Subspace Codes and Orbit Codes

Joachim Rosenthal
University of Zürich

Hong Kong University, December 12, 2013

joint work with
Elisa Gorla, Felice Manganiello, Kyle Marshall
Natalia Silberstein and Anna-Lena Trautmann
Outline

1. Kötter-Kschischang Setting
2. List decoding, a problem in Schubert calculus
3. Relation to Rank Matrix Codes
4. Construction of Spread and Orbit Codes
Traditional Communication Channel
Setting:
- Communication between single source and sink.
- In the channel messages are forwarded.
Traditional Communication Channel

Setting:
- Communication between single source and sink.
- In the channel messages are forwarded.

Question

*Why do we consider only communications between single entities? Is it natural?*
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!
Linear Network Coding
Linear Network Coding

sources  other nodes  sinks
Setting:

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

source  channel  receivers
Kötter-Kschischang Setting
List decoding, a problem in Schubert calculus
Relation to Rank Matrix Codes
Construction of Spread and Orbit Codes

Single User many Receivers

source other nodes receivers
What is Network Coding useful for?

- P2P file exchanges over the Internet,
What is Network Coding useful for?

- P2P file exchanges over the Internet,
- Data Streaming over Wireless Networks,
What is Network Coding useful for?

- P2P file exchanges over the Internet,
- Data Streaming over Wireless Networks,
- Network security:
  1. prevents an eavesdropper from recovering messages,
  2. against the modification of packets by an attacker,
What is Network Coding useful for?

- P2P file exchanges over the Internet,
- Data Streaming over Wireless Networks,
- Network security:
  1. prevents an eavesdropper from recovering messages,
  2. against the modification of packets by an attacker,
- others.
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 $\mathbb{F}_q^n$. 
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: $d_s : \mathcal{P}(n) \times \mathcal{P}(n) \rightarrow \mathbb{N}_+$ defines a metric on $\mathcal{P}(n)$. 
Subspace Codes for Linear Network Codes

Definition

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

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

Definition

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

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

and the size of $C$ as $M := |C|$. 
Subspace Codes for Linear Network Codes

Definition

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

Definition

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

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

and the size of $C$ as $M := |C|$.

Remark

In the usual way one has the goal to construct for any natural numbers $n, M$ and any finite field $\mathbb{F}_q$ codes having maximal distance $d$ and efficient decoding algorithms.
Definition

In the sequel we will assume that a subspace 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 subspace 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 subspace 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 $G(k, \mathbb{F}_q^n)$:

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

**Remark**

The main constant-dimension subspace 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?*
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.
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* ↔ *Increase in dimension*.
- *Erasure* ↔ *Decrease in dimension*. 
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.
List Decoding Problem

Given a subspace code $\mathcal{C} \subseteq \text{Grass}(k, V)$ and a received subspace $W \subseteq V$, whose dimension is not necessarily $k$. 
List Decoding Problem

Given a subspace code $C \subset \text{Grass}(k, V)$ and a received subspace $W \subset V$, whose dimension is not necessarily $k$.

Consider a fixed distance parameter $t$ and the set.

$$S_W := \{ U \in \text{Grass}(k, V) \mid d(U, W) \leq t \}$$
List Decoding Problem

Given a subspace code $C \subset \text{Grass}(k, V)$ and a received subspace $W \subset V$, whose dimension is not necessarily $k$.

Consider a fixed distance parameter $t$ and the set.

$$S_W := \{ U \in \text{Grass}(k, V) \mid d(U, W) \leq t \}$$

The list decoding problem asks for efficient methods to compute:

$$S_W \cap C$$
List Decoding Problem

Given a subspace code $\mathcal{C} \subset \text{Grass}(k, V)$ and a received subspace $W \subset V$, whose dimension is not necessarily $k$.

