Universitat d'Alacant
Universidad de Alicante

University of Zurich[UZH]

Algebraic Coding Theory e-Summer School **ACT21**

An Orbital Construction of Optimum Distance Flag Codes

Miguel Ángel Navarro-Pérez

Joint work with Clementa Alonso-González and Xaro Soler-Escrivà

June 9, 2021

miguelangel.np@ua.es

Outline

1. Constant dimension codes
2. Flag codes
   - Optimum distance full flag codes
3. Our construction

Notation

Let...

- q be a prime power,
- $\mathbb{F}_q$ denote the *finite field* with q elements,
- n be a positive integer.
- $\mathbb{F}_q^n$ is the n-dimensional vector space over $\mathbb{F}_q$,
- $\mathcal{G}_q(k, n)$, the *Grassmannian* of dimension k.

Outline

1. Constant dimension codes
2. Flag codes
   - Optimum distance full flag codes
3. Our construction

Constant dimension codes

Definition

A **constant dimension code** $\mathcal{C}$ in $\mathcal{G}_q(k,n)$ is a nonempty collection of k-dimensional subspaces of $\mathbb{F}_q^n$.

Given two subspaces $\mathcal{U},\mathcal{V}$ of $\mathbb{F}_q^n$, with $\dim(\mathcal{U}) = \dim(\mathcal{V}) = k$, then

$$d_S(\mathcal{U},\mathcal{V}) = 2\left(k - \dim(\mathcal{U}\cap\mathcal{V})\right).$$

Group action

For every $1 \leqslant k \leqslant n-1$, the group $GL(n,q)$ acts on the Grassmannian $\mathcal{G}_q(k,n)$:

$$\mathcal{G}_q(k,n) \times GL(n,q) \to \mathcal{G}_q(k,n), \quad \mathcal{V} \cdot A \mapsto \mathrm{rowsp}(VA),$$

with V a generator matrix of $\mathcal{V}$.

Definition

Given a subspace $\mathcal{V} \in \mathcal{G}_q(k,n)$ and a subgroup T of $GL(n,q)$, the **orbit code** generated by $\mathcal{V}$ (under the action of T) is

$$\mathrm{Orb}_{\mathsf{T}}(\mathcal{V}) = \{\mathcal{V} \cdot A \mid A \in \mathsf{T}\}.$$

Its stabilizer is the subgroup $\mathrm{Stab}_{\mathsf{T}}(\mathcal{V}) = \{A \in \mathsf{T} \mid \mathcal{V} \cdot A = \mathcal{V}\}$ and it holds $|\mathrm{Orb}_{\mathsf{T}}(\mathcal{V})| = |\mathsf{T}|/|\mathrm{Stab}_{\mathsf{T}}(\mathcal{V})|$.

Spread codes

Definition

A *k*-**spread code** $\mathcal{S}$ of $\mathbb{F}_q^n$ is a constant dimension code in $\mathcal{G}_q(k,n)$ such that every nonzero vector of $\mathbb{F}_q^n$ lies on one, and only one, subspace in $\mathcal{S}$. Vector space partition

Properties:

- k-spread codes exist $\Leftrightarrow$ k divides n,
- $d_S(\mathcal{S}) = 2k$ and
- $|\mathcal{S}| = \frac{q^n-1}{q^k-1}$.

Spreads codes

In [13], Manganiello, Gorla and Rosenthal present the next construction of a k-spread code.

Theorem ([13, Th. 1])

Let P be the companion matrix of a primitive polynomial of degree k in $\mathbb{F}_q[x]$. Then the set

$$\mathcal{S} = \{\mathrm{rowsp}(I_k|P^i),\ \mathrm{rowsp}(0_k|I_k) \mid 1 \leqslant i \leqslant q^k - 2\} \qquad (1)$$

is a k-spread of $\mathbb{F}_q^{2k}$.

In [16], the authors provide an orbital description of $\mathcal{S}$.

Spreads as orbit codes

Consider matrices in $GL(2k, q)$

$$g = \left[\begin{array}{c|c} 0_k & I_k \\ \hline I_k & 0_k \end{array}\right] \quad \text{and} \quad g_i = \left[\begin{array}{c|c} I_k & P^i \\ \hline 0_k & I_k \end{array}\right], \ 0 \leqslant i \leqslant q^k - 2.$$

Form the group

$$\mathrm{G} = \left\langle g, g_i, \mid 0 \leqslant i \leqslant q^k - 2 \right\rangle.$$

and take $\mathcal{U}_k = \mathrm{rowsp}(I_k \mid 0_k)$.

Lemma ([16, Lemma 15])

The orbit code $\mathrm{Orb}_{\mathrm{G}}(\mathcal{U}_k) = \mathcal{S}$ is the k-spread code in (1).

