A Construction of Orbit Codes

Joan-Josep Climent[1] Verónica Requena[2] Xaro Soler-Escrivà[1]

[1]Departament de Matemàtiques, Universitat d'Alacant
[2]Departamento de Estadística, Matemáticas e Informática
Universidad Miguel Hernández de Elche

5ICMCTA, Vihula Manor. August 28-31, 2017

Universitat d'Alacant
Universidad de Alicante

Outline

1. Introduction
2. Preliminaries
3. Our construction
4. Open questions

Overview

1 Introduction

2 Preliminaries

3 Our construction

4 Open questions

Introduction

Network coding was introduced for satellite communication networks

R. W. YEUNG and Z. ZHANG.
Distributed source coding for satellite communications.
IEEE Transactions on Information Theory, **45(4)**: 1111–1120 (1999).

Introduction

Network coding was introduced for satellite communication networks

R. W. YEUNG and Z. ZHANG.
Distributed source coding for satellite communications.
IEEE Transactions on Information Theory, **45(4)**: 1111–1120 (1999).

R. AHLSWEDE, N. CAI, S.-Y. R. LI and R. W. YEUNG.
Network information flow.
IEEE Transactions on Information Theory, **46(4)**: 1204–1216 (2000).

Introduction

Network coding was introduced for satellite communication networks

R. W. YEUNG and Z. ZHANG.
Distributed source coding for satellite communications.
IEEE Transactions on Information Theory, **45(4)**: 1111–1120 (1999).

R. AHLSWEDE, N. CAI, S.-Y. R. LI and R. W. YEUNG.
Network information flow.
IEEE Transactions on Information Theory, **46(4)**: 1204–1216 (2000).

Optimality can be achieved by linear network coding

S.-Y. R. LI, R. W. YEUNG and N. CAI.
Linear network coding.
IEEE Transactions on Information Theory, **49(2)**: 371–381 (2003).

Universitat d'Alacant
Universidad de Alicante

Introduction

Network coding was introduced for satellite communication networks

R. W. YEUNG and Z. ZHANG.
Distributed source coding for satellite communications.
IEEE Transactions on Information Theory, **45(4)**: 1111–1120 (1999).

R. AHLSWEDE, N. CAI, S.-Y. R. LI and R. W. YEUNG.
Network information flow.
IEEE Transactions on Information Theory, **46(4)**: 1204–1216 (2000).

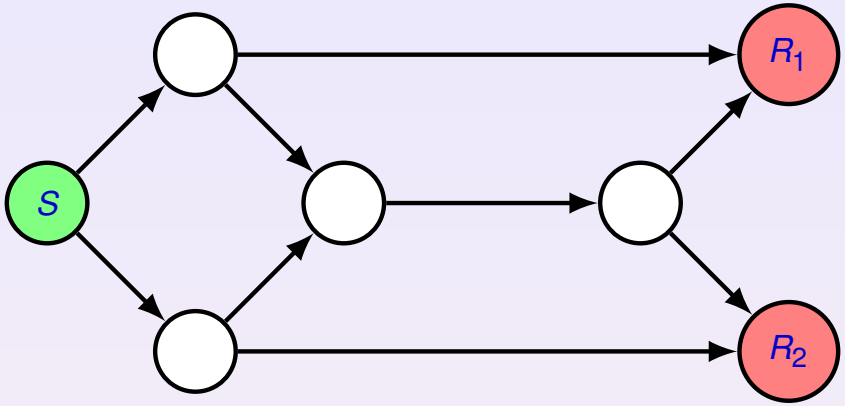
Optimality can be achieved by linear network coding

S.-Y. R. LI, R. W. YEUNG and N. CAI.
Linear network coding.
IEEE Transactions on Information Theory, **49(2)**: 371–381 (2003).

where the communication network is modeled as a finite directed acyclic multigraph, and information travels as packets from one or multiple sources to multiple receivers through intermediate nodes.

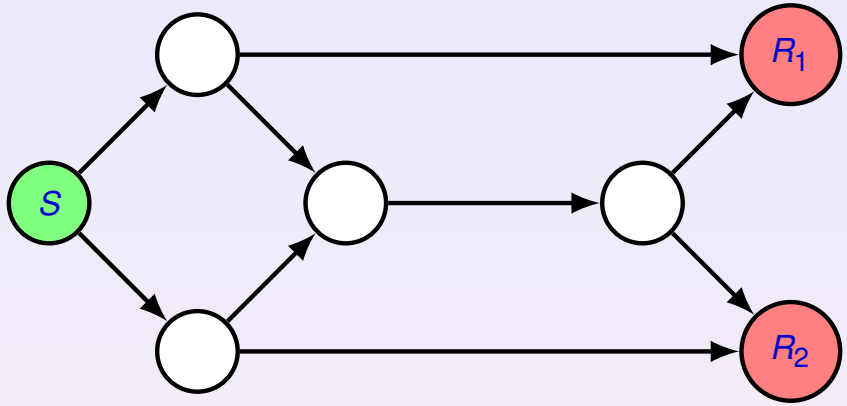
Introduction

This can be illustrated by the butterfly network:

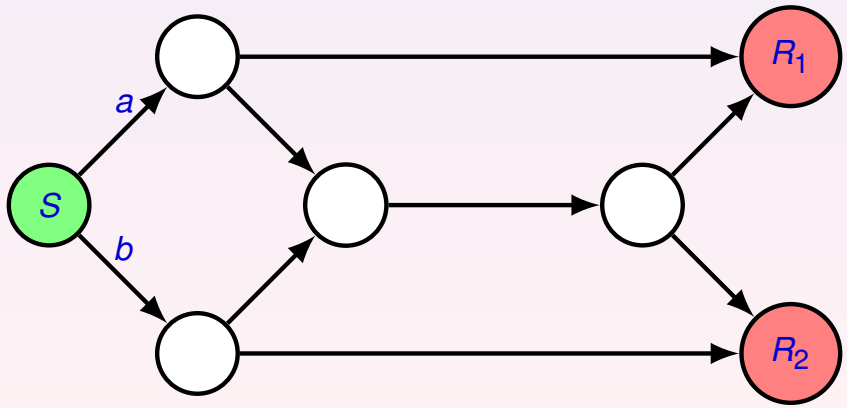


Introduction

This can be illustrated by the butterfly network:

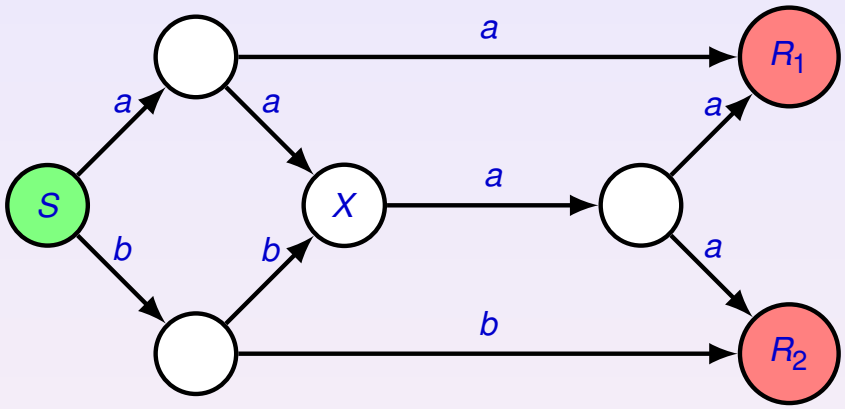


Assume that the source S wants to send the same information, a and b, to both receivers R_1 and R_2.



Introduction

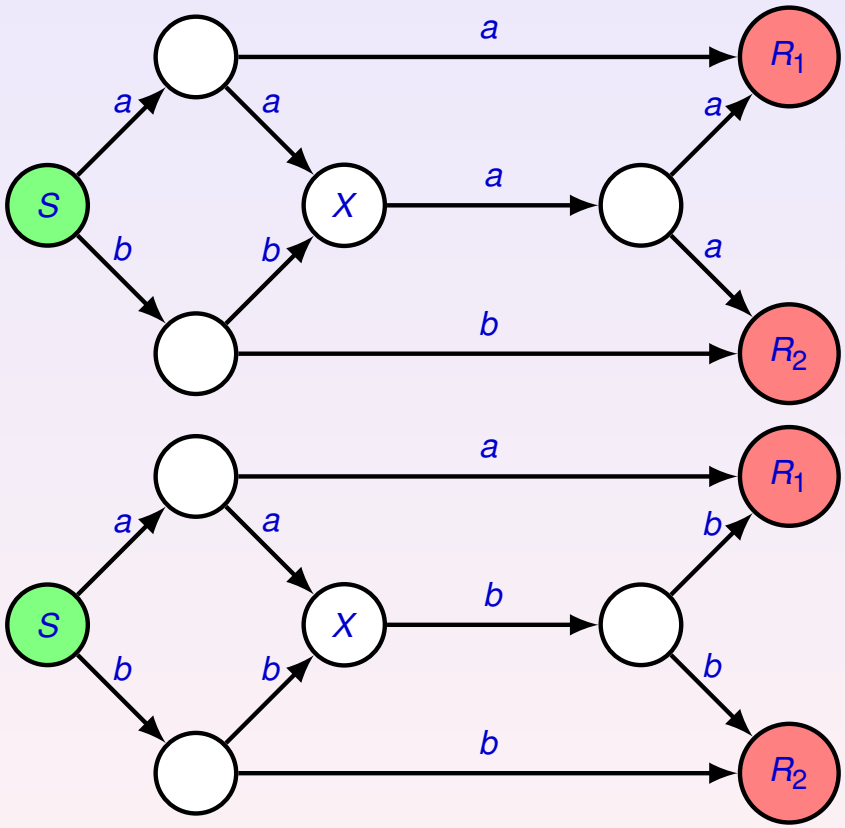
Under forwarding every inner node forwards the incoming information and thus has to decide on either a or b at the bottleneck vertex, marked by X.



Thus, R_1 does not receive b

Introduction

Under forwarding every inner node forwards the incoming information and thus has to decide on either a or b at the bottleneck vertex, marked by X.

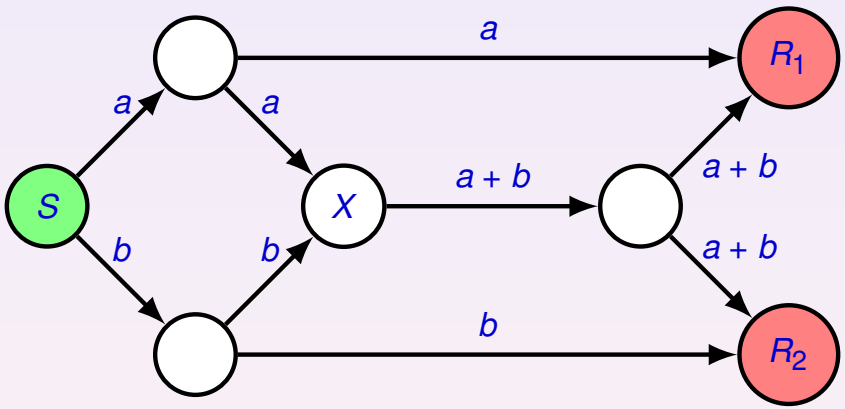


Thus, R_1 does not receive b

Thus, R_2 does not receive a

Introduction

With linear network coding we allow the bottleneck vertex to send the sum of the two incoming informations, which allows both receivers to recover both a and b with a simple operation.



