Weight Distributions of Cyclic Orbit Codes

Heide Gluesing-Luerssen, **Hunter Lehmann**

University of Kentucky

January 5, 2022

Subspace Codes

Grassmannian:

$$\mathcal{G}_q(k,n) = \{k\text{-dim. } \mathbb{F}_q\text{-subspaces of } \mathbb{F}_{q^n}\}$$

Constant dimension subspace code:

A collection of k-dimensional $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^n}$, i.e. $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$

Subspace distance:

$$\mathrm{d_s}(\mathcal{U},\mathcal{V}) = \dim(\mathcal{U}) + \dim(\mathcal{V}) - 2\dim(\mathcal{U}\cap\mathcal{V})$$
$$\mathrm{d_s}(\mathcal{C}) = \min_{\mathcal{U},\mathcal{V}\in\mathcal{C}}\{\mathrm{d}(\mathcal{U},\mathcal{V}) \mid \mathcal{U}\neq\mathcal{V}\}$$

- If $\dim(\mathcal{U}) = \dim(\mathcal{V}) = k$, $\mathrm{d_s}(\mathcal{U},\mathcal{V}) = 2k - 2\dim(\mathcal{U}\cap\mathcal{V})$ is even.

Cyclic Orbit Codes

The cyclic (Singer) subgroup $S = \mathbb{F}_{q^n}^* \leq \mathrm{GL}_n(q)$ acts on $\mathcal{G}_q(k,n)$ by multiplication: for any $\alpha \in \mathbb{F}_{q^n}^*$,

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

A **cyclic orbit code** is the orbit of a single subspace under this action

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

The stabilizer of a subspace is always the multiplicative group of a subfield

$$\mathrm{Stab}_S(\mathcal{U}) = \mathbb{F}_{q^t}^*, \text{ for some } t \mid \gcd(n,k).$$

Goal: Find finer invariant for **optimal cyclic orbit codes**:

$$|\mathrm{Orb}_S(\mathcal{U})| = \frac{q^n-1}{q-1} \quad \text{and} \quad \mathrm{d_s}(\mathrm{Orb}_S(\mathcal{U})) = 2k-2.$$

Projective Spaces

Projective space:

$$\mathbb{P}(\mathbb{F}_{q^n}) = \mathbb{F}_{q^n}^* / \sim,$$

where $\sim$ is the equivalence relation defined by

$$a \sim b \Leftrightarrow \frac{a}{b} \in \mathbb{F}_q^*.$$

Projective subspace: For any $\mathcal{U} \in \mathcal{G}_q(k, n)$, define

$$\mathbb{P}(\mathcal{U}) = (\mathcal{U} \setminus \{0\}) / \sim$$

Notation: We write $\overline{\alpha}$ for the equivalence class of α in $\mathbb{P}(\mathbb{F}_{q^n})$.

Distributions

Distance distribution of a subspace code $\mathcal{C}$:

$$(\delta_0, \delta_1, \dots, \delta_{d-1}, \delta_d),$$

where δ_i counts the number of pairs $(\mathcal{U}, \mathcal{V}) \in \mathcal{C} \times \mathcal{C}$ such that $\mathrm{d_s}(\mathcal{U}, \mathcal{V}) = i$.

Weight distribution of an orbit code $\mathcal{C}$ with generator $\mathcal{U}$:

$$(d_0, d_2, \dots, d_{2k-2}, d_{2k}),$$

where d_i counts the number of subspaces $\mathcal{V} \in \mathcal{C}$ such that $\mathrm{d_s}(\mathcal{U}, \mathcal{V}) = i$.

Intersection distribution of a cyclic orbit code $\mathcal{C}$ with generator $\mathcal{U}$:

$$(\lambda_0, \lambda_1, \dots, \lambda_\ell),$$

where $\lambda_i = |\mathcal{L}_i| = |\{\overline{\alpha} \in \mathbb{P}(\mathbb{F}_{q^n}) \mid \dim(\mathcal{U} \cap \alpha\mathcal{U}) = i\}|$.

Simplest case: spread codes

Spread code:

$$\text{Each } \mathcal{W} \in \mathcal{G}_q(n,1) \text{ is contained in exactly one } \mathcal{U} \in \mathcal{C}$$

Equivalently, for $\mathcal{U}, \mathcal{V} \in \mathcal{C}$:

$$\mathcal{U} \cap \mathcal{V} = \{0\} \qquad \text{and} \qquad \bigcup_{\mathcal{U} \in \mathcal{C}} \mathcal{U} = \mathbb{F}_{q^n}.$$

