, form a relative difference set in $\mathbb{Z}_{q^n-1}$.

Theorem

Let α be a primitive element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Let $U = \{0, \alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_{q^k-1}}\}$ be a subspace in $\mathbb{F}_{q^n}$ of dimension k such that U generates a full-length orbit. If the subspace code $Orb(U)$ is an r-intersecting equidistant code $(r > 0)$ then the indices i_j, $1 \leq j \leq q^k - 1$, form a relative difference set in $\mathbb{Z}_{q^n-1}$.

Proof idea:

- Let $\mathrm{Orb}(U)$ be an equidistant subspace code, and let $d_s(\mathrm{Orb}(U)) = 2(k - r)$, where $r > 0$.
- Let $D = \{i_j \mid \alpha^{i_j} \in U\}$ and $N = \{j \mid \alpha^j \in \mathbb{F}_q^*\}$. Then N is a subgroup of $\mathbb{Z}_{q^n-1}$ and $|N| = q - 1$.
- For any $i \in \mathbb{Z}_{q^n-1} \backslash N$, $\alpha^i \in \mathbb{F}_{q^n} \backslash \mathbb{F}_q$ and thus $\dim(U \cap \alpha^i U) = r$. From this, we get $|D \cap (i + D)| = q^r - 1$ for all $i \in \mathbb{Z}_{q^n-1} \backslash N$.
- Now for any $t \in N$, $\alpha^t \in \mathbb{F}_q$ and $\dim(U \cap \alpha^t U) = q^k$. Thus, for any $t \in N$, $|D \cap (t + D)| = q^k - 1$. Hence the set of indices D constitutes a $(q - 1, \frac{q^n-1}{q-1}, q^k - 1, q^k - 1, q^r - 1)$ relative difference set in $\mathbb{Z}_{q^n-1}$ (relative to N).

Contd..

Theorem

There is only the trivial equidistant (full length) single-orbit cyclic subspace code in $\mathcal{P}_q(n)$ for $n \geq 3$.

Contd..

Theorem

There is only the trivial equidistant (full length) single-orbit cyclic subspace code in $\mathcal{P}_q(n)$ for $n \geq 3$.

Proof idea:

- Let α be a primitive element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and let $U = \{0, \alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_{q^k-1}}\}$ be a subspace of dimension k in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.
- Let Orb(U) be an equidistant subspace code with subspace distance $2(k-r)$, where $r > 0$. Then the set of indices $\{i_j \mid \alpha^{i_j} \in U\}$ constitutes a $(q-1, \frac{q^n-1}{q-1}, q^k-1, q^k-1, q^r-1)$- relative difference set in $\mathbb{Z}_{q^n-1}$.
- So, we get

$$(q^k-1)(q^k-2) = (q-1)\left(\frac{q^n-1}{q-1} - 1\right)(q^r-1) + (q-2)(q^k-1)\,.$$

- On simplifying the above equation, we get

$$(q^k-1)(q^{k-1}-1) = (q^{n-1}-1)(q^r-1)\,.$$

Contd..

- Further this gives

$$q^{2k-1} - (q+1)q^{k-1} = q^{n+r-1} - q^{n-1} - q^{r} \; . \qquad (1)$$

- Let $r > k-1$. On dividing both sides of equation (1) by q^{k-1}, we get

$$q^{k} - (q+1) = q^{n+r-k} - q^{n-k} - q^{r-k+1} \; .$$

  As $n > k, r-k+1 > 0$, the right side of the above equation is a multiple of q but the left side is not. This is a contradiction.

- Let $r < k-1$. On dividing both sides of equation (1) by q^{r}, we get

$$q^{2k-r-1} - (q+1)q^{k-r-1} = q^{n-1} - q^{n-r-1} - 1 \; .$$

  As $n > k > r+1$, the left side of the above equation is a multiple of q but the right side is not. This is a contradiction.

- So, we conclude that $r = k-1$. By putting the value of $r = k-1$ in (1), we get $k = n-1$. Therefore, $\dim(U) = n-1$ and $d_s(\text{Orb(U)}) = 2$. Hence the result.

Contd..

Theorem

Let α be a primitive element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Let $U = \{0, \alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_{q^k-1}}\}$ be a subspace in $\mathbb{F}_{q^n}$ of dimension k such that U does not generate a full-length orbit. If the subspace code Orb(U) is r-intersecting equidistant code $(r > 0)$, then the indices i_j, $1 \leq j \leq q^k - 1$, form a relative difference set in $\mathbb{Z}_{q^n-1}$.

