# Cyclic Orbit Codes

Anna-Lena Trautmann

Institute of Mathematics
University of Zurich

Workshop on Algebraic Structure in Network Information Theory
Banff, August 17th 2011

joint work with F. Manganiello, M. Braun, J. Rosenthal

Notation:

- $\mathcal{G}_q(k,n)$ the Grassmannian
- $\mathcal{U} \in \mathcal{G}_q(k,n)$ a vector space
- $U \in Mat_{k\times n}$ its matrix representation
- $GL_n$ the general linear group
- $A \in GL_n$ a matrix
- $G \leq GL_n$ a subgroup
- group operation from the right on $\mathcal{G}_q(k,n)$:

$$\begin{array}{ccc} \mathcal{G}_q(k,n) \times GL_n & \longrightarrow & \mathcal{G}_q(k,n) \\ (\mathcal{U}, A) & \longmapsto & \mathcal{U}A := \text{row space}(UA) \end{array}$$

**Definition**

Let $\mathcal{U} \in \mathcal{G}_q(k,n)$ be fixed and $G$ a subgroup of $GL_n$. Then

$$\mathcal{U}G := \{\mathcal{U}A \mid A \in G\}$$

is called an *orbit code* .
If an orbit code can be defined by a cyclic subgroup $G \leq GL_n$, it is called a *cyclic* orbit code.

**Definition**

Let $\mathcal{U} \in \mathcal{G}_q(k,n)$ be fixed and $G$ a subgroup of $GL_n$. Then

$$\mathcal{U}G := \{\mathcal{U}A \mid A \in G\}$$

is called an *orbit code* .
If an orbit code can be defined by a cyclic subgroup $G \leq GL_n$, it is called a *cyclic* orbit code.

**Theorem**

*Let $\mathcal{C} = \{\mathcal{U}A \mid A \in G\}$ be an orbit code. Then*

$$\begin{aligned} d_{\min}(\mathcal{C}) &= \min\{d_S(\mathcal{U}A,\mathcal{U}A') \mid A, A' \in G/Stab(\mathcal{U})\} \\ &= \min\{d_S(\mathcal{U},\mathcal{U}A) \mid A \in G/Stab(\mathcal{U})\}. \end{aligned}$$

*("Linearity")*

### Theorem

*Let $G \leq GL_n$ and $H = S^{-1}GS$ for some $S \in GL_n$. Moreover, let $\mathcal{U} \in \mathcal{G}_q(k,n)$ and $\mathcal{V} := \mathcal{U}S$. Then the conjugate orbit codes*

$$\mathcal{C} := \{\mathcal{U}A | A \in G\} \text{ and } \mathcal{C}' := \{\mathcal{V}B | B \in H\}$$

*have the same cardinality and minimum distance.*
*("Equivalence")*

### Theorem

*Let $G \leq GL_n$ and $H = S^{-1}GS$ for some $S \in GL_n$. Moreover, let $\mathcal{U} \in \mathcal{G}_q(k,n)$ and $\mathcal{V} := \mathcal{U}S$. Then the conjugate orbit codes*

$$\mathcal{C} := \{\mathcal{U}A | A \in G\} \text{ and } \mathcal{C}' := \{\mathcal{V}B | B \in H\}$$

*have the same cardinality and minimum distance.*
*("Equivalence")*

Cyclic case: Any matrix is conjugate to its rational canonical form.

$\Longrightarrow$ It is sufficient to investigate the orbits of groups generated by rational canonical forms!!!

The results are then carried over to any irreducible cyclic orbit code via the choice of starting point of the orbit.

Spread codes are constant dimension codes with minimum distance $2k$ ("no intersection") and cardinality $\frac{q^n-1}{q^k-1}$ (covering the whole space).

Spread codes are constant dimension codes with minimum distance $2k$ ("no intersection") and cardinality $\frac{q^n-1}{q^k-1}$ (covering the whole space).

### Theorem

*If* $k|n, c := \frac{q^n-1}{q^k-1}$ *and* $\alpha$ *a primitive element of* $\mathbb{F}_{q^n}$, *then the vector space generated by* $1, \alpha^c, ..., \alpha^{(k-1)c}$ *is equal to* $\{\alpha^{ic}|i = 0, ..., q^k - 2\} \cup \{0\} = \mathbb{F}_{q^k}$.

### Theorem

*The set*

$$\mathcal{S} = \left\{\alpha^i \cdot \mathbb{F}_{q^k} \mid i = 0, \ldots, c-1\right\}$$

*defines a spread code in* $\mathbb{F}_{q^n} \cong \mathbb{F}_q^n$.