- $\mathrm{d_s}(\mathrm{Orb}_S(\mathcal{U})) = 2k \Rightarrow \mathrm{Stab}(\mathcal{U}) = \mathbb{F}_{q^k}^*$ and $\mathrm{Orb}_S(\mathcal{U})$ is a spread code
- Intersection distribution is a single entry:

$$\lambda_0 = \frac{q^n - q^k}{q-1}.$$

Distance distribution for full-length orbit codes

Theorem (Gluesing-Luerssen,L.). *Let $\mathcal{C} = \mathrm{Orb}_S(\mathcal{U})$ have full-length orbit with $d_s(\mathcal{C}) = 2k - 2\ell$ and recall $\mathcal{L}_i = \{\overline{\alpha} \in \mathbb{P}(\mathbb{F}_{q^n}) \mid \dim(\mathcal{U} \cap \alpha\mathcal{U}) = i\}$. Then*

$$\psi : \{(\overline{u}, \overline{v}) \mid \overline{u} \neq \overline{v} \in \mathbb{P}(\mathcal{U}))\} \to \bigcup_{i=1}^{\ell} \mathcal{L}_i$$

by $\psi(\overline{u}, \overline{v}) = \overline{uv^{-1}}$ is well-defined, surjective, and $\overline{\alpha} \in \mathcal{L}_i \Leftrightarrow |\psi^{-1}(\overline{\alpha})| = \frac{q^i-1}{q-1}$.

- **Key Idea:** If $\dim(\mathcal{U} \cap \alpha\mathcal{U}) \geq 1$, we can write $\overline{\alpha} = \frac{\overline{u}}{\overline{v}}$ for each equivalence class $\overline{u}$ for $u \in \mathcal{U} \cap \alpha\mathcal{U}$.

Corollary (Gluesing-Luerssen,L.). *Let $\mathcal{U}$ have full-length orbit and $d_s(\mathrm{Orb}_S(\mathcal{U})) = 2k - 2\ell$. Then*

$$\sum_{i=1}^{\ell} \left(\frac{q^i - 1}{q - 1} \right) \lambda_i = \frac{q^k - 1}{q - 1} \frac{q^k - q}{q - 1}.$$

Corollary (Gluesing-Luerssen,L.). *Let $\mathrm{Orb}_S(\mathcal{U})$ be an optimal cyclic orbit code. Then $\mathrm{Orb}(\mathcal{U})$ has intersection distribution (λ_0, λ_1), where*

$$\lambda_1 = \frac{q^k - 1}{q - 1} \frac{q^k - q}{q - 1}, \quad \lambda_0 = \frac{q^n - 1}{q - 1} - 1 - \frac{q^k - 1}{q - 1} \frac{q^k - q}{q - 1}.$$

Full length orbits with smaller minimum distance

Theorem (Gluesing-Luerssen, L.). *Let $\mathcal{U}$ have full-length orbit and $d_s(\mathrm{Orb}_S(\mathcal{U})) = 2k-4$. Then the intersection distribution of $\mathcal{U}$ depends only on q, n, k, and a new parameter r describing the orbits of the 2-dimensional intersections $\mathcal{U} \cap \alpha\mathcal{U}$.*

- Proof uses group actions, structure of small dimensional intersections, previous Corollary.
- The theorem does not hold if $\mathrm{d_s}(\mathrm{Orb}_S(\mathcal{U})) \leq 2k-6$.
- General behavior of intersection distribution for $\mathrm{d_s}(\mathrm{Orb}_S(\mathcal{U})) \leq 2k-6$ is open.

Example with $\mathbf{d_s}(\mathcal{C}) = 2k - 4$

$q = 2, n = 8, k = 3$: Fix a generator ω for $\mathbb{F}_{2^8}^*$ and take $\mathcal{U} = \langle 1, \omega^{85}, \omega^{17} \rangle$.

- **Corollary:** $\frac{q^k-1}{q-1}\frac{q^k-q}{q-1} = \lambda_1 + \frac{q^2-1}{q-1}\lambda_2$
- $42 = \lambda_1 + 3\lambda_2$
- **Q:** What can we learn about $\mathcal{V} = \mathcal{U} \cap \alpha\mathcal{U}$ such that $\dim(\mathcal{V}) = 2$?

  Case 1: $\mathcal{V} = \mathbb{F}_{2^2}$
  - $\overline{\alpha} \in \mathbb{P}(\mathbb{F}_2^2) \setminus \{\overline{1}\} = \{\overline{\omega^{85}}, \overline{\omega^{170}}\}$

  Case 2: $\mathcal{V}$ has full-length orbit, e.g. $\mathcal{V} = \langle 1, \omega^{17} \rangle$
  - 2 possibilities for $\overline{\alpha}$ e.g. $\overline{\alpha} \in \{\overline{\omega^{187}}, \overline{\omega^{238}}\}$
  - Also, $\omega^{-187}\mathcal{V} = \mathcal{U} \cap \omega^{-187}\mathcal{U}$ and $\omega^{-238}\mathcal{V} = \mathcal{U} \cap \omega^{-238}\mathcal{U}$.
  - r counts the number of these sets (e.g. $\{\mathcal{V}, \omega^{-187}\mathcal{V}, \omega^{-238}\mathcal{V}\}$) of related $\mathcal{V}$
- $\lambda_2 = q + rq(q+1) = 2 + 2(2)(2+1) = 14$
- $\lambda_1 = 42 - 3\lambda_2 = 0$
- $\lambda_0 = \frac{q^n-1}{q-1} - 1 - \lambda_1 - \lambda_2 = 240$

Thank you.