Contd..

Theorem

Let α be a primitive element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Let $U = \{0, \alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_{q^k-1}}\}$ be a subspace in $\mathbb{F}_{q^n}$ of dimension k such that U does not generate a full-length orbit. If the subspace code Orb(U) is r-intersecting equidistant code $(r > 0)$, then the indices i_j, $1 \leq j \leq q^k - 1$, form a relative difference set in $\mathbb{Z}_{q^n-1}$.

Proof idea:

- Let Orb(U) be an equidistant subspace code with subspace distance $2(k - r)$, where $r > 0$. Let Stab$(U) = \mathbb{F}^*_{q^t}$ for some t, $1 < t < k$ and t divides gcd(k, n).
- Let $N = \{i_j \mid \alpha^{i_j} \in \mathbb{F}^*_{q^t}\}$. Then N is a subgroup of $\mathbb{Z}_{q^n-1}$. Clearly, the cardinality of N is $q^t - 1$.
- Let $D = \{i_j \mid \alpha^{i_j} \in U\}$. For any $j \in N$, $U = \alpha^j U$. This gives $|D \cap (j + D)| = q^k - 1$.
- For any $m \in \mathbb{Z}_{q^n-1} \setminus N$, $\dim(U \cap \alpha^m U) = q^r$. So, we get $|D \cap (m + D)| = q^r - 1$. Thus, the set of indices D constitutes a $(q^t - 1, \frac{q^n-1}{q^t-1}, q^k - 1, q^k - 1, q^r - 1)$-relative difference set in $\mathbb{Z}_{q^n-1}$.

Contd..

Lemma

Let U be a subspace of dimension k in $\mathbb{F}_{q^n}$. For any $\alpha \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$ and $s \in \mathbb{F}_q^*$, $\dim(U \cap (\alpha + s)U) = \dim(U \cap \alpha U)$.

Theorem

Let n be an even integer and let U be a subspace in $\mathbb{F}_{q^n}$. Let α be an element of degree 2 in $\mathbb{F}_q^n$. Let $V = U \cap \alpha U$ and $V \neq \{0\}$. Then $\mathbb{F}_{q^2}^* \subseteq Stab(V)$.

Theorem

Let n be an even number and U be a subspace in $\mathbb{F}_{q^n}$. For any element β of degree 2 in $\mathbb{F}_{q^n}$ with $\beta \notin Stab(U)$, $Orb_\beta(U)$ is a sunflower.

Theorem

Let n be an even number and U be a subspace in $\mathbb{F}_{q^n}$. For any element β of degree 2 in $\mathbb{F}_{q^n}$ with $\beta \notin Stab(U)$, $Orb_{\beta}(U)$ is a sunflower.

Proof idea:

- The proof consists of two parts. First, we prove that $\mathrm{Orb}_{\beta}(U)$ is an equidistant code.
- Then, we show that the intersecting subspace of the reference space U and elements of $\mathrm{Orb}_{\beta}(U)$ are same.
- As β is an element of degree 2 in $\mathbb{F}_{q^n}$, $\mathbb{F}_q[\beta] = \{a + c\beta \mid a, c \in \mathbb{F}_q\}$. Clearly, $\{\beta^i \mid 0 \leq i \leq |\beta| - 1\} \subseteq \mathbb{F}_q[\beta]$.
- Since $\dim(U \cap \beta U) = \dim(U \cap (a + c\beta))$ for all $a \in \mathbb{F}_q$ and $c \in \mathbb{F}_q^*$, $\mathrm{Orb}_{\beta}(U)$ is an equidistant code.
- If $\dim(U \cap \beta U) = 0$ then $\mathrm{Orb}_{\beta}(U)$ is a sunflower with a trivial center.
- Let $\dim(U \cap \beta U) \neq 0$ and let $V = U \cap \beta U$. Then $\mathbb{F}_{q^2}^* \subseteq \mathrm{Stab}(V)$. Consider an element $\beta^j = a\beta + c$ for some $a, c \in \mathbb{F}_q$ and $a \neq 0$ such that $\beta^j U \neq U$.

Contd..

- As $\mathbb{F}_{q^2}^* \subseteq \text{Stab}(V)$, $(a\beta + c)^{-1}V = V$. Thus $(a\beta + c)^{-1}V \subseteq U$ and $V \subseteq U \cap (a\beta + c)U$.
- Since $\text{Orb}_\beta(U)$ is an equidistant code, $\dim(U \cap (a\beta + c)U) = \dim(U \cap \beta U)$. So, we get $V = U \cap (a\beta + c)U$. Hence, $\text{Orb}_\beta(U)$ is a sunflower.

