Orbit Codes for Network Coding

Joachim Rosenthal
University of Zürich

EPFL, September 9, 2011

joint work with
Elisa Gorla, Felice Manganiello and Anna-Lena Trautmann
Outline

1. Linear Network Coding
2. Kötter-Kschischang Setting
3. Construction of Spread Codes
4. Orbit codes
Linear Network Coding

Orbit Codes for Network Coding
Setting:

- digraph $\mathcal{G} = (V, E)$ with capacities on the edges.
- the output messages of a channel nodes are linear combinations of input ones.
Question

*Is it possible that both $S_1$ and $S_2$ communicate their messages to both $R_1$ and $R_2$ in only one “round time”?*

Channel setting
Question

Is it possible that both $S_1$ and $S_2$ communicate their messages to both $R_1$ and $R_2$ in only one “round time”?

Traditional communication channel approach:
Throughput is limited by the Max-Flow, Min-Cut Theorem.
Example - Butterfly Network

**Question**

*Is it possible that both $S_1$ and $S_2$ communicate their messages to both $R_1$ and $R_2$ in only one “round time”?*

Linear Network coding approach increases Throughput!
Let $\mathbb{F}_q$ be a finite field and $n, k$ two nonzero natural numbers. Denote by $m_1, \ldots, m_k \in \mathbb{F}_q^n$ the messages transmitted by $k$ different sources. Assume the messages to be linear independent.

$$m_1, \ldots, m_k \rightarrow M = \begin{pmatrix} m_1^t \\ m_2^t \\ \vdots \\ m_k^t \end{pmatrix} \in \text{Mat}_{k \times n}(\mathbb{F}_q) \rightarrow \text{rowsp}(M) \in G(k, \mathbb{F}_q^n)$$

where $G(k, \mathbb{F}_q^n)$ is the Grassmannian of all $k$-dimensional vector subspaces of $\mathbb{F}_q^n$. 
Metric on $\mathcal{P}(n)$

Definition

Denote by $\mathcal{P}(n)$ the set of all linear subspaces inside the vector space $\mathbb{F}_q^n$. 
Metric on $\mathcal{P}(n)$

Definition

Denote by $\mathcal{P}(n)$ the set of all linear subspaces inside the vector space $\mathbb{F}_q^n$.

Definition

On $\mathcal{P}(n)$ define a metric through:

$$d_S(V, W) := \dim(V + W) - \dim(V \cap W).$$
**Metric on $\mathcal{P}(n)$**

**Definition**

Denote by $\mathcal{P}(n)$ the set of all linear subspaces inside the vector space $\mathbb{F}_q^n$.

**Definition**

On $\mathcal{P}(n)$ define a metric through:

$$d_S(V, W) := \dim(V + W) - \dim(V \cap W).$$

**Remark**

Check that the map $d_S : \mathcal{P}(n) \times \mathcal{P}(n) \to \mathbb{N}_+$ defines a metric on $\mathcal{P}(n)$. 
Definition

A subset $C$ of $\mathcal{P}(n)$ will be called a linear network code.
Linear Network Codes

**Definition**

A subset $C$ of $\mathcal{P}(n)$ will be called a linear network code.

**Definition**

In the usual way one defines the distance of the network code $C \subset \mathcal{P}(n)$ through:

$$\text{dist}(C) := \min \{d_S(V, W) | V, W \in C, \ V \neq W\}$$

and the size of $C$ as $M := |C|$. 
Induced Metric on the the Grassmannian $G(k, \mathbb{F}_q^n)$

**Definition**

In the sequel we will assume that a linear network code is a subset of the Grassmannian $G(k, \mathbb{F}_q^n)$. We call such codes also constant-dimension codes.
Induced Metric on the Grassmannian $G(k, \mathbb{F}_q^n)$

**Definition**

In the sequel we will assume that a linear network code is a subset of the Grassmannian $G(k, \mathbb{F}_q^n)$. We call such codes also constant-dimension codes.