Introduction

In this linear network coding setting, when the topology of the underlying network is unknown or time-varying, one speaks of random (linear) network coding.

R. KOETTER and M. MÉDARD.
An algebraic approach to network coding.
IEEE/ACM Transactions on Networking, **11(5)**: 782–795 (2003).

T. HO, R. KOETTER, M. MÉDARD, D. R. KARGER and M. EFFROS.
The benefits of coding over routing in a randomized setting.
In *Proceedings of the 2003 IEEE International Symposium on Information Theory (ISIT 2003)*, page 442. IEEE, Yokohama, Japan, June/July 2003.

T. HO, M. MÉDARD, R. KOETTER, D. R. KARGER, M. EFFROS, J. SHI and B. LEONG.
A random linear network coding approach to multicast.
IEEE Transactions on Information Theory, **52(10)**: 4413–4430 (2006).

Introduction

In this linear network coding setting, when the topology of the underlying network is unknown or time-varying, one speaks of random (linear) network coding.

R. KOETTER and M. MÉDARD.
An algebraic approach to network coding.
IEEE/ACM Transactions on Networking, **11(5)**: 782–795 (2003).

T. HO, R. KOETTER, M. MÉDARD, D. R. KARGER and M. EFFROS.
The benefits of coding over routing in a randomized setting.
In *Proceedings of the 2003 IEEE International Symposium on Information Theory (ISIT 2003)*, page 442. IEEE, Yokohama, Japan, June/July 2003.

T. HO, M. MÉDARD, R. KOETTER, D. R. KARGER, M. EFFROS, J. SHI and B. LEONG.
A random linear network coding approach to multicast.
IEEE Transactions on Information Theory, **52(10)**: 4413–4430 (2006).

Kötter and Kschischang proposed a mathematical description of network communications in which the transmitted messages are vector subspaces, rather than vectors.

R. KOETTER and F. R. KSCHISCHANG.
Coding for errors and erasures in random network coding.
IEEE Transactions on Information Theory, **54(8)**: 3579–3591 (2008).

Introduction

This approach is known as subspace codes.

D. BARTOLI and F. PAVESE.

A note on equidistant subspace codes.
Discrete Applied Mathematics, **198**: 291–296 (2016).

E. BEN-SASSON, T. ETZION, A. GABIZON and N. RAVIV.

Subspace polynomials and cyclic subspace codes.
IEEE Transactions on Information Theory, **62(3)**: 1157–1165 (2016).

A. COSSIDENTE and F. PAVESE.

On subspace codes.
Designs, Codes and Cryptography, **78(2)**: 527–531 (2016).

T. ETZION and A. VARDY.

Error-correcting codes in projective space.
IEEE Transactions on Information Theory, **57(2)**: 1165–1173 (2011).

H. GLUESING-LUERSSEN, K. MORRISON and C. TROHA.

Cyclic orbit codes and stabilizer subfields.
Advances in Mathematics of Communications, **9(2)**: 177–197 (2015).

H. GLUESING-LUERSSEN and C. TROHA.

Construction of subspace codes through linkage.
Advances in Mathematics of Communications, **10(3)**: 525–540 (2016).

Introduction

E. G. Gorla and A. Ravagnani.

Equidistant subspace codes.
Linear Algebra and its Applications, **490**: 48–65 (2016).

J. Rosenthal and A.-L. Trautmann.

A complete characterization of irreducible cyclic orbit codes and their Plücker embedding.
Designs, Codes and Cryptography, **66**: 275–289 (2013).

N. Silberstein and A.-L. Trautmann.

New lower bounds for constant dimension codes.
In *Proceedings of the 2013 IEEE International Symposium on Information Theory (ISIT 2013)*, pages 514–518. IEEE, Istanbul, July 2013.

A.-L. Trautmann.

Isometry and automorphisms of constant dimension codes.
Advances in Mathematics of Communications, **7(2)**: 147–160 (2013).

A.-L. Trautmann, F. Manganiello, M. Braun and J. Rosenthal.

Cyclic orbit codes.
IEEE Transactions on Information Theory, **59(11)**: 7386–7404 (2013).

A.-L. Trautmann, F. Manganiello and J. Rosenthal.

Orbit codes – a new concept in the area of network coding.
In *Proceedings of the 2010 IEEE Information Theory Workshop (ITW 2010)*. IEEE, Dublin, Ireland, August 2010.

Most of these authors focus on constant dimension codes.

Universitat d'Alacant
Universidad de Alicante

Introduction

We focus our attention on constant dimension codes which are obtained as orbits of certain groups.

Introduction

We focus our attention on constant dimension codes which are obtained as orbits of certain groups.

In the linear network coding setting, Trautmann, Manganiello and Rosenthal defined such codes as orbit codes by the action of subgroups of the general linear group.

A.-L. TRAUTMANN, F. MANGANIELLO and J. ROSENTHAL.
Orbit codes – a new concept in the area of network coding.
In *Proceedings of the 2010 IEEE Information Theory Workshop (ITW 2010)*. IEEE, Dublin, Ireland, August 2010.

Introduction

Since then, several papers have been written about the structure of orbit codes.

F. BARDESTANI and A. IRANMANESH.
Cyclic orbit codes with the normalizer of a Singer subgroup.
Journal of Sciences, Islamic Republic of Iran, **26(1)**: 49–55 (2015).

A. GHATAK.
Construction of Singer subgroup orbit codes based on cyclic difference sets.
In *Proceedings of the Twentieth National Conference on Communications (NCC 2014)*, pages 1–4. IEEE, Kanpur, India, February 2014.

H. GLUESING-LUERSSEN, K. MORRISON and C. TROHA.
Cyclic orbit codes and stabilizer subfields.
Advances in Mathematics of Communications, **9(2)**: 177–197 (2015).

A.-L. TRAUTMANN.
Isometry and automorphisms of constant dimension codes.
Advances in Mathematics of Communications, **7(2)**: 147–160 (2013).

A.-L. TRAUTMANN, F. MANGANIELLO, M. BRAUN and J. ROSENTHAL.
Cyclic orbit codes.
IEEE Transactions on Information Theory, **59(11)**: 7386–7404 (2013).

Universitat d'Alacant
Universidad de Alicante

Introduction

When we consider cyclic subgroups of the general linear group, we talk about cyclic orbit codes.

Introduction

When we consider cyclic subgroups of the general linear group, we talk about cyclic orbit codes.

These codes were introduced by Trautmann, Manganiello, Braun, and Rosenthal

A.-L. Trautmann, F. Manganiello, M. Braun and J. Rosenthal.
Cyclic orbit codes.
IEEE Transactions on Information Theory, **59(11)**: 7386–7404 (2013).

where the authors gave a characterization of a particular subclass of them.

Introduction

In this talk we are interested on Abelian orbit codes; that is, orbit codes which are generated by Abelian subgroups of the general linear group.

Introduction

In this talk we are interested on Abelian orbit codes; that is, orbit codes which are generated by Abelian subgroups of the general linear group.

Since Abelian subgroups are direct product of cyclic subgroups, it seems a natural extension of the research on cyclic orbit codes.

Introduction

In this talk we are interested on Abelian orbit codes; that is, orbit codes which are generated by Abelian subgroups of the general linear group.

Since Abelian subgroups are direct product of cyclic subgroups, it seems a natural extension of the research on cyclic orbit codes.

Specifically, we present a construction of an Abelian non-cyclic orbit code for which we calculate its cardinality and its minimum subspace distance.

Introduction

In this talk we are interested on Abelian orbit codes; that is, orbit codes which are generated by Abelian subgroups of the general linear group.

Since Abelian subgroups are direct product of cyclic subgroups, it seems a natural extension of the research on cyclic orbit codes.

Specifically, we present a construction of an Abelian non-cyclic orbit code for which we calculate its cardinality and its minimum subspace distance.

Moreover, the minimum subspace distance of our code is maximal.

Overview

1 Introduction

2 Preliminaries

3 Our construction

4 Open questions

Preliminaries

Let $\mathbb{F}_q$ be the finite field of q elements, where q is a prime power.

Preliminaries

Let $\mathbb{F}_q$ be the finite field of q elements, where q is a prime power.

For any integer $n \geq 1$, the set $\mathcal{P}_q(n)$ of all vector subspaces of $\mathbb{F}_q^n$ forms a metric space with respect to the subspace distance defined by

$$d(\mathcal{U}, \mathcal{V}) = \dim(\mathcal{U} + \mathcal{V}) - \dim(\mathcal{U} \cap \mathcal{V}), \quad \text{for all } \mathcal{U}, \mathcal{V} \in \mathcal{P}_q(n). \tag{1}$$

R. KOETTER and F. R. KSCHISCHANG.
Coding for errors and erasures in random network coding.
IEEE Transactions on Information Theory, **54(8)**: 3579–3591 (2008).

Preliminaries

Let $\mathbb{F}_q$ be the finite field of q elements, where q is a prime power.

For any integer $n \geq 1$, the set $\mathcal{P}_q(n)$ of all vector subspaces of $\mathbb{F}_q^n$ forms a metric space with respect to the subspace distance defined by

$$d(\mathcal{U}, \mathcal{V}) = \dim(\mathcal{U} + \mathcal{V}) - \dim(\mathcal{U} \cap \mathcal{V}), \quad \text{for all } \mathcal{U}, \mathcal{V} \in \mathcal{P}_q(n). \tag{1}$$

R. KOETTER and F. R. KSCHISCHANG.
Coding for errors and erasures in random network coding.
IEEE Transactions on Information Theory, **54(8)**: 3579–3591 (2008).

For any integer k, where $0 \leq k \leq n$, the set $\mathcal{G}_q(k, n)$ of all k-dimensional vector subspaces of $\mathbb{F}_q^n$ is called the Grassmannian.

Obviously, $\mathcal{P}_q(n) = \bigcup_{k=0}^{n} \mathcal{G}_q(k, n)$.

Preliminaries

A subspace code of length n is a nonempty subset $\mathfrak{C}$ of $\mathcal{P}_q(n)$.
A codeword of $\mathfrak{C}$ is a vector subspace of $\mathfrak{C}$.

Preliminaries

A subspace code of length n is a nonempty subset $\mathfrak{C}$ of $\mathcal{P}_q(n)$.
A codeword of $\mathfrak{C}$ is a vector subspace of $\mathfrak{C}$.

The minimum distance of a subspace code $\mathfrak{C} \subseteq \mathcal{P}_q(n)$ is defined as

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

Preliminaries

A subspace code of length n is a nonempty subset $\mathfrak{C}$ of $\mathcal{P}_q(n)$.
A codeword of $\mathfrak{C}$ is a vector subspace of $\mathfrak{C}$.

The minimum distance of a subspace code $\mathfrak{C} \subseteq \mathcal{P}_q(n)$ is defined as

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

$\mathfrak{C}$ is a constant dimension code if all codewords of $\mathfrak{C}$ have the same dimension; i.e., if $\mathfrak{C} \subseteq \mathcal{G}_q(k, n)$ for some k.