Theorem

For any sunflower $\text{Orb}_\beta(U)$ ($\beta \notin \text{Stab}(U)$), the center does not generate a full-length orbit.

Contd..

- As $\mathbb{F}_{q^2}^* \subseteq \text{Stab}(V)$, $(a\beta + c)^{-1}V = V$. Thus $(a\beta + c)^{-1}V \subseteq U$ and $V \subseteq U \cap (a\beta + c)U$.
- Since $\text{Orb}_\beta(U)$ is an equidistant code, $\dim(U \cap (a\beta + c)U) = \dim(U \cap \beta U)$. So, we get $V = U \cap (a\beta + c)U$. Hence, $\text{Orb}_\beta(U)$ is a sunflower.

Theorem

For any sunflower $Orb_\beta(U)$ ($\beta \notin Stab(U)$), the center does not generate a full-length orbit.

Proof idea:

- Let V be the center of the sunflower $\text{Orb}_\beta(U)$. If $V = \{0\}$ then the result is trivially true. Let $V \neq \{0\}$.
- Let $\beta^2 \in \mathbb{F}_q$. As $V = U \cap \beta U$,

$$\beta V = \beta U \cap \beta^2 U = \beta U \cap U = V \ .$$

  From this, we get $V = \beta V$.

- Now, let $\beta^2 \notin \mathbb{F}_q$. Since V is the center,

$$V = U \cap \beta U = U \cap \beta^2 U \; .$$

Now, $V \subseteq \beta U \cap \beta^2 U = \beta(U \cap \beta U) = \beta V$. This gives $V = \beta V$. Thus, $\beta \in \mathrm{Stab}(V)$.

Contd..

- Now, let $\beta^2 \notin \mathbb{F}_q$. Since V is the center,

$$V = U \cap \beta U = U \cap \beta^2 U \, .$$

Now, $V \subseteq \beta U \cap \beta^2 U = \beta(U \cap \beta U) = \beta V$. This gives $V = \beta V$. Thus, $\beta \in \mathrm{Stab}(V)$.

Observations:

- By previous theorem, for a sunflower $\mathrm{Orb}_\beta(U)$ with center $V \neq \{0\}$, $\beta \in \mathrm{Stab}(V)$. It is known that Stab(V) is a subgroup of $\mathbb{F}_{q^n}^*$. So, we conclude that $\{\beta^i \mid i = 0, 1, \ldots, |\beta| - 1\} \subseteq \mathrm{Stab}(V)$.
- Since $\mathrm{Stab}(V) \cup \{0\}$ is a subfield of $\mathbb{F}_{q^n}$, for a prime number n, the sunflower $\mathrm{Orb}_\beta(U)$ in $\mathbb{F}_{q^n}$ always has a trivial center.
- We can quickly check that a subspace of dimension one generates a full-length orbit. Thus, according to previous theorem, the dimension of the non-trivial center of a sunflower is always greater than one.

  However, 1-intersecting equidistant orbit codes, which are not sunflower, can exist in $\mathbb{F}_{q^n}$. Next, we provide an example of such a code.

Example

- Consider an irreducible monic polynomial $p(x) = x^{10} + x^6 + x^5 + x^3 + x^2 + x + 1$ of degree 10 over $\mathbb{F}_2$. Let α be a root of $p(x)$. Then $\mathbb{F}_2(\alpha)$ be an extension field of degree 10 over $\mathbb{F}_2$.
- Let $U = \langle 1, \alpha^{13}, \alpha^{70}, \alpha^{177} \rangle_{\mathbb{F}_2}$. The dimension of U over $\mathbb{F}_2$ is 4.
- The cardinality of the code $\text{Orb}(U) = \{\gamma U \mid \gamma \in \mathbb{F}_{2^{10}}^*\}$ is 1023. From this follows that U generates a full-length orbit.
- Let $\beta = \alpha^{93}$ be an element of order 11 in $\mathbb{F}_{2^{10}}^*$. By using the Magma we get that $\dim(U \cap \beta^i U) = 1$ for all i in $\{0, 1, \ldots, |\beta| - 1\}$ with $\beta^i U \neq U$. Thus, $\text{Orb}_\beta(U)$ is 1- intersecting equidistant code.
- As $U \cap \beta U = \{0, \alpha^{457}\}$ and $U \cap \beta^2 U = \{0, \alpha^{415}\}$, $\text{Orb}_\beta(U)$ is not a sunflower.