**Definition**

The metric on $\mathcal{P}(n)$ induces a metric on the Grassmannian $G(k, \mathbb{F}_q^n)$:

$$d_S(V, W) := \dim(V + W) - \dim(V \cap W)$$
Induced Metric on the the Grassmannian $G(k, \mathbb{F}_q^n)$

**Definition**

*In the sequel we will assume that a linear network code is a subset of the Grassmannian $G(k, \mathbb{F}_q^n)$. We call such codes also constant-dimension codes.*

**Definition**

*The metric on $P(n)$ induces a metric on the Grassmannian $G(k, \mathbb{F}_q^n)$:

$$d_S(V, W) := \dim(V + W) - \dim(V \cap W)$$

**Remark**

*The main constant-dimension linear network coding problem is: For every size $M$ construct codes $C \subset G(k, \mathbb{F}_q^n)$ having maximal possible distance.*
**Errors and Erasures**

*Decoder*: Minimum Distance Decoder (closest codeword given a received vector space).

**Question**

*How do we expect errors and erasures to be?*
Decoder: Minimum Distance Decoder (closest codeword given a received vector space).

Question

How do we expect errors and erasures to be?

- Error $\leftrightarrow$ Increase in dimension.
Errors and Erasures

*Decoder*: Minimum Distance Decoder (closest codeword given a received vector space).

**Question**

*How do we expect errors and erasures to be?*

- Error $\leftrightarrow$ Increase in dimension.
- Erasure $\leftrightarrow$ Decrease in dimension.
Fundamental Research Questions

- For every finite field and positive integers $d, k, n$ find the maximum number of subspaces in the Grassmannian $G(k, \mathbb{F}_q^n)$ such that this code has distance $d$. 
Fundamental Research Questions

- For every finite field and positive integers $d, k, n$ find the maximum number of subspaces in the Grassmannian $G(k, \mathbb{F}_q^n)$ such that this code has distance $d$.

- Find constructions of codes together with efficient decoding algorithms.
Question: What is the algebraic structure of the balls of radius $t$ around an element $W \in \text{Grass}(k, V)$?
Question: What is the algebraic structure of the balls of radius $t$ around an element $W \in \text{Grass}(k, V)$?

Answer: $d(U, W) \leq t$ if and only if $\dim(U \cap W) \geq k - t/2 =: r$. 
What is the algebraic structure of balls of radius $t$ around an element $W \in \text{Grass}(k, V)$?

**Answer:** $d(U, W) \leq t$ if and only if $\dim(U \cap W) \geq k - t/2 =: r$.

**Remark**

The ball of radius $t$ around the subspace $W$ defines a so called Schubert variety:

$$\{ U \in \text{Grass}(k, V) \mid \dim(U \cap W) \geq r \}$$
Schubert Varieties

Definition

A flag $\mathcal{F}$ is a sequence of nested subspaces

$$\{0\} \subset V_1 \subset V_2 \subset \ldots \subset V_n = V$$

(1)

where we assume that $\dim V_i = i$ for $i = 1, \ldots, n$.

Let $\underline{i} = (i_1, \ldots, i_k)$ denote a sequence of numbers having the property that

$$1 \leq i_1 < \ldots < i_k \leq n.$$  

(2)

Definition

For each flag $\mathcal{F}$ and each multiindex $\underline{i}$ a Schubert variety is defined through:

$$S(\underline{i}; \mathcal{F}) := \{ W \in \text{Grass}(k, V) \mid \dim(W \cap V_{i_s}) \geq s, s = 1, \ldots, k \}$$
Remark

If \( \{e_1, \ldots, e_n\} \) is a basis of \( V \) and \( \mathcal{F} \) is the standard flag with respect to this basis then \( S(i; \mathcal{F}) \) consists of the closure of all subspaces having a certain row reduced echelon form:

\[
\begin{bmatrix}
* & \cdots & * & 1 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\
* & \cdots & * & 0 & * & \cdots & * & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
* & \cdots & * & 0 & * & \cdots & * & 0 & \cdots & * & \cdots & * & 1 & 0 & \cdots & 0
\end{bmatrix}
\]
Example of Schubert Calculus

Example

Given 4 lines in 3-space in general position. Is there a line intersecting all 4 lines.
Example of Schubert Calculus

Example

Given 4 lines in 3-space in general position. Is there a line intersecting all 4 lines.

**Geometric Problem:** Intersection of Schubert varieties of the form $S(2, 4)$ inside the Grassmannian $\text{Grass}(2, \mathbb{F}^4)$. 
Example of Schubert Calculus

**Example**

Given 4 lines in 3-space in general position. Is there a line intersecting all 4 lines.

**Geometric Problem:** Intersection of Schubert varieties of the form \( S(2, 4) \) inside the Grassmannian \( \text{Grass}(2, \mathbb{F}^4) \).