Preliminaries

A subspace code of length n is a nonempty subset $\mathfrak{C}$ of $\mathcal{P}_q(n)$.
A codeword of $\mathfrak{C}$ is a vector subspace of $\mathfrak{C}$.

The minimum distance of a subspace code $\mathfrak{C} \subseteq \mathcal{P}_q(n)$ is defined as

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

$\mathfrak{C}$ is a constant dimension code if all codewords of $\mathfrak{C}$ have the same dimension; i.e., if $\mathfrak{C} \subseteq \mathcal{G}_q(k, n)$ for some k.

In this talk we consider $\mathcal{G}_q(k, n)$, and we assume, without loss of generality, that $2k \leq n$.

Preliminaries

A subspace code of length n is a nonempty subset $\mathfrak{C}$ of $\mathcal{P}_q(n)$.
A codeword of $\mathfrak{C}$ is a vector subspace of $\mathfrak{C}$.

The minimum distance of a subspace code $\mathfrak{C} \subseteq \mathcal{P}_q(n)$ is defined as

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

$\mathfrak{C}$ is a constant dimension code if all codewords of $\mathfrak{C}$ have the same dimension; i.e., if $\mathfrak{C} \subseteq \mathcal{G}_q(k, n)$ for some k.

In this talk we consider $\mathcal{G}_q(k, n)$, and we assume, without loss of generality, that $2k \leq n$.

Otherwise, we can consider the complementary code (or dual code) of $\mathfrak{C}$:

$$\mathfrak{C}^{\perp} = \left\{ \mathcal{U}^{\perp} \subseteq \mathcal{G}_q(n-k, n) \mid \mathcal{U} \in \mathfrak{C} \right\}$$

obtained from the orthogonal subspaces of the codewords of $\mathfrak{C}$ which has the same length, cardinality and minimum distance.

Preliminaries

If $\mathcal{U} \in \mathcal{G}_q(k, n)$, then

$$\mathcal{U} = \text{rowspace}\,(U) = \left\{ \boldsymbol{x}U \mid \boldsymbol{x} \in \mathbb{F}_q^k \right\}$$

for some full-rank matrix $U \in \mathbb{F}_q^{k \times n}$.

Preliminaries

If $\mathcal{U} \in \mathcal{G}_q(k,n)$, then

$$\mathcal{U} = \text{rowspace}\,(U) = \left\{ \boldsymbol{x}U \mid \boldsymbol{x} \in \mathbb{F}_q^k \right\}$$

for some full-rank matrix $U \in \mathbb{F}_q^{k\times n}$.

If $\mathcal{U}, \mathcal{V} \in \mathcal{G}_q(k,n)$, then

$$d(\mathcal{U},\mathcal{V}) = 2(k - \dim(\mathcal{U}\cap\mathcal{V})) = 2\ \text{rank}\begin{bmatrix} U \\ V \end{bmatrix} - 2\,k \tag{2}$$

for some full-rank matrices $U, V \in \mathbb{F}_q^{k\times n}$ such that

$$\mathcal{U} = \text{rowspace}\,(U) \quad \text{and} \quad \mathcal{V} = \text{rowspace}\,(V)\,.$$

Preliminaries

We focus on constant dimension codes arising from group actions, which are called orbit codes

A.-L. TRAUTMANN, F. MANGANIELLO and J. ROSENTHAL.

Orbit codes – a new concept in the area of network coding.
In *Proceedings of the 2010 IEEE Information Theory Workshop (ITW 2010)*. IEEE, Dublin, Ireland, August 2010.

Preliminaries

We focus on constant dimension codes arising from group actions, which are called orbit codes

A.-L. Trautmann, F. Manganiello and J. Rosenthal.
Orbit codes – a new concept in the area of network coding.
In *Proceedings of the 2010 IEEE Information Theory Workshop (ITW 2010)*. IEEE, Dublin, Ireland, August 2010.

The general linear group of degree n:

$$\mathrm{GL}_n = \left\{ A \in \mathbb{F}_q^{n \times n} \mid A \text{ is invertible} \right\}$$

Preliminaries

We focus on constant dimension codes arising from group actions, which are called orbit codes

A.-L. Trautmann, F. Manganiello and J. Rosenthal.
Orbit codes – a new concept in the area of network coding.
In *Proceedings of the 2010 IEEE Information Theory Workshop (ITW 2010)*. IEEE, Dublin, Ireland, August 2010.

The general linear group of degree n:

$$\mathrm{GL}_n = \left\{ A \in \mathbb{F}_q^{n \times n} \mid A \text{ is invertible} \right\}$$

We can define a group action (from the right) on the Grassmannian:

$$\begin{array}{ccc} \mathcal{G}_q(k,n) \times \mathrm{GL}_n & \longrightarrow & \mathcal{G}_q(k,n) \\ (\mathcal{U}, A) & \mapsto & \mathcal{U} \cdot A \end{array}$$

Universitat d'Alacant
Universidad de Alicante

Preliminaries

We focus on constant dimension codes arising from group actions, which are called orbit codes

A.-L. Trautmann, F. Manganiello and J. Rosenthal.
Orbit codes – a new concept in the area of network coding.
In *Proceedings of the 2010 IEEE Information Theory Workshop (ITW 2010)*. IEEE, Dublin, Ireland, August 2010.

The general linear group of degree n:

$$\mathrm{GL}_n = \left\{ A \in \mathbb{F}_q^{n\times n} \mid A \text{ is invertible} \right\}$$

We can define a group action (from the right) on the Grassmannian:

$$\begin{array}{ccc} \mathcal{G}_q(k,n) \times \mathrm{GL}_n & \longrightarrow & \mathcal{G}_q(k,n) \\ (\mathcal{U}, A) & \mapsto & \mathcal{U}\cdot A \end{array}$$

where $\mathcal{U} = \mathrm{rowspace}\,(U)$, $U \in \mathbb{F}_q^{k\times n}$ a full-rank matrix, and

$$\mathcal{U}\cdot A = \mathrm{rowspace}\,(UA)\,.$$

Preliminaries

Now, let **G** be a subgroup of GL_n and consider the action of **G** on $\mathcal{G}_q(k, n)$.

Preliminaries

Now, let **G** be a subgroup of GL_n and consider the action of **G** on $\mathcal{G}_q(k,n)$.

Then the orbit of a subspace $\mathcal{U} \in \mathcal{G}_q(k,n)$ under the action of **G** is

$$\mathfrak{C} = \{\mathcal{U} \cdot A \mid A \in \mathbf{G}\},$$

which is called the orbit code generated by the action of **G** on $\mathcal{U}$.

Preliminaries

Now, let $\mathbf{G}$ be a subgroup of GL_n and consider the action of $\mathbf{G}$ on $\mathcal{G}_q(k,n)$.

Then the orbit of a subspace $\mathcal{U} \in \mathcal{G}_q(k,n)$ under the action of $\mathbf{G}$ is

$$\mathfrak{C} = \{\mathcal{U} \cdot A \mid A \in \mathbf{G}\},$$

which is called the orbit code generated by the action of $\mathbf{G}$ on $\mathcal{U}$.

The stabilizer of $\mathcal{U}$ under this action is

$$\mathrm{stab}_{\mathbf{G}}(\mathcal{U}) = \{A \in \mathbf{G} \mid \mathcal{U} \cdot A = \mathcal{U}\}$$

Preliminaries

Now, let $\mathbf{G}$ be a subgroup of GL_n and consider the action of $\mathbf{G}$ on $\mathcal{G}_q(k,n)$.

Then the orbit of a subspace $\mathcal{U} \in \mathcal{G}_q(k,n)$ under the action of $\mathbf{G}$ is

$$\mathfrak{C} = \{\mathcal{U} \cdot A \mid A \in \mathbf{G}\},$$

which is called the orbit code generated by the action of $\mathbf{G}$ on $\mathcal{U}$.

The stabilizer of $\mathcal{U}$ under this action is

$$\mathrm{stab}_{\mathbf{G}}(\mathcal{U}) = \{A \in \mathbf{G} \mid \mathcal{U} \cdot A = \mathcal{U}\} = \mathbf{G} \cap \mathrm{stab}_{\mathrm{GL}_n}(\mathcal{U})$$

Preliminaries

Now, let $\mathbf{G}$ be a subgroup of GL_n and consider the action of $\mathbf{G}$ on $\mathcal{G}_q(k,n)$.

Then the orbit of a subspace $\mathcal{U} \in \mathcal{G}_q(k,n)$ under the action of $\mathbf{G}$ is

$$\mathfrak{C} = \{\mathcal{U} \cdot A \mid A \in \mathbf{G}\},$$

which is called the orbit code generated by the action of $\mathbf{G}$ on $\mathcal{U}$.

The stabilizer of $\mathcal{U}$ under this action is

$$\mathrm{stab}_{\mathbf{G}}(\mathcal{U}) = \{A \in \mathbf{G} \mid \mathcal{U} \cdot A = \mathcal{U}\} = \mathbf{G} \cap \mathrm{stab}_{\mathrm{GL}_n}(\mathcal{U})$$

and the size of the orbit code is $|\mathfrak{C}| = \dfrac{|\mathbf{G}|}{|\mathrm{stab}_{\mathbf{G}}(\mathcal{U})|}$.

Preliminaries

Now, let $\mathbf{G}$ be a subgroup of GL_n and consider the action of $\mathbf{G}$ on $\mathcal{G}_q(k,n)$.

Then the orbit of a subspace $\mathcal{U} \in \mathcal{G}_q(k,n)$ under the action of $\mathbf{G}$ is

$$\mathfrak{C} = \{\mathcal{U} \cdot A \mid A \in \mathbf{G}\},$$

which is called the orbit code generated by the action of $\mathbf{G}$ on $\mathcal{U}$.

The stabilizer of $\mathcal{U}$ under this action is

$$\mathrm{stab}_{\mathbf{G}}(\mathcal{U}) = \{A \in \mathbf{G} \mid \mathcal{U} \cdot A = \mathcal{U}\} = \mathbf{G} \cap \mathrm{stab}_{\mathrm{GL}_n}(\mathcal{U})$$

and the size of the orbit code is $|\mathfrak{C}| = \dfrac{|\mathbf{G}|}{|\mathrm{stab}_{\mathbf{G}}(\mathcal{U})|}$.

Since, the subspace distance is GL_n-invariant:

$$d(\mathcal{U},\mathcal{V}) = d(\mathcal{U} \cdot A, \mathcal{V} \cdot A), \quad \text{for all } A \in \mathrm{GL}_n,$$

Preliminaries

Now, let $\mathbf{G}$ be a subgroup of GL_n and consider the action of $\mathbf{G}$ on $\mathcal{G}_q(k,n)$.

Then the orbit of a subspace $\mathcal{U} \in \mathcal{G}_q(k,n)$ under the action of $\mathbf{G}$ is

$$\mathfrak{C} = \{\mathcal{U} \cdot A \mid A \in \mathbf{G}\},$$

which is called the orbit code generated by the action of $\mathbf{G}$ on $\mathcal{U}$.