Consider a fixed distance parameter $t$ and the set.

$$S_W := \{ U \in \text{Grass}(k, V) \mid d(U, W) \leq t \}$$

The list decoding problem asks for efficient methods to compute:

$$S_W \cap \mathcal{C}$$

Nota Bene: It will turn out that the problem of list decoding is an intersection problem between the Schubert variety $S_W$ and the subspace code $\mathcal{C} \subset \text{Grass}(k, V)$. 
Hermann Schubert studied in the 19th century geometric questions of the following type:
Hermann Schubert studied in the 19th century geometric questions of the following type:

**Example**

Given 4 lines in 3-space in general position. Is there a line intersecting all 4 lines.
Hermann Schubert studied in the 19th century geometric questions of the following type:

**Example**

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

**Answer Schubert:** By Poncelet's principle of conservation of numbers we can assume lines 1 and 2 intersect and lines 3 and 4 intersect. So there are 2 solutions in general.
A Result of Schubert

Theorem (Schubert [2])

Given \( N := k(n - k) \) linear subspace \( U_i, i = 1, \ldots, N \) in \( V \) having dimension \( k \) each. If the base field \( \mathbb{F} \) is algebraically closed and the subspaces are in general position then there exist exactly

\[
\frac{1!2! \cdots (k - 1)!(N)!}{(n - k)!(n - k + 1)! \cdots (n - 1)!}
\]

subspaces \( W \) of dimension \( (n - k) \) intersecting each of the subspaces \( U_i \) nontrivially.
Kötter-Kschischang Setting
List decoding, a problem in Schubert calculus
Relation to Rank Matrix Codes
Construction of Spread and Orbit Codes

Hermann Cäsar Hannibal Schubert (1848-1911)

Hermann Cäsar Hannibal Schubert (1848-1911)
A flag $\mathcal{F}$ is a sequence of nested subspaces

$$\{0\} \subset V_1 \subset V_2 \subset \ldots \subset V_n = V \quad (2)$$

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

Definition

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

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

(2)

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

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

(3)
A flag $\mathcal{F}$ is a sequence of nested subspaces

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

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

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

For each flag $\mathcal{F}$ and each multiindex $\underline{i}$

$$S(\underline{i}; \mathcal{F}) := \{ W \in \text{Grass}(k, V) \mid \dim(W \bigcap V_{i_s}) \geq s \}$$
Central Question of Schubert Calculus

Problem

Given two Schubert varieties $S(\nu; \mathcal{F})$ and $S(\tilde{\nu}; \tilde{\mathcal{F}})$. Describe as explicitly as possible the intersection variety

$$S(\nu; \mathcal{F}) \cap S(\tilde{\nu}; \tilde{\mathcal{F}}).$$
Hilbert Problem Number 15, Paris 1900
Rigorous foundation of Schubert’s enumerative calculus

The problem consists in this: To establish rigorously and with an exact determination of the limits of their validity those geometrical numbers which Schubert especially has determined on the basis of the so-called principle of special position, or conservation of number, by means of the enumerative calculus developed by him. Although the algebra of today guarantees, in principle, the possibility of carrying out the processes of elimination, yet for the proof of the theorems of enumerative geometry decidedly more is requisite, namely, the actual carrying out of the process of elimination in the case of equations of special form in such a way that the degree of the final equations and the multiplicity of their solutions may be foreseen.
Kötter-Kschischang Setting
List decoding, a problem in Schubert calculus
Relation to Rank Matrix Codes
Construction of Spread and Orbit Codes

David Hilbert (1862-1943)
Consider the vector space of alternating $k$–tensors $\wedge^k V$. Let $\mathbb{P}(\wedge^k V)$ be the projective space consisting of all lines in $\wedge^k V$. 
Consider the vector space of alternating $k$–tensors $\wedge^k V$. Let $\mathbb{P}(\wedge^k V)$ be the projective space consisting of all lines in $\wedge^k V$. The Plücker embedding is defined through:

$$\varphi : \text{Grass}(k, V) \longrightarrow \mathbb{P}(\wedge^k V)$$

$$\text{span}(v_1, \ldots, v_k) \longmapsto \mathbb{F}v_1 \wedge \cdots \wedge v_k.$$
Assume

\[ v_i = \sum_{j=1}^{n} a_{ij} e_j, \quad i = 1, \ldots, k. \]