**Algebraic Problem:** One has the equation of \( \text{Grass}(2, \mathbb{F}^4) \):

\[
x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23} = 0
\]

together with 4 linear equations describing the 4 Schubert varieties. \( \mapsto 2 \) Solutions.
Given 4 lines in 3-space in general position. Is there a line intersecting all 4 lines.

**Geometric Problem:** Intersection of Schubert varieties of the form $S(2, 4)$ inside the Grassmannian $\text{Grass}(2, \mathbb{F}^4)$.

**Algebraic Problem:** One has the equation of $\text{Grass}(2, \mathbb{F}^4)$:

$$x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23} = 0$$

together with 4 linear equations describing the 4 Schubert varieties. $\mapsto 2$ Solutions.
Definition

$S \subset G(k, \mathbb{F}_q^n)$ is a spread of $\mathbb{F}_q^n$ if:

- $V \cap W = \{0\}$ for all $V, W \in S$, and
- for any $v \in \mathbb{F}_q^n$, $v \neq 0$, exists unique $V \in S$ such that $v \in V$. 

Spread and Spread codes of $\mathbb{F}_q^n$
Spread and Spread codes of $\mathbb{F}_q^n$

**Definition**

$S \subset G(k, \mathbb{F}_q^n)$ is a spread of $\mathbb{F}_q^n$ if:

- $V \cap W = \{0\}$ for all $V, W \in S$, and
- for any $v \in \mathbb{F}_q^n$, $v \neq 0$, exists unique $V \in S$ such that $v \in V$.  

**Question**

*Spreads exist for every choice of $k$ and $n$?*
Spread and Spread codes of $\mathbb{F}_q^n$

**Definition**

$S \subset \text{G}(k, \mathbb{F}_q^n)$ is a spread of $\mathbb{F}_q^n$ if:

- $V \cap W = \{0\}$ for all $V, W \in S$, and
- for any $v \in \mathbb{F}_q^n, v \neq 0$, exists unique $V \in S$ such that $v \in V$.

**Question**

Spreads exist for every choice of $k$ and $n$?

**Theorem**

There exists a spread $S \subset \text{G}(k, \mathbb{F}_q^n)$ if and only if $k \mid n$. 

University of Zurich
Remark

\( k \)-dim subspaces in \( \mathbb{F}_q^n \) \( \xrightarrow{1-1} \) \( (k - 1) \)-dim subspaces in \( \mathbb{P}^{n-1}_{\mathbb{F}_q} \).

It follows \( G(k, \mathbb{F}_q^n) \cong G(k - 1, \mathbb{P}^{n-1}_{\mathbb{F}_q}) \).

Definition

\( S \subset G(k - 1, \mathbb{P}^{n-1}_{\mathbb{F}_q}) \) is a spread of \( \mathbb{P}^{n-1}_{\mathbb{F}_q} \) if:

- \( V \cap W = \emptyset \) for all \( V, W \in S \), and
- \( \bigcup_{V \in S} V = \mathbb{P}^{n-1}_{\mathbb{F}_q} \).
Spreads in Projective Geometry [Hirschfeld 98]

**Remark**

$k$-dim subspaces in $\mathbb{F}_q^n \leftrightarrow (k - 1)$-dim subspaces in $\mathbb{P}_{\mathbb{F}_q}^{n-1}$.

It follows $G(k, \mathbb{F}_q^n) \cong G(k - 1, \mathbb{P}_{\mathbb{F}_q}^{n-1})$.

**Definition**

$S \subset G(k - 1, \mathbb{P}_{\mathbb{F}_q}^{n-1})$ is a spread of $\mathbb{P}_{\mathbb{F}_q}^{n-1}$ if:

- $V \cap W = \emptyset$ for all $V, W \in S$, and
- $\bigcup_{V \in S} V = \mathbb{P}_{\mathbb{F}_q}^{n-1}$.