The stabilizer of $\mathcal{U}$ under this action is

$$\mathrm{stab}_{\mathbf{G}}(\mathcal{U}) = \{A \in \mathbf{G} \mid \mathcal{U} \cdot A = \mathcal{U}\} = \mathbf{G} \cap \mathrm{stab}_{\mathrm{GL}_n}(\mathcal{U})$$

and the size of the orbit code is $|\mathfrak{C}| = \dfrac{|\mathbf{G}|}{|\mathrm{stab}_{\mathbf{G}}(\mathcal{U})|}$.

Since, the subspace distance is GL_n-invariant:

$$d(\mathcal{U},\mathcal{V}) = d(\mathcal{U} \cdot A, \mathcal{V} \cdot A), \quad \text{for all } A \in \mathrm{GL}_n,$$

it follows that

$$d(\mathfrak{C}) = \min\{d(\mathcal{U}, \mathcal{U} \cdot A) \mid A \in \mathbf{G} \setminus \mathrm{stab}_{\mathbf{G}}(\mathcal{U})\}.$$

Preliminaries

Lemma 1

Assume that $A \in \mathbb{F}^{r\times r}$, $B \in \mathbb{F}^{s\times s}$, *and* $P \in \mathbb{F}^{r\times s}$ *and consider*

$$M = \begin{bmatrix} A & P \\ O & B \end{bmatrix}$$

where O *denotes the zero matrix of the appropriate size.*
If h *is a nonnegative integer, then*

$$M^h = \begin{bmatrix} A^h & \sigma_h(A,B,P) \\ O & B^h \end{bmatrix}$$

where

$$\sigma_h(A,B,P) = \begin{cases} O, & \text{if } h = 0, \\ \displaystyle\sum_{i=1}^{h} A^{h-i} P B^{i-1}, & \text{if } h \geq 1. \end{cases}$$

Overview

1 Introduction

2 Preliminaries

3 Our construction

4 Open questions

Our construction

Our aim is to construct an orbit code $\mathfrak{C}$ by considering the orbit of the vector subspace $\mathcal{U}_k$ generated by the first k unit vectors of $\mathbb{F}_q^n$, under the action of a concrete subgroup $\mathbf{H}$ of GL_n .

Our construction

Assume that

$$\mathbf{H} = \left\{ H \in \mathrm{GL}_n \mid H = \begin{bmatrix} H_{11} & H_{12} \\ O & H_{22} \end{bmatrix} \right.$$

$$\left. \text{where } H_{11} \in \mathrm{GL}_k \,,\, H_{12} \in \mathbb{F}_q^{k\times(n-k)},\, H_{22} \in \mathrm{GL}_{n-k} \right\}. \qquad (3)$$

Our construction

Assume that

$$\mathbf{H} = \left\{ H \in \mathrm{GL}_n \mid H = \begin{bmatrix} H_{11} & H_{12} \\ O & H_{22} \end{bmatrix} \right.$$
$$\left. \text{where } H_{11} \in \mathrm{GL}_k\,,\ H_{12} \in \mathbb{F}_q^{k\times(n-k)},\ H_{22} \in \mathrm{GL}_{n-k} \right\}. \qquad (3)$$

Since $\mathcal{U}_k = \text{rowspace}\left(\begin{bmatrix} I_k & O \end{bmatrix}\right)$,

Our construction

Assume that

$$\mathbf{H} = \left\{ H \in \mathrm{GL}_n \mid H = \begin{bmatrix} H_{11} & H_{12} \\ O & H_{22} \end{bmatrix} \right.$$
$$\left. \text{where } H_{11} \in \mathrm{GL}_k\,,\ H_{12} \in \mathbb{F}_q^{k\times(n-k)},\ H_{22} \in \mathrm{GL}_{n-k} \right\}. \qquad (3)$$

Since $\mathcal{U}_k = \text{rowspace}\left(\begin{bmatrix} I_k & O \end{bmatrix}\right)$, it follows that

$$\mathfrak{C} = \{\mathcal{U}_k \cdot H \mid H \in \mathbf{H}\} = \left\{\text{rowspace}\left(\begin{bmatrix} H_{11} & H_{12} \end{bmatrix}\right) \mid H \in \mathbf{H}\right\}. \qquad (4)$$

Our construction

Assume that

$$\mathbf{H} = \left\{ H \in \mathrm{GL}_n \mid H = \begin{bmatrix} H_{11} & H_{12} \\ O & H_{22} \end{bmatrix} \right.$$
$$\left. \text{where } H_{11} \in \mathrm{GL}_k\,,\ H_{12} \in \mathbb{F}_q^{k\times(n-k)},\ H_{22} \in \mathrm{GL}_{n-k} \right\}. \qquad (3)$$

Since $\mathcal{U}_k = \text{rowspace}\left(\begin{bmatrix} I_k & O \end{bmatrix}\right)$, it follows that

$$\mathfrak{C} = \{\mathcal{U}_k \cdot H \mid H \in \mathbf{H}\} = \left\{\text{rowspace}\left(\begin{bmatrix} H_{11} & H_{12} \end{bmatrix}\right) \mid H \in \mathbf{H}\right\}. \qquad (4)$$

Moreover, according to (2) and (3), for any $H \in \mathbf{H}$

$$d(\mathcal{U}_k, \mathcal{U}_k \cdot H) = 2\ \text{rank} \begin{bmatrix} I_k & O \\ H_{11} & H_{12} \end{bmatrix} - 2k = 2\ \text{rank}\,(H_{12}) \leq 2k. \qquad (5)$$

Our construction

Assume that

$$\mathbf{H} = \left\{ H \in \mathrm{GL}_n \mid H = \begin{bmatrix} H_{11} & H_{12} \\ O & H_{22} \end{bmatrix} \right.$$
$$\left. \text{where } H_{11} \in \mathrm{GL}_k\,,\ H_{12} \in \mathbb{F}_q^{k\times(n-k)},\ H_{22} \in \mathrm{GL}_{n-k} \right\}. \tag{3}$$

Since $\mathcal{U}_k = \text{rowspace}\left(\begin{bmatrix} I_k & O \end{bmatrix}\right)$, it follows that

$$\mathfrak{C} = \{\mathcal{U}_k \cdot H \mid H \in \mathbf{H}\} = \left\{\text{rowspace}\left(\begin{bmatrix} H_{11} & H_{12} \end{bmatrix}\right) \mid H \in \mathbf{H}\right\}. \tag{4}$$

Moreover, according to (2) and (3), for any $H \in \mathbf{H}$

$$d(\mathcal{U}_k, \mathcal{U}_k \cdot H) = 2\ \text{rank} \begin{bmatrix} I_k & O \\ H_{11} & H_{12} \end{bmatrix} - 2k = 2\ \text{rank}\,(H_{12}) \leq 2k. \tag{5}$$

Our construction

On the other hand

$$\mathrm{stab}_{\mathrm{GL}_n}(\mathcal{U}_k) = \left\{ \begin{bmatrix} A & O \\ Q & B \end{bmatrix} \mid A \in \mathrm{GL}_k\,,\ Q \in \mathbb{F}_q^{(n-k)\times k} \text{ and } B \in \mathrm{GL}_{n-k} \right\}.$$

Our construction

On the other hand

$$\mathrm{stab}_{\mathrm{GL}_n}(\mathcal{U}_k) = \left\{ \begin{bmatrix} A & O \\ Q & B \end{bmatrix} \mid A \in \mathrm{GL}_k\,,\ Q \in \mathbb{F}_q^{(n-k)\times k} \text{ and } B \in \mathrm{GL}_{n-k} \right\}.$$

Since $\mathrm{stab}_{\mathbf{H}}(\mathcal{U}_k) = \mathbf{H} \cap \mathrm{stab}_{\mathrm{GL}_n}(\mathcal{U}_k)$, and using the previous partition of matrices of $\mathbf{H}$ given by (3), then

$$\mathrm{stab}_{\mathbf{H}}(\mathcal{U}_k) = \left\{ \begin{bmatrix} H_{11} & H_{12} \\ O & H_{22} \end{bmatrix} \in \mathbf{H} \mid H_{12} = O \right\}. \tag{6}$$

Our construction

From now on, we will assume that q is a prime number such that $q \geq n - k$.

Our construction

From now on, we will assume that q is a prime number such that $q \geq n - k$.

Let λ be a generator of the multiplicative cyclic group $\mathbb{F}_q^*$; i.e., λ is a primitive element of $\mathbb{F}_q$ (in particular $o(\lambda) = q - 1$ is the multiplicative order of λ).

Our construction

From now on, we will assume that q is a prime number such that $q \geq n - k$.

Let λ be a generator of the multiplicative cyclic group $\mathbb{F}_q^*$; i.e., λ is a primitive element of $\mathbb{F}_q$ (in particular $o(\lambda) = q - 1$ is the multiplicative order of λ).

Let us denote by J_ℓ the Jordan block of size $\ell \times \ell$ associated to 1:

$$J_\ell = \begin{bmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

Our construction

From now on, we will assume that q is a prime number such that $q \geq n - k$.

Let λ be a generator of the multiplicative cyclic group $\mathbb{F}_q^*$; i.e., λ is a primitive element of $\mathbb{F}_q$ (in particular $o(\lambda) = q - 1$ is the multiplicative order of λ).

Let us denote by J_ℓ the Jordan block of size $\ell \times \ell$ associated to 1:

$$J_\ell = \begin{bmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

Lemma 2

If $q^{t-1} < \ell \leq q^t$ for some nonnegative integer t, then $o(J_\ell) = q^t$.

Our construction

We consider the following two matrices of GL_n :

$$S = \begin{bmatrix} \lambda I_{n-k} & X \\ O & I_k \end{bmatrix}, \qquad T = \begin{bmatrix} J_{n-k} & Y \\ O & \lambda I_k \end{bmatrix} \quad \text{where } X, Y \in \mathbb{F}_q^{(n-k)\times k}. \tag{7}$$

Our construction

We consider the following two matrices of GL_n:

$$S = \begin{bmatrix} \lambda I_{n-k} & X \\ O & I_k \end{bmatrix}, \qquad T = \begin{bmatrix} J_{n-k} & Y \\ O & \lambda I_k \end{bmatrix} \quad \text{where } X, Y \in \mathbb{F}_q^{(n-k)\times k}. \tag{7}$$

Lemma 3

For the matrices S and T given by (7)*, it follows that*

1. $o(S) = o(\lambda) = q - 1$.
2. $o(T) = o(J_{n-k})\, o(\lambda) = q(q-1)$.