Let \( A \) be the \( k \times n \) matrix \((a_{i,j})\). The Plücker embedding writes:

\[ \varphi : \text{Mat}_{k \times n} \longrightarrow \mathbb{P}(\wedge^k V) \]

\[ \text{rowspace}(A) \longmapsto \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1,\ldots,i_k} \cdot e_{i_1} \wedge \ldots \wedge e_{i_k}. \]

The coordinates \( x_i := x_{i_1,\ldots,i_k} \) are called the Plücker coordinates of \( \text{rowspace}(A) \).
Theorem

\[ \sum_{\lambda=1}^{k+1} (-1)^{\lambda} \cdot x_{i_1, \ldots, i_{k-1}, j_\lambda} \cdot x_{j_1, \ldots, j_{\lambda}, \ldots, j_{k+1}} = 0 \]  

describes the image of the Grassmannian in the projective space \( \mathbb{P}(\wedge^k V) \).
Shuffle Relations

**Theorem**

\[
\sum_{\lambda=1}^{k+1} (-1)^\lambda \cdot x_{i_1,\ldots,i_{k-1},j_\lambda} \cdot x_{j_1,\ldots,j_\lambda,\ldots,j_{k+1}} = 0
\]

(6)

*describes the image of the Grassmannian in the projective space* \(\mathbb{P}(\wedge^k V)\)

**Example**

Grass(2, \(\mathbb{F}^4\)) is embedded in \(\mathbb{P}^5\) and \(\varphi(\text{Grass}(2, 4))\) is described by a single relation

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

(7)
Example

Grass(2, \mathbb{F}^5) is embedded in \mathbb{P}^9 and the defining relations are:

\begin{align*}
x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23} &= 0 \\
x_{12}x_{35} - x_{13}x_{25} + x_{15}x_{23} &= 0 \\
x_{12}x_{45} - x_{14}x_{25} + x_{15}x_{14} &= 0 \\
x_{13}x_{45} - x_{14}x_{35} + x_{15}x_{34} &= 0 \\
x_{23}x_{45} - x_{24}x_{35} + x_{25}x_{34} &= 0
\end{align*}
Bruhat order:
Let \( i := (i_1, \ldots, i_k) \) and \( j := (j_1, \ldots, j_k) \) be two set of indices satisfying
\[
1 \leq i_1 < \ldots < i_k \leq n
\]
respectively
\[
1 \leq j_1 < \ldots < j_k \leq n.
\]
Then one defines:
\[
i \leq j
\]
if and only if \( i_t \leq j_t \) for \( t = 1, \ldots, k \).
Bruhat order:
Let \( \underline{i} := (i_1, \ldots, i_k) \) and \( \underline{j} := (j_1, \ldots, j_k) \) be two set of indices satisfying
\[
1 \leq i_1 < \ldots < i_k \leq n
\]
respectively
\[
1 \leq j_1 < \ldots < j_k \leq n.
\]
Then one defines:
\[
\underline{i} \leq \underline{j}
\]
if and only if \( i_t \leq j_t \) for \( t = 1, \ldots, k \).

Theorem

The defining equations in terms of Plücker coordinates of the Schubert variety \( S(\underline{i}; \mathcal{F}) \) are given by the quadratic shuffle relations together with the linear equations \( x_{\underline{j}} = 0 \) for all \( \underline{j} \not\leq \underline{i} \).
List Decoding Problem

Given a subspace code $\mathcal{C} \subset \text{Grass}(k, V)$ and a received subspace $\mathcal{W} \subset V$, whose dimension is not necessarily $k$. 
List Decoding Problem

Given a subspace code $C \subset \text{Grass}(k, V)$ and a received subspace $W \subset V$, whose dimension is not necessarily $k$.