**Theorem**

There exists a spread $S \subset G(k - 1, \mathbb{P}_{\mathbb{F}_q}^{n-1})$ if and only if $k \mid n$. 
Spread Codes

Setting:

- \( n, k, r \in \mathbb{N}_+ \) such that \( n = kr \);
- \( p \in \mathbb{F}_q[x] \) irreducible of degree \( k \) and \( P \in \text{Mat}_{k \times k}(\mathbb{F}_q) \) its companion matrix;
- \( \mathbb{F}_q[P] \subset \text{GL}_k(\mathbb{F}_q), \mathbb{F}_q[P] \cong \mathbb{F}_{q^k} \).
Spread Codes

Setting:
- \( n, k, r \in \mathbb{N}_+ \) such that \( n = kr \);
- \( p \in \mathbb{F}_q[x] \) irreducible of degree \( k \) and \( P \in \text{Mat}_{k \times k}(\mathbb{F}_q) \) its companion matrix;
- \( \mathbb{F}_q[P] \subset GL_k(\mathbb{F}_q) \), \( \mathbb{F}_q[P] \cong \mathbb{F}_{q^k} \).

**Theorem**

*The collection of subspaces*

\[
S := \bigcup_{i=1}^{r} \{ \text{rowsp} [0_k \cdots 0_k l_k A_{i+1} \cdots A_r] \mid A_{i+1}, \ldots, A_r \in \mathbb{F}_q[P] \}
\]

is a subset of \( G(k, \mathbb{F}_q^n) \) and a spread of \( \mathbb{F}_q^n \).
Definition

The set $S$ constructed as in the previous slide will be called a Spread Codes of $G(k, \mathbb{F}_q^n)$. 
Definition

The set $S$ constructed as in the previous slide will be called a Spread Codes of $G(k, \mathbb{F}_q^n)$.

Properties:

- MDS-like for the distance $d = 2k$.
- every nonzero vector of $\mathbb{F}_q^n$ belong to one and only one codeword.
Orbit codes

$GL_n(\mathbb{F}_q)$ (right) action on Grassmannians:

$$\text{Grass}(k, n) \times GL_n(\mathbb{F}_q) \rightarrow \text{Grass}(k, n)$$

$$(U, A) \mapsto U \cdot A := \text{rowsp}(U \cdot A)$$

Proposition

Let $U, V \in \text{Grass}(k, n)$. Then

$$d(U, V) = d(U \cdot A, V \cdot A) \quad \forall A \in GL_n(\mathbb{F}_q).$$
Orbit codes

$GL_n(\mathbb{F}_q)$ (right) action on Grassmannians:

$$\text{Grass}(k, n) \times GL_n(\mathbb{F}_q) \rightarrow \text{Grass}(k, n)$$

$$(U, A) \mapsto U \cdot A := \text{rowsp}(U \cdot A)$$

Proposition

Let $U, V \in \text{Grass}(k, n)$. Then

$$d(U, V) = d(U \cdot A, V \cdot A) \quad \forall A \in GL_n(\mathbb{F}_q).$$

Definition (orbit codes)

Let $U \in \text{Grass}(k, n)$ and $\mathcal{G} < GL_n(\mathbb{F}_q)$. An orbit code is

$$\mathcal{C} = \{U \cdot A \mid A \in \mathcal{G}\}.$$
Definition

- Let $\mathcal{U} \in \text{Grass}(k, n)$. The stabilizer of $\mathcal{U}$ is
  \[ \text{Stab}(\mathcal{U}) := \{ A \in GL_n(F_q) \mid \mathcal{U} = \mathcal{U} \cdot A \} . \]

- Let $A, B \in GL_n(F_q)$. Then
  \[ A \sim B : \iff \exists S \in \text{Stab}(\mathcal{U}) : A = SB . \]

Theorem

Let $\mathcal{U} \in \text{Grass}(k, n)$. Then
\[ \text{Grass}(k, n) \cong GL_n(F_q)/\text{Stab}(\mathcal{U}) . \]
Cyclic orbit codes

\[ \text{GL}_n(\mathbb{F}_q) \xrightarrow{\pi} \text{GL}_n(\mathbb{F}_q)/\text{Stab}(\mathcal{U}) \longleftrightarrow \text{Grass}(k, n) \]

**Proposition**

Let \( \mathcal{G}_1, \mathcal{G}_2 < \text{GL}_n \). Then

\[ \pi(\mathcal{G}_1) = \pi(\mathcal{G}_2) \iff C_{\mathcal{G}_1} = C_{\mathcal{G}_2}. \]

**Definition**

An orbit code \( C \) is cyclic if there exists \( \mathcal{G} < \text{GL}_n(\mathbb{F}_q) \) cyclic defining it.
Let $\mathcal{G} < GL_n(\mathbb{F}_q)$. Then