Our construction

We consider the following two matrices of GL_n:

$$S = \begin{bmatrix} \lambda I_{n-k} & X \\ O & I_k \end{bmatrix}, \qquad T = \begin{bmatrix} J_{n-k} & Y \\ O & \lambda I_k \end{bmatrix} \quad \text{where } X, Y \in \mathbb{F}_q^{(n-k)\times k}. \tag{7}$$

Lemma 3

For the matrices S and T given by (7)*, it follows that*

1. $o(S) = o(\lambda) = q - 1$.
2. $o(T) = o(J_{n-k})\, o(\lambda) = q(q-1)$.

$$\langle S \rangle = \left\{ S^a \mid 0 \le a < q-1 \right\}, \quad \langle T \rangle = \left\{ T^b \mid 0 \le b < q(q-1) \right\}$$

Our construction

We consider the following two matrices of GL_n:

$$S = \begin{bmatrix} \lambda I_{n-k} & X \\ O & I_k \end{bmatrix}, \qquad T = \begin{bmatrix} J_{n-k} & Y \\ O & \lambda I_k \end{bmatrix} \quad \text{where } X, Y \in \mathbb{F}_q^{(n-k)\times k}. \tag{7}$$

Lemma 3

For the matrices S and T given by (7), it follows that

1. $o(S) = o(\lambda) = q - 1$.
2. $o(T) = o(J_{n-k})\, o(\lambda) = q(q-1)$.

$$\langle S \rangle = \left\{ S^a \mid 0 \le a < q-1 \right\}, \quad \langle T \rangle = \left\{ T^b \mid 0 \le b < q(q-1) \right\}$$

Lemma 4

1. $\langle S \rangle \cap \langle T \rangle = \{ I_n \}$.
2. *If $X \neq O$ and $Y = \frac{1}{1-\lambda} (\lambda I_{n-k} - J_{n-k})\, X$, then $ST = TS$.*

Our construction

Our construction

From now on, we assume that matrices X and Y are defined as in Lemma 4.2.

Our construction

From now on, we assume that matrices X and Y are defined as in Lemma 4.2.

Since $\langle S \rangle \cap \langle T \rangle = \{I_n\}$ and $ST = TS$, it follows that

$$\begin{aligned} \mathbf{H} &= \langle S, T \rangle = \langle S \rangle \times \langle T \rangle \\ &= \left\{ S^a T^b \mid 0 \leq a < q-1,\ 0 \leq b < q(q-1) \right\} \cong C_{q-1} \times C_{q(q-1)}, \end{aligned} \tag{8}$$

Our construction

From now on, we assume that matrices X and Y are defined as in Lemma 4.2.

Since $\langle S \rangle \cap \langle T \rangle = \{I_n\}$ and $ST = TS$, it follows that

$$\begin{aligned} \mathbf{H} &= \langle S, T \rangle = \langle S \rangle \times \langle T \rangle \\ &= \left\{ S^a T^b \mid 0 \leq a < q-1,\ 0 \leq b < q(q-1) \right\} \cong C_{q-1} \times C_{q(q-1)}, \end{aligned} \tag{8}$$

that is, $\mathbf{H}$ is an Abelian non-cyclic group of order $q(q-1)^2$

Our construction

From now on, we assume that matrices X and Y are defined as in Lemma 4.2.

Since $\langle S \rangle \cap \langle T \rangle = \{I_n\}$ and $ST = TS$, it follows that

$$\begin{aligned} \mathbf{H} &= \langle S, T \rangle = \langle S \rangle \times \langle T \rangle \\ &= \left\{ S^a T^b \mid 0 \leq a < q-1,\ 0 \leq b < q(q-1) \right\} \cong C_{q-1} \times C_{q(q-1)}, \end{aligned} \tag{8}$$

that is, $\mathbf{H}$ is an Abelian non-cyclic group of order $q(q-1)^2$ and the elements of $\mathbf{H}$ present the following form

$$\begin{aligned} S^a T^b &= \begin{bmatrix} \lambda^a I_{n-k} & \sigma_a(\lambda I_{n-k}, I_k, X) \\ O & I_k \end{bmatrix} \begin{bmatrix} J_{n-k}^b & \sigma_b(J_{n-k}, \lambda I_k, Y) \\ O & \lambda^b I_k \end{bmatrix} \\ &= \begin{bmatrix} \lambda^a J_{n-k}^b & \lambda^a \sigma_b(J_{n-k}, \lambda I_k, Y) + \lambda^b \sigma_a(\lambda I_{n-k}, I_k, X) \\ O & \lambda^b I_k \end{bmatrix}. \end{aligned} \tag{9}$$

Our construction

Lemma 5

For any nonnegative integer b it follows that

$$J^b_{n-k} = \begin{bmatrix} 1 & \binom{b}{1} & \binom{b}{2} & \cdots & \binom{b}{n-k-2} & \binom{b}{n-k-1} \\ 0 & 1 & \binom{b}{1} & \cdots & \binom{b}{n-k-3} & \binom{b}{n-k-2} \\ 0 & 0 & 1 & \cdots & \binom{b}{n-k-4} & \binom{b}{n-k-3} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \binom{b}{1} \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

Our construction

Lemma 6

For matrices X and Y as in Lemma 4.2, then

$$\lambda^a \sigma_b(J_{n-k}, \lambda I_k, Y) + \lambda^b \sigma_a(\lambda I_{n-k}, I_k, X)$$
$$= \begin{bmatrix} c & e_1 & e_2 & \cdots & e_{n-k-2} & e_{n-k-1} \\ 0 & c & e_1 & \cdots & e_{n-k-3} & e_{n-k-2} \\ 0 & 0 & c & \cdots & e_{n-k-4} & e_{n-k-3} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & c & e_1 \\ 0 & 0 & 0 & \cdots & 0 & c \end{bmatrix} X,$$

where $c = \dfrac{\lambda^a - \lambda^b}{\lambda - 1}$ *and* $e_i = \dfrac{\lambda^a}{\lambda - 1}\binom{b}{i}$, *for* $i = 1, 2, \ldots, n-k-1$.

Our construction

Lemma 6

For matrices X and Y as in Lemma 4.2, then

$$\lambda^a \sigma_b(J_{n-k}, \lambda I_k, Y) + \lambda^b \sigma_a(\lambda I_{n-k}, I_k, X)$$
$$= \begin{bmatrix} c & e_1 & e_2 & \cdots & e_{n-k-2} & e_{n-k-1} \\ 0 & c & e_1 & \cdots & e_{n-k-3} & e_{n-k-2} \\ 0 & 0 & c & \cdots & e_{n-k-4} & e_{n-k-3} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & c & e_1 \\ 0 & 0 & 0 & \cdots & 0 & c \end{bmatrix} X,$$

where $c = \dfrac{\lambda^a - \lambda^b}{\lambda - 1}$ *and* $e_i = \dfrac{\lambda^a}{\lambda - 1}\binom{b}{i}$, *for* $i = 1, 2, \ldots, n-k-1$.

Lemma 7

With the notation of Lemma 6, $c = 0$ if, and only if, $a \equiv b \pmod{(q-1)}$.

Our construction

So, we consider the following partition

$$S^a T^b = \left[\begin{array}{c|c} \lambda^a J^b_{n-k} & \lambda^a \sigma_b(J_{n-k}, \lambda I_k, Y) + \lambda^b \sigma_a(\lambda I_{n-k}, I_k, X) \\ \hline O & \lambda^b I_k \end{array}\right]$$

$$= \left[\begin{array}{c|c|c} & \overbrace{}^{n-2k} & \overbrace{}^{k} \\ \lambda^a J^b_k & (S^a T^b)_{12} & (S^a T^b)_{13} \\ \hline O & \lambda^a J^b_{n-2k} & (S^a T^b)_{23} \\ \hline O & O & \lambda^b I_k \end{array}\right] \begin{array}{l} \}k \\ \\ \}n-2k \\ \\ \end{array}$$

Our construction

So, we consider the following partition

$$S^a T^b = \left[\begin{array}{c|c} \lambda^a J^b_{n-k} & \lambda^a \sigma_b(J_{n-k}, \lambda I_k, Y) + \lambda^b \sigma_a(\lambda I_{n-k}, I_k, X) \\ \hline O & \lambda^b I_k \end{array}\right]$$

$$= \left[\begin{array}{c|c|c} \lambda^a J^b_k & (S^a T^b)_{12} & (S^a T^b)_{13} \\ \hline O & \lambda^a J^b_{n-2k} & (S^a T^b)_{23} \\ \hline O & O & \lambda^b I_k \end{array}\right] \begin{array}{l} \}k \\ \\ \}n-2k \end{array}$$

($n-2k$ over the second column, k over the third column)

where, as a consequence of Lemma 5,

$$(S^a T^b)_{12} = \lambda^a \begin{bmatrix} \binom{b}{k} & \binom{b}{k+1} & \cdots & \binom{b}{n-k-1} \\ \binom{b}{k-1} & \binom{b}{k} & \cdots & \binom{b}{n-k-2} \\ \vdots & \vdots & & \vdots \\ \binom{b}{1} & \binom{b}{2} & \cdots & \binom{b}{n-2k} \end{bmatrix}. \qquad (10)$$

Our construction

Moreover, if we assume that

$$X = \begin{bmatrix} X_1 \\ X_2 \end{bmatrix} \quad \text{where } X_1 \in \mathbb{F}_q^{k\times k},\ X_2 \in \mathbb{F}_q^{(n-2k)\times k},$$

Our construction

Moreover, if we assume that

$$X = \begin{bmatrix} X_1 \\ X_2 \end{bmatrix} \quad \text{where } X_1 \in \mathbb{F}_q^{k\times k},\ X_2 \in \mathbb{F}_q^{(n-2k)\times k},$$

then, from Lemma 6, it follows that

$$(S^a T^b)_{13} = \begin{bmatrix} c & e_1 & e_2 & \cdots & e_{k-2} & e_{k-1} \\ 0 & c & e_1 & \cdots & e_{k-3} & e_{k-2} \\ 0 & 0 & c & \cdots & e_{k-4} & e_{k-3} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & c & e_1 \\ 0 & 0 & 0 & \cdots & 0 & c \end{bmatrix} X_1$$

$$+ \begin{bmatrix} e_k & e_{k+1} & e_{k+2} & \cdots & e_{n-k-2} & e_{n-k-1} \\ e_{k-1} & e_k & e_{k+1} & \cdots & e_{n-k-3} & e_{n-k-2} \\ e_{k-2} & e_{k-1} & e_k & \cdots & e_{n-k-4} & e_{n-k-3} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ e_2 & e_3 & e_4 & \cdots & e_{n-2k-2} & e_{n-2k-1} \\ e_1 & e_2 & e_3 & \cdots & e_{n-2k-3} & e_{n-2k} \end{bmatrix} X_2. \qquad (11)$$

Our construction

According to (4), the orbit code $\mathfrak{C}$ generated by the action of $\mathbf{H}$ on $\mathcal{U}_k$ is

$$\begin{aligned}\mathfrak{C} &= \left\{\mathcal{U}_k \cdot (S^a T^b) \mid 0 \leq a < q-1,\ 0 \leq b < q(q-1)\right\} \\ &= \left\{\text{rowspace}\left(\left[\begin{array}{ccc} \lambda^a J_k^b & (S^a T^b)_{12} & (S^a T^b)_{13} \end{array}\right]\right)\right. \\ &\qquad \left. \mid 0 \leq a < q-1,\ 0 \leq b < q(q-1)\right\}.\end{aligned}$$

Our construction

According to (4), the orbit code $\mathfrak{C}$ generated by the action of $\mathbf{H}$ on $\mathcal{U}_k$ is

$$\begin{aligned}\mathfrak{C} &= \left\{\mathcal{U}_k \cdot (S^a T^b) \mid 0 \leq a < q-1,\ 0 \leq b < q(q-1)\right\} \\ &= \left\{\text{rowspace}\left(\left[\begin{array}{ccc} \lambda^a J_k^b & (S^a T^b)_{12} & (S^a T^b)_{13} \end{array}\right]\right)\right. \\ &\qquad\qquad \left. \mid 0 \leq a < q-1,\ 0 \leq b < q(q-1)\right\}.\end{aligned}$$