Consider the Schubert variety.

$$S_W := \{ U \in \text{Grass}(k, V) \mid d(U, W) \leq t \}$$
List Decoding Problem

Given a subspace code $\mathcal{C} \subset \text{Grass}(k, V)$ and a received subspace $W \subset V$, whose dimension is not necessarily $k$.

Consider the Schubert variety.

$$S_W := \{ U \in \text{Grass}(k, V) \mid d(U, W) \leq t \}$$

Find efficient methods to compute:

$$S_W \cap \mathcal{C}$$
List Decoding Problem

Given a subspace code $C \subseteq \text{Grass}(k, V)$ and a received subspace $W \subseteq V$, whose dimension is not necessarily $k$.

Consider the Schubert variety.

$$S_W := \{ U \in \text{Grass}(k, V) \mid d(U, W) \leq t \}$$

Find efficient methods to compute:

$$S_W \cap C$$

We could show how to efficiently describe the equations for the variety $S_W$. 

Subspace Codes and Orbit Codes
In 1978 Delsarte introduced a class of codes called *rank matrix codes*. 
In 1978 Delsarte introduced a class of codes called *rank matrix codes*.

**Definition**

On the set $\mathbb{F}^{k \times m}$ consisting of all $k \times m$ matrices over $\mathbb{F}$ define the rank distance:

$$d_R(X, Y) := \text{rank}(X - Y)$$
In 1978 Delsarte introduced a class of codes called *rank matrix codes*.

**Definition**

On the set $\mathbb{F}^{k \times m}$ consisting of all $k \times m$ matrices over $\mathbb{F}$ define the rank distance:

$$d_R(X, Y) := \text{rank}(X - Y)$$

**Remark**

$d_R(X, Y)$ is a metric.
In 1978 Delsarte introduced a class of codes called *rank matrix codes*. 

**Definition**

*On the set* $\mathbb{F}^{k \times m}$ *consisting of all* $k \times m$ *matrices over* $\mathbb{F}$ *define the rank distance:*

$$d_R(X, Y) := \text{rank}(X - Y)$$

**Remark**

$d_R(X, Y)$ *is a metric.*

**Remark**

*Gabidulin provided several constructions and decoding algorithms of rank metric codes with good distances.*
Rank distance and subspace distance

The rank distance and the subspace distance are related through the following theorem:
The rank distance and the subspace distance are related through the following theorem:

**Theorem**

Let $X, Y \in \mathbb{F}^{k \times m}$ and let $V := \text{rowsp}[I_k \ X]$ and $W := \text{rowsp}[I_k \ Y]$. Then

$$d_S(V, W) = 2d_R(X, Y).$$
The rank distance and the subspace distance are related through the following theorem:

**Theorem**

Let $X, Y \in \mathbb{F}^{k \times m}$ and let

$$V := \text{rowsp}[I_k X]$$

and

$$W := \text{rowsp}[I_k Y].$$

Then

$$d_S(V, W) = 2d_R(X, Y).$$

**Remark**

The map

$$\phi : \mathbb{F}^{k \times m} \rightarrow G(k, \mathbb{F}_q^{k+m}), \ X \mapsto \text{rowsp}[I_k X]$$

defines an embedding and one sometimes calls the image the thick open cell of the Grassmannian.
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 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 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 $n$?

**Theorem**

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

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

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

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

Theorem

There exists a spread $S \subset G(k - 1, \mathbb{P}^{n-1}_{\mathbb{F}_q})$ 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 \( P \in Mat_{k \times k}(\mathbb{F}_q) \) its companion matrix;
- \( \mathbb{F}_q[P] \subset GL_k(\mathbb{F}_q), \mathbb{F}_q[P] \cong \mathbb{F}_{q^k}. \)
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*

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

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

$GL_n(F_q)$ (right) action on Grassmannians:

$G(k, n) \times GL_n(F_q) \rightarrow G(k, n) \quad (U, A) \mapsto U \cdot A := \text{rowsp}(U \cdot A)$