- $|C| = \frac{|\mathcal{G}|}{|\mathcal{G} \cap \text{Stab}(U)|}$.
- $d_{\text{min}} = \min_{A \in \mathcal{G} \setminus \text{Stab}(U)} d(U, U \cdot A)$.
- $C^\perp := \{ U^\perp \in \text{Grass}(n-k, n) \mid U \in C \}$ is an orbit code.
Proposition

Let $\mathcal{U}, \mathcal{V} \in \text{Grass}(k, n)$ and $M \in \text{GL}_n(\mathbb{F}_q)$ such that $\mathcal{V} = \mathcal{U} \cdot M$. Then

$$\text{Stab}(\mathcal{V}) = M^{-1}\text{Stab}(\mathcal{U})M,$$
Let $\mathcal{U}, \mathcal{V} \in \text{Grass}(k, n)$ and $M \in \text{GL}_n(\mathbb{F}_q)$ such that $\mathcal{V} = \mathcal{U} \cdot M$. Then

$$\text{Stab}(\mathcal{V}) = M^{-1}\text{Stab}(\mathcal{U})M,$$

$$\downarrow$$

$$\text{Stab}(\text{rowsp}[I \ 0]) = \left\{ \begin{pmatrix} A_1 & 0 \\ A_2 & A_3 \end{pmatrix} \bigg| A_1 \in \text{GL}_k(\mathbb{F}_q), A_3 \in \text{GL}_{n-k}(\mathbb{F}_q) \right\}$$

$$\downarrow$$

$$\mathcal{C} = \{\mathcal{U} \cdot A \mid A \in \mathcal{G}\} \quad \rightarrow \quad \mathcal{C} = \{\text{rowsp}[I \ 0] \cdot A \mid A \in \tilde{\mathcal{G}}\}$$
Linear Network Coding
Kötter-Kschischang Setting
Construction of Spread Codes
Orbit codes

Spread codes as cyclic orbit codes

Lemma

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 $1, \alpha^c, \ldots, \alpha^{(k-1)c}$ is equal to

$\{\alpha^{ic} | i = 0, \ldots, q^k - 2\} \cup \{0\} = \mathbb{F}_{q^k}$. 
### Lemma

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 $1, \alpha^c, \ldots, \alpha^{(k-1)c}$ is equal to $\{\alpha^{ic} | i = 0, \ldots, q^k - 2\} \cup \{0\} = \mathbb{F}_{q^k}$.

### Proof.

Since $k | n$ it holds that $c \in \mathbb{N}$. Moreover it holds that $(\alpha^c)^{q^k - 1} = \alpha^{q^n - 1} = 1$ and $(\alpha^c)^{q^k - 2} = \alpha^{-c} \neq 1$, hence the order of $\alpha^c$ is $q^k - 1$. It is well-known that if $k$ divides $n$ the field $\mathbb{F}_{q^n}$ has exactly one subfield $\mathbb{F}_{q^k}$. Thus the group generated by $\alpha^c$ has to be $\mathbb{F}_{q^k} \setminus \{0\}$, which again is isomorphic to $\mathbb{F}_q^k$ as a vector space. \qed
Let $\alpha$ be a primitive of $\mathbb{F}_{q^n}$ and assume $k|n$ and $c := \frac{q^n - 1}{q^k - 1}$. Consider the $\mathbb{F}_q$-subspace $\mathbb{F}_{q^k} = \{\alpha^{ic} | i = 0, \ldots, q^k - 2\} \cup \{0\}$.

**Lemma**

*For every $\beta \in \mathbb{F}_{q^n}$ the set*

$$\beta \cdot \mathbb{F}_{q^k} = \{\beta \alpha^{ic} | i = 0, \ldots, q^k - 2\} \cup \{0\}$$

*defines an $\mathbb{F}_q$-subspace of dimension $k$.***
Let $\alpha$ be a primitive of $\mathbb{F}_{q^n}$ and assume $k|n$ and $c := \frac{q^n-1}{q^k-1}$.
Consider the $\mathbb{F}_q$-subspace $\mathbb{F}_{q^k} = \{\alpha^{ic} | i = 0, \ldots, q^k - 2\} \cup \{0\}$.