Note that, according to (5),

$$d(\mathcal{U}_k, \mathcal{U}_k \cdot (S^a T^b)) = 2 \text{ rank}\left[\begin{array}{cc} (S^a T^b)_{12} & (S^a T^b)_{13} \end{array}\right] \leq 2k.$$

Our construction

According to (4), the orbit code $\mathfrak{C}$ generated by the action of $\mathbf{H}$ on $\mathcal{U}_k$ is

$$\begin{aligned}\mathfrak{C} &= \left\{\mathcal{U}_k \cdot (S^a T^b) \mid 0 \leq a < q-1,\ 0 \leq b < q(q-1)\right\} \\ &= \left\{\text{rowspace}\left(\left[\begin{array}{ccc} \lambda^a J_k^b & (S^a T^b)_{12} & (S^a T^b)_{13} \end{array}\right]\right)\right. \\ &\qquad \left. \mid 0 \leq a < q-1,\ 0 \leq b < q(q-1)\right\}.\end{aligned}$$

Note that, according to (5),

$$d(\mathcal{U}_k, \mathcal{U}_k \cdot (S^a T^b)) = 2 \operatorname{rank}\left[\begin{array}{cc} (S^a T^b)_{12} & (S^a T^b)_{13} \end{array}\right] \leq 2k.$$

Our next goal will be to choose X in such a way that

$$\operatorname{rank}\left[\begin{array}{cc} (S^a T^b)_{12} & (S^a T^b)_{13} \end{array}\right] = k, \quad \text{for all } S^a T^b \in \mathbf{H} \setminus \operatorname{stab}_{\mathbf{H}}(\mathcal{U}_k).$$

Our construction

According to (4), the orbit code $\mathfrak{C}$ generated by the action of $\mathbf{H}$ on $\mathcal{U}_k$ is

$$\begin{aligned}\mathfrak{C} &= \left\{\mathcal{U}_k \cdot (S^a T^b) \mid 0 \leq a < q-1,\ 0 \leq b < q(q-1)\right\} \\ &= \left\{\text{rowspace}\left(\left[\begin{array}{ccc} \lambda^a J_k^b & (S^a T^b)_{12} & (S^a T^b)_{13} \end{array}\right]\right)\right. \\ &\qquad \left. \mid 0 \leq a < q-1,\ 0 \leq b < q(q-1)\right\}.\end{aligned}$$

Note that, according to (5),

$$d(\mathcal{U}_k, \mathcal{U}_k \cdot (S^a T^b)) = 2 \operatorname{rank}\left[\begin{array}{cc} (S^a T^b)_{12} & (S^a T^b)_{13} \end{array}\right] \leq 2k.$$

Our next goal will be to choose X in such a way that

$$\operatorname{rank}\left[\begin{array}{cc} (S^a T^b)_{12} & (S^a T^b)_{13} \end{array}\right] = k, \quad \text{for all } S^a T^b \in \mathbf{H} \setminus \operatorname{stab}_{\mathbf{H}}(\mathcal{U}_k).$$

Consequently, $d(\mathfrak{C}) = 2k$, and the minimum distance of our code will be maximal for a concrete choice of X.

Our construction

Theorem 8

If $X_1 \neq O$, *then* $\mathrm{stab}_{\mathbf{H}}(\mathcal{U}_k) = \langle ST^q \rangle$.

Our construction

Theorem 8

If $X_1 \neq O$, *then* $\mathrm{stab}_{\mathbf{H}}(\mathcal{U}_k) = \langle ST^q \rangle$.

Recall that by means of (6) we obtain

$$\mathrm{stab}_{\mathbf{H}}(\mathcal{U}_k) = \left\{ S^a T^b \in \mathbf{H} \mid (S^a T^b)_{12} = O \text{ and } (S^a T^b)_{13} = O \right\}.$$

Our construction

Theorem 8

If $X_1 \neq O$, *then* $\mathrm{stab}_{\mathbf{H}}(\mathcal{U}_k) = \langle ST^q \rangle$.

Recall that by means of (6) we obtain

$$\mathrm{stab}_{\mathbf{H}}(\mathcal{U}_k) = \left\{ S^a T^b \in \mathbf{H} \mid (S^a T^b)_{12} = O \text{ and } (S^a T^b)_{13} = O \right\}.$$

Moreover, $\langle ST^q \rangle = \left\{ S^a T^b \in \mathbf{H} \mid b = qa,\ 0 \leq a < q-1 \right\} \cong C_{q-1}$.

Our construction

Theorem 8

If $X_1 \neq O$, *then* $\mathrm{stab}_{\mathbf{H}}(\mathcal{U}_k) = \langle ST^q \rangle$.

Recall that by means of (6) we obtain

$$\mathrm{stab}_{\mathbf{H}}(\mathcal{U}_k) = \left\{ S^a T^b \in \mathbf{H} \mid (S^a T^b)_{12} = O \text{ and } (S^a T^b)_{13} = O \right\}.$$

Moreover, $\langle ST^q \rangle = \left\{ S^a T^b \in \mathbf{H} \mid b = qa,\ 0 \leq a < q-1 \right\} \cong C_{q-1}$.

Then

$$\left\{ S^a T^b \in \mathbf{H} \mid b = qa,\ 0 \leq a < q-1 \right\} = \left\{ S^a T^b \in \mathbf{H} \mid (S^a T^b)_{12} = O \text{ and } (S^a T^b)_{13} = O \right\}.$$

Our construction

Theorem 9

If

$$X_1 = I_k \quad \text{and} \quad X_2 = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}, \tag{12}$$

then

$$\operatorname{rank} \begin{bmatrix} (S^a T^b)_{12} & (S^a T^b)_{13} \end{bmatrix} = k, \quad \text{for all } S^a T^b \in \mathbf{H} \setminus \operatorname{stab}_{\mathbf{H}}(\mathcal{U}_k).$$

Our construction

Theorem 9

If

$$X_1 = I_k \quad \text{and} \quad X_2 = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}, \tag{12}$$

then

$$\operatorname{rank} \begin{bmatrix} (S^a T^b)_{12} & (S^a T^b)_{13} \end{bmatrix} = k, \quad \text{for all } S^a T^b \in \mathbf{H} \setminus \operatorname{stab}_{\mathbf{H}}(\mathcal{U}_k).$$

Let $S^a T^b \in \mathbf{H} \setminus \operatorname{stab}_{\mathbf{H}}(\mathcal{U}_k)$. From Theorem 8, $0 \leq a < q-1$, $0 \leq b < q(q-1)$ and $b \neq qa$.

Our construction

Theorem 9

If

$$X_1 = I_k \quad \text{and} \quad X_2 = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}, \tag{12}$$

then

$$\operatorname{rank} \begin{bmatrix} (S^a T^b)_{12} & (S^a T^b)_{13} \end{bmatrix} = k, \quad \text{for all } S^a T^b \in \mathbf{H} \setminus \operatorname{stab}_{\mathbf{H}}(\mathcal{U}_k).$$

Let $S^a T^b \in \mathbf{H} \setminus \operatorname{stab}_{\mathbf{H}}(\mathcal{U}_k)$. From Theorem 8, $0 \leq a < q-1$, $0 \leq b < q(q-1)$ and $b \neq qa$.

This means that $e_1 = \dfrac{\lambda^a}{\lambda - 1} b \neq 0$.

Our construction

Now, by (11) and (12), it follows that

$$(S^a T^b)_{13} = \begin{bmatrix} c+e_k & e_1 & e_2 & e_3 & \cdots & e_{k-2} & e_{k-1} \\ e_{k-1} & c & e_1 & e_2 & \cdots & e_{k-3} & e_{k-2} \\ e_{k-2} & 0 & c & e_1 & \cdots & e_{k-4} & e_{k-3} \\ e_{k-3} & 0 & 0 & c & \cdots & e_{k-5} & e_{k-4} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ e_2 & 0 & 0 & 0 & \cdots & c & e_1 \\ e_1 & 0 & 0 & 0 & \cdots & 0 & c \end{bmatrix}.$$

Our construction

Now, by (11) and (12), it follows that

$$(S^a T^b)_{13} = \begin{bmatrix} 0+e_k & e_1 & e_2 & e_3 & \cdots & e_{k-2} & e_{k-1} \\ e_{k-1} & 0 & e_1 & e_2 & \cdots & e_{k-3} & e_{k-2} \\ e_{k-2} & 0 & 0 & e_1 & \cdots & e_{k-4} & e_{k-3} \\ e_{k-3} & 0 & 0 & 0 & \cdots & e_{k-5} & e_{k-4} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ e_2 & 0 & 0 & 0 & \cdots & 0 & e_1 \\ e_1 & 0 & 0 & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

If $c = 0$, then $\det(S^a T^b)_{13} = (-1)^k e_1^k \neq 0$ and $\operatorname{rank}(S^a T^b)_{13} = k$.

Our construction

Now, by (11) and (12), it follows that

$$(S^a T^b)_{13} = \begin{bmatrix} c+e_k & e_1 & e_2 & e_3 & \cdots & e_{k-2} & e_{k-1} \\ e_{k-1} & c & e_1 & e_2 & \cdots & e_{k-3} & e_{k-2} \\ e_{k-2} & 0 & c & e_1 & \cdots & e_{k-4} & e_{k-3} \\ e_{k-3} & 0 & 0 & c & \cdots & e_{k-5} & e_{k-4} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ e_2 & 0 & 0 & 0 & \cdots & c & e_1 \\ e_1 & 0 & 0 & 0 & \cdots & 0 & c \end{bmatrix}.$$

If $c = 0$, then $\det(S^a T^b)_{13} = (-1)^k e_1^k \neq 0$ and $\operatorname{rank}(S^a T^b)_{13} = k$.

If $c \neq 0$, it follows that $k - 1 \leq \operatorname{rank}(S^a T^b)_{13} \leq k$.

Our construction

Now, by (11) and (12), it follows that

$$(S^a T^b)_{13} = \begin{bmatrix} c+e_k & e_1 & e_2 & e_3 & \cdots & e_{k-2} & e_{k-1} \\ e_{k-1} & c & e_1 & e_2 & \cdots & e_{k-3} & e_{k-2} \\ e_{k-2} & 0 & c & e_1 & \cdots & e_{k-4} & e_{k-3} \\ e_{k-3} & 0 & 0 & c & \cdots & e_{k-5} & e_{k-4} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ e_2 & 0 & 0 & 0 & \cdots & c & e_1 \\ e_1 & 0 & 0 & 0 & \cdots & 0 & c \end{bmatrix}.$$

If $c = 0$, then $\det(S^a T^b)_{13} = (-1)^k e_1^k \neq 0$ and $\operatorname{rank}(S^a T^b)_{13} = k$.

If $c \neq 0$, it follows that $k - 1 \leq \operatorname{rank}(S^a T^b)_{13} \leq k$.

Assume that $\operatorname{rank}(S^a T^b)_{13} = k - 1$.