**Proposition**

Let $U, V \in G(k, n)$. Then

$$d(U, V) = d(U \cdot A, V \cdot A) \quad \forall A \in GL_n(F_q).$$
Orbit codes

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

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

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

**Proposition**

Let $U, V \in G(k, n)$. Then

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

**Definition (orbit codes)**

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

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

Let $\mathcal{U} \in \mathcal{G}(k, n)$. The stabilizer of $\mathcal{U}$ is

$$\text{Stab}(\mathcal{U}) := \{A \in GL_n(\mathbb{F}_q) \mid \mathcal{U} = \mathcal{U} \cdot A\}.$$ 

Theorem

Let $\mathcal{U} \in \mathcal{G}(k, n)$. Then

$$\mathcal{G}(k, n) \cong GL_n(\mathbb{F}_q)/\text{Stab}(\mathcal{U}).$$
Cyclic orbit codes

\[
GL_n(\mathbb{F}_q) \xrightarrow{\pi} GL_n(\mathbb{F}_q)/\text{Stab}(U) \leftrightarrow G(k, n)
\]

**Proposition**

Let \( \mathcal{G}_1, \mathcal{G}_2 \subset GL_n \). 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 \( \mathcal{G} \subset GL_n(\mathbb{F}_q) \) cyclic defining it.
“Linearity” of orbit codes

Let $\mathcal{G} < \text{GL}_n(\mathbb{F}_q)$. Then

- $|C| = \frac{|\mathcal{G}|}{|\mathcal{G} \cap \text{Stab}(U)|}$.
- $d_{\text{min}} = \min_{A \in \mathcal{G} \setminus \text{Stab}(U)} d(U, U \cdot A)$.
- $C^\perp := \{U^\perp \in \mathcal{G}(n - k, n) \mid U \in C\}$ is an orbit code.
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
\[
\{\alpha^{ic} | i = 0, \ldots, q^k - 2\} \cup \{0\} = \mathbb{F}_{q^k}.
\]

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 $k$.
The set
\[ S = \{ \alpha^i \cdot \mathbb{F}_q^k \mid i = 0, \ldots, c - 1 \} \]
defines a spread code.
The set
\[ S = \{ \alpha^i \cdot F_{q^k} \mid i = 0, \ldots, c - 1 \} \]
defines a spread code.

Proof.

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

\[ \nu = \alpha^i c_i = \alpha^j c_j \in \alpha^i \cdot F_{q^k} \cap \alpha^j \cdot F_{q^k}. \]

If \( \nu \neq 0 \) then \( \alpha^{i-j} = c_j c_i^{-1} \in F_{q^k} \). But this means \( i - j \equiv 0 \) mod \( c \) and \( \alpha^i \cdot F_{q^k} = \alpha^j \cdot F_{q^k} \). It follows that \( S \) is a spread.
Translation into matrix setting

**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

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

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

\[
\begin{array}{ccc}
v & \xrightarrow{\cdot P} & vP \\
\phi & \downarrow & \downarrow \phi \\
v' & \xrightarrow{\cdot \alpha} & v' \alpha
\end{array}
\]
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:

\[
\begin{align*}
    u_1 &= \phi^{-1}(1) = (100000) \\
    u_2 &= \phi^{-1}(\alpha^9) = \phi^{-1}(\alpha^4 + \alpha^3) = (000110) \\
    u_3 &= \phi^{-1}(\alpha^{18}) = \phi^{-1}(\alpha^3 + \alpha^2 + \alpha + 1) = (111100)
\end{align*}
\]

The starting point is

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

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

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

and the orbit of the group generated by \( P \) is a spread code.
Thank you for your attention.
T. Etzion and N. Silberstein.
Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams.

R. Kötter and F.R. Kschischang.
Coding for errors and erasures in random network coding.

F. Manganiello, E. Gorla, and J. Rosenthal.
Spread codes and spread decoding in network coding.
A complete characterization of irreducible cyclic orbit codes and their Plücker embedding.

H. Schubert.
*Kalkühl der abzählenden Geometrie.*
Teubner, Leipzig, 1879.

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

Cyclic orbit codes.  

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

New improvements on the echelon-ferrers construction.  