Outline

1. Constant dimension codes
2. Flag codes
   - Optimum distance full flag codes
3. Our construction

Full flags

Definition

A **full flag** on $\mathbb{F}_q^n$ is a sequence

$$\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_{n-1})$$

such that

- $\mathcal{F}_1 \subsetneq \mathcal{F}_2 \subsetneq \cdots \subsetneq \mathcal{F}_{n-1}$.
- $\dim(\mathcal{F}_i) = i$, i**-th subspace of** $\mathcal{F}$.

Full flag codes

The **flag distance** between two full flags $\mathcal{F}$ and $\mathcal{F}'$ on $\mathbb{F}_q^n$ is

$$d_f(\mathcal{F},\mathcal{F}') = \sum_{i=1}^{n-1} d_S(\mathcal{F}_i,\mathcal{F}'_i).$$

Definition

A **full flag code** on $\mathbb{F}_q^n$ is a nonempty collection of full flags. Its **minimum distance** is

$$d_f(\mathcal{C}) = \min\{d_f(\mathcal{F},\mathcal{F}') \mid \mathcal{F},\mathcal{F}' \in \mathcal{C},\ \mathcal{F} \neq \mathcal{F}'\}$$

Optimum distance full flag codes

Definition

A full flag code $\mathcal{C}$ on $\mathbb{F}_q^n$ is said to be an **optimum distance flag code** if

$$d_f(\mathcal{C}) = \begin{cases} \frac{n^2}{2} & \text{if } n \text{ is even,} \\ \frac{n^2-1}{2} & \text{if } n \text{ is odd.} \end{cases}$$

Projected codes of flag code

Definition

Let $\mathcal{C}$ be a full flag code on $\mathbb{F}_q^n$. For every $i \in \{1, \ldots, n-1\}$, the **i-projected code of $\mathcal{C}$** is the subspace code $\mathcal{C}_i$ given by the **set of all the i-th subspaces** of flags in $\mathcal{C}$.

$$\mathcal{C}_i = \{\mathcal{F}_i \in \mathcal{G}_q(i,n) \mid (\mathcal{F}_1, \ldots, \mathcal{F}_i, \ldots, \mathcal{F}_{n-1}) \in \mathcal{C}\}.$$

- $\mathcal{C}_i \subseteq \mathcal{G}_q(i,n)$,
- $|\mathcal{C}_i| \leqslant |\mathcal{C}|$.
- If $|\mathcal{C}_1| = \cdots = |\mathcal{C}_{n-1}| = |\mathcal{C}|$ we say that $\mathcal{C}$ is **disjoint**.

Optimum distance flag codes

Theorem ([3, Theorem 3.11])

Let $\mathcal{C}$ be a full flag code on $\mathbb{F}_q^n$. The following statements are equivalent.

1. $\mathcal{C}$ is an **optimum distance** flag code.
2. $\mathcal{C}$ is disjoint and every $\mathcal{C}_i$ attains the maximum (subspace) distance.

For $n = 2k$, we have the following result.

Theorem ([3, Th. 3.12])

Let $\mathcal{C}$ be an optimum distance full flag code on $\mathbb{F}_q^{2k}$. Then $|\mathcal{C}| \leqslant q^k + 1$ and the equality holds if, and only if, $\mathcal{C}_k$ is a k-spread of $\mathbb{F}_q^{2k}$.

Orbit flag codes

Consider a full flag $\mathcal{F}$ on $\mathbb{F}_q^n$ and a matrix $A \in GL(n,q)$, then

$$\mathcal{F} \cdot A = (\mathcal{F}_1 \cdot A, \ldots, \mathcal{F}_{n-1} \cdot A)$$

is a full flag.

Definition

Given a group $\mathsf{T} \subseteq GL(n,q)$, the **orbit flag code** generated by $\mathcal{F}$ (under the action of T) is $\mathrm{Orb}_{\mathsf{T}}(\mathcal{F})$.

- $\mathrm{Orb}_{\mathsf{T}}(\mathcal{F})_i = \mathrm{Orb}_{\mathsf{T}}(\mathcal{F}_i)$
- $\mathrm{Stab}_{\mathsf{T}}(\mathcal{F}) = \bigcap_{i=1}^{n-1} \mathrm{Stab}_{\mathsf{T}}(\mathcal{F}_i)$.

Orbit flag codes

Proposition ([2, Prop. 3.5])

The code $\mathrm{Orb}_{\mathsf{T}}(\mathcal{F})$ is disjoint iff $\mathrm{Stab}_{\mathsf{T}}(\mathcal{F}_1) = \cdots = \mathrm{Stab}_{\mathsf{T}}(\mathcal{F}_{n-1})$.