Our construction

Now, by (11) and (12), it follows that

$$(S^a T^b)_{13} = \begin{bmatrix} c+e_k & e_1 & e_2 & e_3 & \cdots & e_{k-2} & e_{k-1} \\ e_{k-1} & c & e_1 & e_2 & \cdots & e_{k-3} & e_{k-2} \\ e_{k-2} & 0 & c & e_1 & \cdots & e_{k-4} & e_{k-3} \\ e_{k-3} & 0 & 0 & c & \cdots & e_{k-5} & e_{k-4} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ e_2 & 0 & 0 & 0 & \cdots & c & e_1 \\ e_1 & 0 & 0 & 0 & \cdots & 0 & c \end{bmatrix}.$$

If $c = 0$, then $\det(S^a T^b)_{13} = (-1)^k e_1^k \neq 0$ and $\operatorname{rank}(S^a T^b)_{13} = k$.

If $c \neq 0$, it follows that $k - 1 \leq \operatorname{rank}(S^a T^b)_{13} \leq k$.

Assume that $\operatorname{rank}(S^a T^b)_{13} = k - 1$. Then

$$0 = \det(S^a T^b)_{13}$$

Our construction

Now, by (11) and (12), it follows that

$$(S^a T^b)_{13} = \begin{bmatrix} c+e_k & e_1 & e_2 & e_3 & \cdots & e_{k-2} & e_{k-1} \\ e_{k-1} & c & e_1 & e_2 & \cdots & e_{k-3} & e_{k-2} \\ e_{k-2} & 0 & c & e_1 & \cdots & e_{k-4} & e_{k-3} \\ e_{k-3} & 0 & 0 & c & \cdots & e_{k-5} & e_{k-4} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ e_2 & 0 & 0 & 0 & \cdots & c & e_1 \\ e_1 & 0 & 0 & 0 & \cdots & 0 & c \end{bmatrix}.$$

If $c = 0$, then $\det(S^a T^b)_{13} = (-1)^k e_1^k \neq 0$ and $\operatorname{rank}(S^a T^b)_{13} = k$.

If $c \neq 0$, it follows that $k - 1 \leq \operatorname{rank}(S^a T^b)_{13} \leq k$.

Assume that $\operatorname{rank}(S^a T^b)_{13} = k - 1$. Then

$$0 = \det(S^a T^b)_{13} = \det \begin{bmatrix} c+e_k & \boldsymbol{u} \\ \boldsymbol{v}^T & M \end{bmatrix} \tag{13}$$

Our construction

Now, by (11) and (12), it follows that

$$(S^a T^b)_{13} = \begin{bmatrix} c+e_k & e_1 & e_2 & e_3 & \cdots & e_{k-2} & e_{k-1} \\ e_{k-1} & c & e_1 & e_2 & \cdots & e_{k-3} & e_{k-2} \\ e_{k-2} & 0 & c & e_1 & \cdots & e_{k-4} & e_{k-3} \\ e_{k-3} & 0 & 0 & c & \cdots & e_{k-5} & e_{k-4} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ e_2 & 0 & 0 & 0 & \cdots & c & e_1 \\ e_1 & 0 & 0 & 0 & \cdots & 0 & c \end{bmatrix}.$$

If $c = 0$, then $\det(S^a T^b)_{13} = (-1)^k e_1^k \neq 0$ and $\operatorname{rank}(S^a T^b)_{13} = k$.

If $c \neq 0$, it follows that $k - 1 \leq \operatorname{rank}(S^a T^b)_{13} \leq k$.

Assume that $\operatorname{rank}(S^a T^b)_{13} = k - 1$. Then

$$0 = \det(S^a T^b)_{13} = \det \begin{bmatrix} c+e_k & \boldsymbol{u} \\ \boldsymbol{v}^T & M \end{bmatrix} \tag{13}$$

where $\boldsymbol{u} = \begin{bmatrix} e_1 & e_2 & e_3 & \cdots & e_{k-2} \end{bmatrix}$, $\boldsymbol{v} = \begin{bmatrix} e_{k-1} & e_{k-2} & e_{k-3} & \cdots & e_1 \end{bmatrix}$, and $\det(M) = c^{k-1} \neq 0$.

Our construction

Assume that $\operatorname{rank}\left[\begin{array}{cc}(S^aT^b)_{12} & (S^aT^b)_{13}\end{array}\right] = k-1$.

Our construction

Assume that $\operatorname{rank}\left[\begin{array}{cc}(S^aT^b)_{12} & (S^aT^b)_{13}\end{array}\right] = k-1$. Then

$$k-1 = \operatorname{rank}\left[\begin{array}{c|ccccc} \lambda^a\binom{b}{k} & e_1 & e_2 & e_3 & \cdots & e_{k-1} \\ \hline \lambda^a\binom{b}{k-1} & c & e_1 & e_2 & \cdots & e_{k-2} \\ \lambda^a\binom{b}{k-2} & 0 & c & e_1 & \cdots & e_{k-3} \\ \lambda^a\binom{b}{k-3} & 0 & 0 & c & \cdots & e_{k-4} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ \lambda^a\binom{b}{1} & 0 & 0 & 0 & \cdots & c \end{array}\right] = \operatorname{rank}\left[\begin{array}{cc} e_k & \boldsymbol{u} \\ \boldsymbol{v}^T & M \end{array}\right], \qquad (14)$$

where we have used that $\lambda^a\binom{b}{i} = (\lambda-1)e_i$.

Our construction

Assume that $\operatorname{rank}\left[\begin{array}{cc}(S^aT^b)_{12} & (S^aT^b)_{13}\end{array}\right] = k-1$. Then

$$k-1 = \operatorname{rank}\left[\begin{array}{c|cccc} \lambda^a\binom{b}{k} & e_1 & e_2 & e_3 & \cdots & e_{k-1} \\ \hline \lambda^a\binom{b}{k-1} & c & e_1 & e_2 & \cdots & e_{k-2} \\ \lambda^a\binom{b}{k-2} & 0 & c & e_1 & \cdots & e_{k-3} \\ \lambda^a\binom{b}{k-3} & 0 & 0 & c & \cdots & e_{k-4} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ \lambda^a\binom{b}{1} & 0 & 0 & 0 & \cdots & c \end{array}\right] = \operatorname{rank}\left[\begin{array}{cc} e_k & \boldsymbol{u} \\ \boldsymbol{v}^T & M \end{array}\right], \qquad (14)$$

where we have used that $\lambda^a\binom{b}{i} = (\lambda-1)e_i$.

Now,

$$0 = \det\left[\begin{array}{cc} c+e_k & \boldsymbol{u} \\ \boldsymbol{v}^T & M \end{array}\right] = \det\left[\begin{array}{cc} c & \boldsymbol{u} \\ \boldsymbol{0}^T & M \end{array}\right] + \det\left[\begin{array}{cc} e_k & \boldsymbol{u} \\ \boldsymbol{v}^T & M \end{array}\right] = c^k + 0,$$

which is a contradiction since $c \neq 0$.

Our construction

Assume that $\operatorname{rank}\left[\begin{array}{cc}(S^aT^b)_{12} & (S^aT^b)_{13}\end{array}\right] = k-1$. Then

$$k-1 = \operatorname{rank}\left[\begin{array}{c|cccc} \lambda^a\binom{b}{k} & e_1 & e_2 & e_3 & \cdots & e_{k-1} \\ \hline \lambda^a\binom{b}{k-1} & c & e_1 & e_2 & \cdots & e_{k-2} \\ \lambda^a\binom{b}{k-2} & 0 & c & e_1 & \cdots & e_{k-3} \\ \lambda^a\binom{b}{k-3} & 0 & 0 & c & \cdots & e_{k-4} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ \lambda^a\binom{b}{1} & 0 & 0 & 0 & \cdots & c \end{array}\right] = \operatorname{rank}\left[\begin{array}{cc} e_k & \boldsymbol{u} \\ \boldsymbol{v}^T & M \end{array}\right], \qquad (14)$$

where we have used that $\lambda^a\binom{b}{i} = (\lambda-1)e_i$.

Now,

$$0 = \det\left[\begin{array}{cc} c+e_k & \boldsymbol{u} \\ \boldsymbol{v}^T & M \end{array}\right] = \det\left[\begin{array}{cc} c & \boldsymbol{u} \\ \boldsymbol{0}^T & M \end{array}\right] + \det\left[\begin{array}{cc} e_k & \boldsymbol{u} \\ \boldsymbol{v}^T & M \end{array}\right] = c^k + 0,$$

which is a contradiction since $c \neq 0$.

Consequently $\operatorname{rank}\left[\begin{array}{cc}(S^aT^b)_{12} & (S^aT^b)_{13}\end{array}\right] = k$, for all $S^aT^b \in \mathbf{H} \setminus \operatorname{stab}_{\mathbf{H}}(\mathcal{U}_k)$.

Our construction

Our construction

Theorem 10

Assume that q is a prime number such that $q \geq n - k$ where k and n are nonnegative integers such that $2k \leq n$.
Assume also that $\lambda \in \mathbb{F}_q$ is a primitive element.
Consider the upper triangular matrices S and T defined in (7), and
$X = \begin{bmatrix} X_1 \\ X_2 \end{bmatrix}$ *where X_1 and X_2 are defined in (12).*
If $\mathbf{H} = \langle S, T \rangle$ is the Abelian non-cyclic subgroup of GL_n given in (8), and $\mathfrak{C}$ is the orbit code defined in (4), then $|\mathfrak{C}| = q(q-1)$ and $d(\mathfrak{C}) = 2k$.

Overview

1 Introduction

2 Preliminaries

3 Our construction

4 Open questions

Open questions

If q is a prime number such that $n - k \leq q$, then

- $e_1 = 0$ if and only if $b = qa$ for $0 \leq a < q - 1$,
- $e_1 \neq 0$, for the remaining cases.

Open questions

If q is a prime number such that $n - k \leq q$, then

- $e_1 = 0$ if and only if $b = qa$ for $0 \leq a < q - 1$,
- $e_1 \neq 0$, for the remaining cases.

$$\mathrm{stab}_{\mathbf{H}}(\mathcal{U}_k) = \langle ST^q \rangle = \left\{ S^a T^b \in \mathbf{H} \mid b = qa,\ 0 \leq a < q - 1 \right\} \cong C_{q-1}.$$

$$(S^a T^b)_{12} = O, \qquad (S^a T^b)_{13} = O.$$

Open questions

If q is a prime number such that $n-k \leq q$, then

- $e_1 = 0$ if and only if $b = qa$ for $0 \leq a < q-1$,
- $e_1 \neq 0$, for the remaining cases.

$$\mathrm{stab}_{\mathbf{H}}(\mathcal{U}_k) = \langle ST^q \rangle = \left\{ S^a T^b \in \mathbf{H} \mid b = qa,\ 0 \leq a < q-1 \right\} \cong C_{q-1}.$$

$$(S^a T^b)_{12} = O, \qquad (S^a T^b)_{13} = O.$$

However, if $q = p^r$ where p is a prime number and $r \geq 2$, then

- $e_1 = 0$ if and only if $b = pa$ for $0 \leq a < q-1$,
- $e_1 \neq 0$, for the remaining cases.