Contd..

Theorem

Let U be a subspace of dimension k in $\mathbb{F}_{q^n}$ such that U generates a full-length orbit. Let $Orb_\beta(U)$ ($\beta \in \mathbb{F}_{q^n} \backslash \mathbb{F}_q$) be a sunflower with a non-trivial center then

$$|Orb_\beta(U)| \leq \frac{q^s - 1}{q - 1} ,$$

where $s < k$ is the largest positive divisor of n.

Contd..

Theorem

Let U be a subspace of dimension k in $\mathbb{F}_{q^n}$ such that U generates a full-length orbit. Let $Orb_\beta(U)$ $(\beta \in \mathbb{F}_{q^n} \backslash \mathbb{F}_q)$ be a sunflower with a non-trivial center then

$$|Orb_\beta(U)| \leq \frac{q^s - 1}{q - 1} \ ,$$

where $s < k$ is the largest positive divisor of n.

Proof idea:

- Let V be the center of the sunflower $\mathrm{Orb}_\beta(U)$ such that $V \neq \{0\}$.
- As $\mathrm{Stab}(V) \cup \{0\}$ is a subfield of $\mathbb{F}_{q^n}$ and V is a vector space over $\mathrm{Stab}(V) \cup \{0\}$, let $\mathrm{Stab}(V) = \mathbb{F}^*_{q^s}$ for some positive integer $s > 1$ dividing $\gcd(\dim(V), n)$.
- Since the dimension of U is k, the dimension of V is less than or equal to $k - 1$. So, we get $s \leq k - 1$ and $\{\beta^i \mid i = 0, 1, \ldots, |\beta| - 1\} \subseteq \mathbb{F}^*_{q^s}$.
- Thus, the order of β is less than or equal to $q^s - 1$. As U generates a full-length orbit, $|\mathrm{Orb}_\beta(U)| \leq \frac{q^s-1}{q-1}$.

Contd..

- The cardinality of a sunflower $\mathrm{Orb}_{\beta}(U)$ in $\mathbb{F}_{q^n}$ with a trivial center may be greater than $\frac{q^s-1}{q-1}$ where $s < \mathtt{dim}(U)$ is the largest positive divisor of n.

Contd..

- The cardinality of a sunflower $\mathrm{Orb}_\beta(U)$ in $\mathbb{F}_{q^n}$ with a trivial center may be greater than $\frac{q^s-1}{q-1}$ where $s < \mathtt{dim}(U)$ is the largest positive divisor of n. The following example illustrates this.

Example

- Consider a monic irreducible polynomial $p(x) = x^{12} + x^6 + x^5 + x^4 + x^2 + 2$ of degree 12 over $\mathbb{F}_3$. Let α be a root of $p(x)$. Then, $\mathbb{F}_3(\alpha)$ is an extension field of degree 12 over $\mathbb{F}_3$.
- Let $U = \langle \alpha^{565}, \alpha^{123982}, \alpha^{179292}, \alpha^{208314}, \alpha^{395390} \rangle_{\mathbb{F}_3}$. The dimension of U over $\mathbb{F}_3$ is 5, and U generates a full-length orbit.
- Let $\gamma = \alpha^{4088}$ be an element in $\mathbb{F}_{3^{12}}$. The multiplicative order of γ is 130.
- By using the Magma, we computed that $U \cap \gamma^i U = \{0\}$ for all i in $\{1, \dots, |\gamma|\}$. Thus, $\mathrm{Orb}_\gamma(U)$ is a sunflower with a trivial center.
- The cardinality of $\mathrm{Orb}_\gamma(U)$ is 65. Here, n is 12, and k is 5. So, the largest divisor of n less than k is 4. Clearly, $|\mathrm{Orb}_\gamma(U)| = 65 > \frac{3^4-1}{3-1} = 40$.

Contd..

Theorem

Let U be a subspace of dimension k in $\mathbb{F}_{q^n}$ *such that* $Stab(U) = \mathbb{F}^*_{q^t}$. *Let* $Orb_\gamma(U)$ ($\gamma \notin Stab(U)$) *be a sunflower with a non-trivial center then*

$$|Orb_\gamma(U)| \leq \frac{q^s - 1}{q^t - 1} \, ,$$

where $s < k$ *is the largest positive divisor of n.*

Contd..