Proposition ([2, Prop. 3.6])

Take $n = 2k$. If $d_S(\mathrm{Orb}_{\mathsf{T}}(\mathcal{F}_k)) = 2k$, then $\mathrm{Stab}_{\mathsf{T}}(\mathcal{F}_i) \subseteq \mathrm{Stab}_{\mathsf{T}}(\mathcal{F}_k)$, for all $1 \leqslant i \leqslant n-1$.

Proposition ([2, Prop. 3.7])

Take $n = 2k$. If $d_S(\mathrm{Orb}_{\mathsf{T}}(\mathcal{F}_k)) = 2k$ and $\mathrm{Stab}_{\mathsf{T}}(\mathcal{F}_k) \subseteq \mathrm{Stab}_{\mathsf{T}}(\mathcal{F}_i)$, then $\mathrm{Orb}_{\mathsf{T}}(\mathcal{F})$ is an optimum distance flag code.

In particular, if $\mathrm{Stab}_{\mathsf{T}}(\mathcal{F}_k) = \{I_n\}$, we are done.

Outline

1. Constant dimension codes
2. Flag codes
   - Optimum distance full flag codes
3. Our construction

Starting from a k-spread

Let P be the companion matrix of a primitive plynomial of degree k in $\mathbb{F}_q[x]$ and conider the k-spread

$$\mathcal{S} = \{\mathrm{rowsp}(I_k|P^i),\ \mathrm{rowsp}(0_k|I_k) \mid 1 \leqslant i \leqslant q^k - 2\}. \qquad (2)$$

Recall that $\mathcal{S} = \mathrm{Orb}_{\mathsf{G}}(\mathrm{rowsp}(I_k|0_k))$ with

$$\mathsf{G} = \left\langle \left[\begin{array}{c|c} 0_k & I_k \\ \hline I_k & 0_k \end{array}\right], \left[\begin{array}{c|c} I_k & P^i \\ \hline 0_k & I_k \end{array}\right] \mid 0 \leqslant i \leqslant q^k - 2 \right\rangle.$$

- We start analyzing the group structure of G. Consider a primitive element $\alpha \in \mathbb{F}_{q^k}$.
- The field isomorphism $\phi : \mathbb{F}_{q^k} \to \mathbb{F}_q[P]$ such that $\alpha \mapsto \phi(\alpha) = P$ induces a group isomorphism between

$$\bar{\mathsf{G}} = \left\langle \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & \alpha^i \\ 0 & 1 \end{bmatrix}, 1 \leqslant i \leqslant q^k - 2 \right\rangle$$

and

$$\mathsf{G} = \left\langle \left[\begin{array}{c|c} 0_k & I_k \\ \hline I_k & 0_k \end{array}\right], \left[\begin{array}{c|c} I_k & P^i \\ \hline 0_k & I_k \end{array}\right], 1 \leqslant i \leqslant q^k - 2 \right\rangle.$$

Proposition ([2, Prop. 4.2])

$$\mathsf{G} \cong \bar{\mathsf{G}} = \begin{cases} SL(2, q^k) & \text{if } \mathrm{char}(\mathbb{F}_q) = 2, \\ SL(2, q^k) \rtimes \left\langle \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle, & \text{otherwise.} \end{cases}$$

Remark:

Moreover, we can restrict ourselves to the subgroup $\psi(SL(2, q^k))$ of G since

$$\mathcal{S} = \mathrm{Orb}_{\psi(SL(2,q^k))}(\mathrm{rowsp}(I_k|0_k)).$$

Recall that, if we find a subgroup T of $\psi(SL(2, q^k))$ such that:

- $\mathcal{S} = \mathrm{Orb}_{\mathsf{T}}(\mathcal{V})$ and
- $\mathrm{Stab}_{\mathsf{T}}(\mathcal{V}) = \{I_n\}$,

then we can easily provide an optimum distance flag code. In that case, $|\mathsf{T}| = q^k + 1 = |\mathcal{S}|$.

Let $\bar{\mathsf{H}}$ be a Singer subgroup of $SL(2, q^k)$ and consider $\mathsf{H} = \psi(\bar{\mathsf{H}})$. Then H is cyclic of order $q^k + 1$ and, for every $\mathcal{V} \in \mathcal{S}$, it holds:

Lemma ([2, Lemma 4.11])

$$\mathrm{Stab}_{\mathsf{H}}(\mathcal{V}) = \begin{cases} \{I_n\} & \text{if} \quad \mathrm{char}(\mathbb{F}_q) = 2, \\ \{I_n, -I_n\} & \text{if} \quad \mathrm{char}(\mathbb{F}_q) \neq 2. \end{cases}$$

Theorem ([2, Th. 4.14])