Open questions

If q is a prime number such that $n-k \leq q$, then

- $e_1 = 0$ if and only if $b = qa$ for $0 \leq a < q-1$,
- $e_1 \neq 0$, for the remaining cases.

$$\mathrm{stab}_{\mathbf{H}}(\mathcal{U}_k) = \langle ST^q \rangle = \left\{ S^a T^b \in \mathbf{H} \mid b = qa,\ 0 \leq a < q-1 \right\} \cong C_{q-1}.$$

$$(S^a T^b)_{12} = O, \qquad (S^a T^b)_{13} = O.$$

However, if $q = p^r$ where p is a prime number and $r \geq 2$, then

- $e_1 = 0$ if and only if $b = pa$ for $0 \leq a < q-1$,
- $e_1 \neq 0$, for the remaining cases.

In this case

$$\mathrm{stab}_{\mathbf{H}}(\mathcal{U}_k) = \begin{cases} \langle ST^p \rangle, & \text{if } n-k \leq p, \\ ?, & \text{if } p < n-k \leq q. \end{cases}$$

Open questions

If q is a prime number such that $n-k \leq q$, then

- $e_1 = 0$ if and only if $b = qa$ for $0 \leq a < q-1$,
- $e_1 \neq 0$, for the remaining cases.

$$\mathrm{stab}_{\mathbf{H}}(\mathcal{U}_k) = \langle ST^q \rangle = \left\{ S^a T^b \in \mathbf{H} \mid b = qa,\ 0 \leq a < q-1 \right\} \cong C_{q-1}.$$

$$(S^a T^b)_{12} = O, \qquad (S^a T^b)_{13} = O.$$

However, if $q = p^r$ where p is a prime number and $r \geq 2$, then

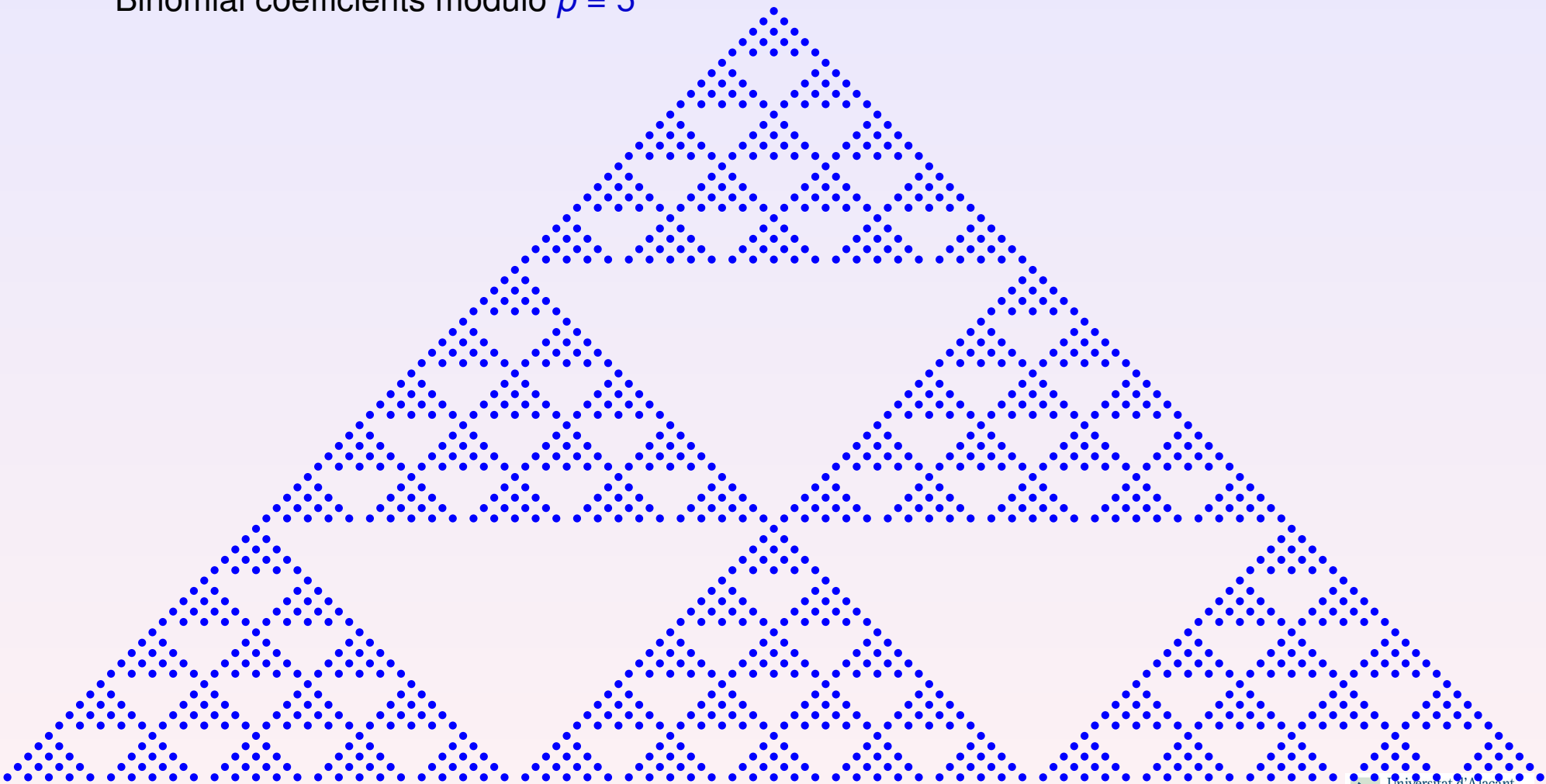
- $e_1 = 0$ if and only if $b = pa$ for $0 \leq a < q-1$,
- $e_1 \neq 0$, for the remaining cases.

In this case

$$\mathrm{stab}_{\mathbf{H}}(\mathcal{U}_k) = \begin{cases} \langle ST^p \rangle, & \text{if } n-k \leq p, \\ ?, & \text{if } p < n-k \leq q. \end{cases}$$

$$(S^a T^b)_{12} = \lambda^a \begin{bmatrix} \binom{b}{k} & \binom{b}{k+1} & \cdots & \binom{b}{n-k-1} \\ \binom{b}{k-1} & \binom{b}{k} & \cdots & \binom{b}{n-k-2} \\ \vdots & \vdots & & \vdots \\ \binom{b}{1} & \binom{b}{2} & \cdots & \binom{b}{n-2k} \end{bmatrix} \neq O.$$

Binomial coefficients modulo $p = 5$



A Construction of Orbit Codes

Joan-Josep Climent[1] Verónica Requena[2] Xaro Soler-Escrivà[1]

[1]Departament de Matemàtiques, Universitat d'Alacant
[2]Departamento de Estadística, Matemáticas e Informática
Universidad Miguel Hernández de Elche

5ICMCTA, Vihula Manor. August 28-31, 2017

Universitat d'Alacant
Universidad de Alicante

A Construction of Orbit Codes

Joan-Josep Climent[1] Verónica Requena[2] Xaro Soler-Escrivà[1]

[1]Departament de Matemàtiques, Universitat d'Alacant
[2]Departamento de Estadística, Matemáticas e Informática
Universidad Miguel Hernández de Elche

5ICMCTA, Vihula Manor. August 28-31, 2017

Universitat d'Alacant
Universidad de Alicante

Overview

5 References

R. Ahlswede, N. Cai, S.-Y. R. Li and R. W. Yeung.

Network information flow.

IEEE Transactions on Information Theory, **46(4)**: 1204–1216 (2000).

F. Bardestani and A. Iranmanesh.

Cyclic orbit codes with the normalizer of a Singer subgroup.

Journal of Sciences, Islamic Republic of Iran, **26(1)**: 49–55 (2015).

D. Bartoli and F. Pavese.

A note on equidistant subspace codes.

Discrete Applied Mathematics, **198**: 291–296 (2016).

E. Ben-Sasson, T. Etzion, A. Gabizon and N. Raviv.

Subspace polynomials and cyclic subspace codes.

IEEE Transactions on Information Theory, **62(3)**: 1157–1165 (2016).

A. Cossidente and F. Pavese.

On subspace codes.

Designs, Codes and Cryptography, **78(2)**: 527–531 (2016).

T. Etzion and A. Vardy.

Error-correcting codes in projective space.

IEEE Transactions on Information Theory, **57(2)**: 1165–1173 (2011).

A. Ghatak.

Construction of Singer subgroup orbit codes based on cyclic difference sets.

In *Proceedings of the Twentieth National Conference on Communications (NCC 2014)*, pages 1–4. IEEE, Kanpur, India, February 2014.

H. GLUESING-LUERSSEN, K. MORRISON and C. TROHA.

Cyclic orbit codes and stabilizer subfields.

Advances in Mathematics of Communications, **9(2)**: 177–197 (2015).

H. GLUESING-LUERSSEN and C. TROHA.

Construction of subspace codes through linkage.

Advances in Mathematics of Communications, **10(3)**: 525–540 (2016).

E. G. GORLA and A. RAVAGNANI.

Equidistant subspace codes.

Linear Algebra and its Applications, **490**: 48–65 (2016).

T. HO, R. KOETTER, M. MÉDARD, D. R. KARGER and M. EFFROS.

The benefits of coding over routing in a randomized setting.

In *Proceedings of the 2003 IEEE International Symposium on Information Theory (ISIT 2003)*, page 442. IEEE, Yokohama, Japan, June/July 2003.

T. HO, M. MÉDARD, R. KOETTER, D. R. KARGER, M. EFFROS, J. SHI and B. LEONG.

A random linear network coding approach to multicast.

IEEE Transactions on Information Theory, **52(10)**: 4413–4430 (2006).

R. KOETTER and F. R. KSCHISCHANG.

Coding for errors and erasures in random network coding.

IEEE Transactions on Information Theory, **54(8)**: 3579–3591 (2008).

R. KOETTER and M. MÉDARD.

An algebraic approach to network coding.

IEEE/ACM Transactions on Networking, **11(5)**: 782–795 (2003).

S.-Y. R. LI, R. W. YEUNG and N. CAI.

Linear network coding.

IEEE Transactions on Information Theory, **49(2)**: 371–381 (2003).

J. ROSENTHAL and A.-L. TRAUTMANN.

A complete characterization of irreducible cyclic orbit codes and their Plücker embedding.

Designs, Codes and Cryptography, **66**: 275–289 (2013).

N. SILBERSTEIN and A.-L. TRAUTMANN.

New lower bounds for constant dimension codes.

In *Proceedings of the 2013 IEEE International Symposium on Information Theory (ISIT 2013)*, pages 514–518. IEEE, Istanbul, July 2013.

A.-L. TRAUTMANN.

Isometry and automorphisms of constant dimension codes.

Advances in Mathematics of Communications, **7(2)**: 147–160 (2013).

A.-L. TRAUTMANN, F. MANGANIELLO, M. BRAUN and J. ROSENTHAL.

Cyclic orbit codes.

IEEE Transactions on Information Theory, **59(11)**: 7386–7404 (2013).

A.-L. TRAUTMANN, F. MANGANIELLO and J. ROSENTHAL.

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

In *Proceedings of the 2010 IEEE Information Theory Workshop (ITW 2010)*. IEEE, Dublin, Ireland, August 2010.

R. W. YEUNG and Z. ZHANG.

Distributed source coding for satellite communications.

IEEE Transactions on Information Theory, **45(4)**: 1111–1120 (1999).