**Lemma**

*For every $\beta \in \mathbb{F}_{q^n}$ the set*

$$\beta \cdot \mathbb{F}_{q^k} = \{\beta \alpha^{ic} | i = 0, \ldots, q^k - 2\} \cup \{0\}$$

*defines an $\mathbb{F}_q$-subspace of dimension $k$.*

**Proof.**

$$\varphi_\beta : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}, \ u \longmapsto \beta u$$

is an $\mathbb{F}_q$-linear isomorphism, $\varphi_\beta(\mathbb{F}_{q^k}) = \beta \cdot \mathbb{F}_{q^k}$ is hence an $\mathbb{F}_q$-linear subspace of dimension $k$. 
The set

\[ S = \{ \alpha^i \cdot \mathbb{F}_{q^k} \mid i = 0, \ldots, c - 1 \} \]

defines a spread code.
Spread codes as cyclic orbit codes

**Theorem**

The set

\[ S = \{ \alpha^i \cdot \mathbb{F}_{q^k} \mid i = 0, \ldots, c - 1 \} \]

defines a spread code.

**Proof.**

It is enough to show that the subspace \( \alpha^i \cdot \mathbb{F}_{q^k} \) and \( \alpha^j \cdot \mathbb{F}_{q^k} \) are pairwise disjoint whenever \( 0 \leq i < j \leq c - 1 \). For this assume that there are field elements \( c_i, c_j \in \mathbb{F}_{q^k} \), such that

\[ v = \alpha^i c_i = \alpha^j c_j \in \alpha^i \cdot \mathbb{F}_{q^k} \cap \alpha^j \cdot \mathbb{F}_{q^k}. \]

If \( v \neq 0 \) then \( \alpha^{i-j} = c_j c_i^{-1} \in \mathbb{F}_{q^k} \). But this means \( i - j \equiv 0 \mod c \) and \( \alpha^i \cdot \mathbb{F}_{q^k} = \alpha^j \cdot \mathbb{F}_{q^k} \). It follows that \( S \) is a spread.
Theorem

Let $p(x)$ be an irreducible polynomial over $\mathbb{F}_q$ of degree $n$ and $P$ its companion matrix. Furthermore let $\alpha \in \mathbb{F}_{q^n}$ be a root of $p(x)$ and $\phi$ be the canonical homomorphism

$$\phi : \mathbb{F}_q^n \rightarrow \mathbb{F}_{q^n}, \ (v_1, \ldots, v_n) \mapsto \sum_{i=1}^{n} v_i \alpha^{i-1}$$

Then the following diagram commutes (for $v \in \mathbb{F}_q^n$):

$$
\begin{array}{c}
v \xrightarrow{\cdot P} vP \\
\phi \downarrow \quad \quad \downarrow \phi \\
v' \xrightarrow{\cdot \alpha} v' \alpha
\end{array}
$$
Example 1

Over the binary field let $p(x) := x^6 + x + 1$ primitive, $\alpha$ a root of $p(x)$ and $P$ its companion matrix. For the 3-dimensional spread compute $c = \frac{63}{7} = 9$ and construct a basis for the starting point of the orbit:

$$u_1 = \phi^{-1}(1) = (100000)$$
$$u_2 = \phi^{-1}(\alpha^9) = \phi^{-1}(\alpha^4 + \alpha^3) = (000110)$$
$$u_3 = \phi^{-1}(\alpha^{18}) = \phi^{-1}(\alpha^3 + \alpha^2 + \alpha + 1) = (111100)$$

The starting point is

$$U = \text{rowsp} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} = \text{rowsp} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

and the orbit of the group generated by $P$ on $U$ is a spread code.
Example 2

For the 2-dimensional spread compute \( c = \frac{63}{3} = 21 \) and construct the starting point

\[
\begin{align*}
u_1 &= \phi^{-1}(1) = (100000) \\
u_2 &= \phi^{-1}(\alpha^{21}) = \phi^{-1}(\alpha^2 + \alpha + 1) = (111000)
\end{align*}
\]

The starting point is

\[
U = \text{rowsp} \left[ \begin{array}{ccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{array} \right] = \text{rowsp} \left[ \begin{array}{ccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \end{array} \right]
\]

and the orbit of the group generated by \( P \) is a spread code.


D. Silva, F.R. Kschischang, and R. Kötter.
A rank-metric approach to error control in random network coding.

Orbit codes - a new concept in the area of network coding.

New improvements on the echelon-ferrers construction.
Thank you for your attention.