Theorem

Let U be a subspace of dimension k in $\mathbb{F}_{q^n}$ *such that Stab*$(U) = \mathbb{F}^*_{q^t}$. *Let Orb*$_\gamma(U)$ $(\gamma \notin Stab(U))$ *be a sunflower with a non-trivial center then*

$$|Orb_\gamma(U)| \leq \frac{q^s - 1}{q^t - 1},$$

where $s < k$ *is the largest positive divisor of n.*

Proof idea:

- Let $\text{Stab}(U) = \mathbb{F}^*_{q^t}$. Let $\gamma \notin \text{Stab}(U)$ and let $\text{Orb}_\gamma(U)$ be a sunflower with a non-trivial center V. Then $V = U \cap \gamma U$.
- For any $\delta \in \mathbb{F}^*_{q^t}$, $\delta V = \delta U \cap \delta\gamma U$. As $\delta \in \text{Stab}(U)$, $\delta U = U$ and $\delta\gamma U = \gamma U$. Thus, $\delta V = V$. From this follows that $\delta \in \text{Stab}(V)$. Since δ was an arbitrary element in $\text{Stab}(U)$, we get $\text{Stab}(U) \subseteq \text{Stab}(V)$.
- Let $\text{Stab}(V) = \mathbb{F}^*_{q^s}$. Now, by the same argument used in previous theorem, we get

  $$|\text{Orb}_\gamma(U)| \leq \frac{q^s - 1}{q^t - 1},$$

  where $s < k$ is the largest positive divisor of n.

Contd..

Definition (Hirschfeld, 1998)

For any $k(< n)$, a k-spread is a collection of k-dimensional subspaces $\{X_1, X_2, \ldots, X_t\}$ of $\mathbb{F}_q^n$ such that

1. $X_i \cap X_j = \{0\}$, for $i \neq j, 1 \leq i, j \leq t$.
2. $\bigcup_{i=1}^{t} X_i = \mathbb{F}_q^n$.

Definition

A partial k-spread of $\mathbb{F}_{q^n}$ is a subset $\mathcal{A} \subseteq \mathcal{G}_q(n, k)$ such that $U \cap V = \{0\}$ for all $U, V \in \mathcal{A}$ with $U \neq V$.

Theorem

A k-spread exists if and only if k divides n. Moreover, the cardinality of a k-spread is $\frac{q^n-1}{q^k-1}$.

Hirschfeld, J.: Projective Geometries over Finite Fields, Second Edition. New York, Oxford University Press (1998).

Lemma

Let $\mathcal{A} \subseteq \mathcal{G}_q(n, k)$ be a partial k-spread code. Denote by r the remainder obtained when n is divided by k. Then $|\mathcal{A}| \leq \frac{q^n - q^r}{q^k - 1}$.

Next, we discuss about the maximum size of a sunflower with a trivial center.

- If k divides n then $\mathrm{Orb}_\beta(U)$ is clearly a subset of k-spread. Thus,

$$|\mathrm{Orb}_\beta(U)| \leq \frac{q^n - 1}{q^k - 1} .$$

Contd..

Lemma

Let $\mathcal{A} \subseteq \mathcal{G}_q(n,k)$ be a partial k-spread code. Denote by r the remainder obtained when n is divided by k. Then $|\mathcal{A}| \leq \frac{q^n - q^r}{q^k - 1}$.

Next, we discuss about the maximum size of a sunflower with a trivial center.

- If k divides n then $\mathrm{Orb}_\beta(U)$ is clearly a subset of k-spread. Thus,

$$|\mathrm{Orb}_\beta(U)| \leq \frac{q^n - 1}{q^k - 1} .$$

The above-stated bound may be attainable. We give below such an example.

Example

- Consider a monic irreducible polynomial $p(x) = x^{12} + x^7 + x^6 + x^5 + x^3 + x + 1$ of degree 12 over $\mathbb{F}_2$. Let α be a root of $p(x)$. Then $\mathbb{F}_2(\alpha)$ is an extension field of degree 12 over $\mathbb{F}_2$ and $\mathbb{F}_2(\alpha) \simeq \mathbb{F}_{2^{12}}$.
- Let $U = \langle 1, \alpha^{470}, \alpha^{3607}, \alpha^{3621} \rangle_{\mathbb{F}_2}$. The dimension of U over $\mathbb{F}_2$ is 4, and U generates a full-length orbit. Let $\gamma = \alpha^{15}$. The multiplicative order of γ in $\mathbb{F}_{2^{12}}^*$ is 273.

Contd..

Example (Contd.)