Example (Spread of $\mathcal{G}_2(2,4)$):

- $c = \frac{q^n-1}{q^k-1} = \frac{15}{3} = 5$
- $p(x) := x^4 + x + 1$ primitive
- $\alpha$ a root of $p(x)$
- $P$ its companion matrix
- $\phi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_{q^n}$ vector space isomorphism

$$u_1 = \phi^{-1}(\alpha^0) = \phi^{-1}(1) = (1000)$$
$$u_2 = \phi^{-1}(\alpha^c) = \phi^{-1}(\alpha^5) = \phi^{-1}(\alpha^2 + \alpha) = (0110)$$

Example (Spread of $\mathcal{G}_2(2,4)$):

- $c = \frac{q^n-1}{q^k-1} = \frac{15}{3} = 5$
- $p(x) := x^4 + x + 1$ primitive
- $\alpha$ a root of $p(x)$
- $P$ its companion matrix
- $\phi : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$ vector space isomorphism

$$u_1 = \phi^{-1}(\alpha^0) = \phi^{-1}(1) = (1000)$$
$$u_2 = \phi^{-1}(\alpha^c) = \phi^{-1}(\alpha^5) = \phi^{-1}(\alpha^2 + \alpha) = (0110)$$

Then the following orbit is a spread code:

$$\mathcal{U}\langle P\rangle = \mathrm{rs}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \left\langle \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \right\rangle$$

Minimum distance decoder:
For an orbit code $\mathcal{C} = \mathcal{U}G$ and a received subspace $\mathcal{R} \in \mathcal{P}(\mathbb{F}_q^n)$ the minimum distance decoder searches for the group element $A \in G$ such that $\dim(\mathcal{R} \cap \mathcal{U}A)$ is maximal.

Syndrome decoding:

$$\begin{tikzcd} \mathcal{U}G: \arrow[r, dash] & \mathcal{U} \arrow[r, dash] \arrow[r, bend left, "A"] \arrow[d, leftrightarrow, "\text{minimial}"'] & \mathcal{S} \arrow[r, dash] \arrow[d, leftrightarrow] & {} \\ \mathcal{U}'G: \arrow[r, dash] & \mathcal{U}' & \mathcal{R} \arrow[l, dash] \arrow[l, bend left, "A^{-1}"] \arrow[r, dash] & {} \end{tikzcd}$$

Question: Are there groups where it is easy to find the "syndrome" and the orbit a given element is on?

Let $p(x)$ be primitive and $P$ its companion matrix.
$\Longrightarrow$ $\langle P\rangle$ acts transitively on $\mathbb{F}_q^n$

---

INPUT: Code $\mathcal{C} = \mathcal{U}\langle P\rangle$, received $\mathcal{R}$
OUTPUT: $A \in \langle P\rangle$ such that $\dim(\mathcal{R} \cap \mathcal{U}A)$ is maximal

---

```
set d := 0, A := I_{n×n}
for all v ∈ U \ {0} do
   for all w ∈ R \ {0} do
      compute A' := φ^{-1}(φ(w)φ(v)^{-1})
      compute d' := dim(R ∩ UA)
      if d' > d then set d := d' and A := A'
return A
```

---

Let $p(x)$ be primitive and $P$ its companion matrix.
$\Longrightarrow$ $\langle P \rangle$ acts transitively on $\mathbb{F}_q^n$

---

INPUT: Code $\mathcal{C} = \mathcal{U}\langle P \rangle$, received $\mathcal{R}$
OUTPUT: $A \in \langle P \rangle$ such that $\dim(\mathcal{R} \cap \mathcal{U}A)$ is maximal

```
set d := 0, A := I_{n×n}
for all v ∈ U \ {0} do
   for all w ∈ R \ {0} do
      compute A' := φ^{-1}(φ(w)φ(v)^{-1})
      compute d' := dim(R ∩ UA)
      if d' > d then set d := d' and A := A'
return A
```

---

Complexity: $\mathcal{O}(q^{k+\dim(\mathcal{R})} n (k + \dim(\mathcal{R}))^2)$ over $\mathbb{F}_q$.

Let $p(x)$ be primitive and $P$ its companion matrix.
$\implies \langle P \rangle$ acts transitively on $\mathbb{F}_q^n$

INPUT: Code $\mathcal{C} = \mathcal{U}\langle P \rangle$, received $\mathcal{R}$
OUTPUT: $A \in \langle P \rangle$ such that $\dim(\mathcal{R} \cap \mathcal{U}A)$ is maximal

```
set d := 0, A := I_{n×n}
for all v ∈ U \ {0} do
   for all w ∈ R \ {0} do
      compute A' := φ^{-1}(φ(w)φ(v)^{-1})
      compute d' := dim(R ∩ UA)
      if d' > d then set d := d' and A := A'
return A
```

Complexity: $\mathcal{O}(q^{k+\dim(\mathcal{R})} n (k + \dim(\mathcal{R}))^2)$ over $\mathbb{F}_q$.

Thank you!