- Consider the orbit code $\mathrm{Orb}_\gamma(U) = \{\gamma^i U \mid 0 \le i \le |\gamma| - 1\}$. Using the magma, we computed that $U \cap xU = \{0\}$ for all $xU \in \mathrm{Orb}_\gamma U$ with $xU \neq U$. Thus, $\mathrm{Orb}_\gamma(U)$ is a sunflower with a trivial center.
- The computation through the magma shows that the cardinality of $\mathrm{Orb}_\gamma(U)$ is 273, which is equal to $\frac{2^{12}-1}{2^4-1}$. Hence, $\mathrm{Orb}_\gamma(U)$ is an optimal sunflower code with a trivial center.

Contd..

Example (Contd.)

- Consider the orbit code $\text{Orb}_\gamma(U) = \{\gamma^i U \mid 0 \leq i \leq |\gamma| - 1\}$. Using the magma, we computed that $U \cap xU = \{0\}$ for all $xU \in \text{Orb}_\gamma U$ with $xU \neq U$. Thus, $\text{Orb}_\gamma(U)$ is a sunflower with a trivial center.
- The computation through the magma shows that the cardinality of $\text{Orb}_\gamma(U)$ is 273, which is equal to $\frac{2^{12}-1}{2^4-1}$. Hence, $\text{Orb}_\gamma(U)$ is an optimal sunflower code with a trivial center.

- If k does not divide n then $\text{Orb}_\beta(U)$ is a subset of partial k-spread. Let r denote the remainder obtained when n is divided by k. So, we get

$$|\text{Orb}_\beta(U)| \leq \frac{q^n - q^r}{q^k - 1} .$$

From this, it follows that $|\text{Orb}_\beta(U)| \leq \frac{q^r(q^{n-r}-1)}{q^k-1}$. We know that the cardinality of $\text{Orb}_\beta(U)$ is a divisor of the order of $\mathbb{F}_{q^n}^*$. However, $\frac{q^r(q^{n-r}-1)}{q^k-1}$ does not divide $q^n - 1$. Hence, in this case, $|\text{Orb}_\beta(U)| < \frac{q^n-q^r}{q^k-1}$.

- Kötter, R., Kschischang, R. F.: Coding for errors and erasures in random network coding, IEEE Trans. Inf. Theory 54, 3579-3591 (2008).
- Etzion, T., Vardy, A.: Error-correcting codes in projective space, IEEE Trans. Inf. Theory 57(2), 1165-1173 (2011).
- Trautmann, L. A., Manganiello, F., Braun, M., Rosenthal, J.: Cyclic orbit codes, IEEE Trans. Inf. Theory 59(11), 7386-7404 (2013).
- Gluesing-Luerssen, H., Morrison, K., Troha, C.: Cyclic orbit codes and stabilizer subfields, Adv. Math. Commun. 9(2), 177-197 (2015).
- Otal, K., Ozbudak, F.: Cyclic subspace codes via subspace polynomials, Des. Codes Cryptogr. 85(2), 191-204 (2017).
- Etzion, T., Raviv, N..: Equidistant codes in the Grassmannian, Discret. Appl. Math. 186, 87-97 (2015).
- Bartoli, D., Pavese, F.: A note on equidistant subspace codes, Discret. Appl. Math. 198, 291-296 (2016).
- Gorla, E., Ravagnani, A.: Equidistant subspace codes, Linear Algebra Appl. 490, 48-65 (2016).

References

- Gluesing-Luerssen, H., Lehmann, H.: Distance distributions of cyclic orbit codes, Des. Codes Cryptogr. 89, 447-470 (2021).
- Stinson, R. D.: Combinatorial Designs: Constructions and Analysis, Springer, New York (2004).
- Van Lint, J.H., Wilson, R.M.: A Course in Combinatorics 2nd Edn. Cambridge University Press, Cambridge (2001).
- Jungnickel, D.: On automorphism groups of divisible designs. Can. J. Math. 34(2), 257-297 (1982).
- Ghatak, A.: Construction of Singer subgroup orbit codes based on cyclic difference sets. In: Proceedings of the Twentieth National Conference on Communications (NCC 2014), pp. 1-4, Kanpur, India. IEEE (2014).
- Gorla, E., Ravagnani, A.: Partial spreads in random network coding. Finite Fields Appl. 26, 104-115 (2014).
- Bosma, W., Cannon, J.: Handbook of Magma Functions, School of Mathematics and Statistics, Univ. of Sydney (1995).

Thank You.