Let $\mathcal{F}$ be a full flag on $\mathbb{F}_q^{2k}$ with $\mathcal{F}_k \in \mathcal{S}$. Then $\mathrm{Orb}_{\mathsf{H}}(\mathcal{F})$ is an optimum distance flag code with cardinality

$$\begin{cases} q^k + 1 & \text{if} \quad \mathrm{char}(\mathbb{F}_q) = 2, \\ \frac{q^k+1}{2} & \text{if} \quad \mathrm{char}(\mathbb{F}_q) \neq 2. \end{cases}$$

Proposition ([2, Prop. 4.15])

For odd characteristic: Let $\mathcal{F}$ and $\mathcal{F}'$ be full flags on $\mathbb{F}_q^{2k}$ with $\mathcal{F}_k, \mathcal{F}'_k \in \mathcal{S}$ such that $\mathrm{Orb}_{\mathsf{H}}(\mathcal{F}_k) \neq \mathrm{Orb}_{\mathsf{H}}(\mathcal{F}'_k)$. Then

$$\mathcal{C} = \mathrm{Orb}_{\mathsf{H}}(\mathcal{F}) \cup \mathrm{Orb}_{\mathsf{H}}(\mathcal{F}')$$

is an optimum distance flag code with size $q^k + 1$.


J. L. Alperin and R. B. Bell, *Groups and Representations*. Graduate Texts in Mathematics, Vol. 162. Springer, New York, 1995.


C. Alonso-González, M. A. Navarro-Pérez and X. Soler-Escrivà, *An Orbital Construction of Optimum Distance Flag Codes*, Finite Fields and Their Applications, Vol. 73 (2021), 101861.


C. Alonso-González, M. A. Navarro-Pérez and X. Soler-Escrivà, *Flag Codes from Planar Spreads in Network Coding*, Finite Fields and Their Applications, Vol. 68 (2020), 101745.


C. Alonso-González, M. A. Navarro-Pérez and X. Soler-Escrivà, *Flag Codes from Spreads via Perfect Matchings in Graphs*, `https://arxiv.org/abs/2005.09370` (preprint).


M. Greferath, M. O. Pavčević, N. Silberstein and M. A. Vázquez-Castro, *Network Coding and Subspace Designs*, Springer, 2018.


M. D. Hestenes, *Singer Groups*, Canadian Journal of Mathematics, Vol. XXII, 3 (1970), pp. 492-513.


J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, second edition, 1998.


T. Ho, R. Kötter, M. Médard, D. Karger and M. Effros, *The Benefits of Coding over Routing in a Randomized Setting*, in: IEEE International Symposium on Information Theory, Proceedings (ISIT), Yokohama, Japan, 2003, p. 442.


B. Huppert, *Endliche Gruppen*, Vol. I. Springer-Verlag, New York, 1967.


R. Kötter and F. Kschischang, *Coding for Errors and Erasures in Random Network Coding*, in: IEEE Transactions on Information Theory, Vol. 54 (2008) 3579-3591.


R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*. Cambridge University Press, Cambridge, London, 1994. Revised edition.

D. Liebhold, G. Nebe and A. Vazquez-Castro, *Network Coding with Flags*, Designs, Codes and Cryptography, Vol. 86 (2) (2018) 269-284.

F. Manganiello, E. Gorla and J. Rosenthal, *Spread Codes and Spread Decoding in Network Coding*, in: IEEE International Symposium on Information Theory, Proceedings (ISIT), Toronto, Canada, 2008, pp. 851-855.

R. W. Nóbrega and B. F. Uchôa-Filho, *Multishot Codes for Network Coding: Bounds and a Multilevel Construction*, in: 2009 IEEE International Symposium on Information Theory, Proceedings (ISIT), Seoul, South Korea, 2009, pp. 428-432.

B. Segre, *Teoria di Galois, Fibrazioni Proiettive e Geometrie non Desarguesiane*, Annali di Matematica Pura ed Applicata, Vol. 64 (1964), 1-76.

A.-L. Trautmann, F. Manganiello and J. Rosenthal, *Orbit Codes - A New Concept in the Area of Network Coding* in: 2010 IEEE Information Theory Workshop, ITW 2010 - Proceedings, Dublin, Ireland, 2010, pp. 1-4.

A.-L. Trautmann, F. Manganiello, M. Braun and J. Rosenthal, *Cyclic Orbit Codes* in: IEEE Trans. Inform. Theory, Vol. 59 (11) (2013) 7386-7404.

A.-L. Trautmann and J. Rosenthal, *Constructions of Constant Dimension Codes*, in: M. Greferath et al. (Eds.), Network Coding and Subspace Designs, E-Springer International Publishing AG, 2018, pp. 25-42.

Universitat d'Alacant
Universidad de Alicante

University of Zurich[UZH]

Algebraic Coding Theory e-Summer School **ACT21**

An Orbital Construction of Optimum Distance Flag Codes

Miguel Ángel Navarro-Pérez

Joint work with Clementa Alonso-González and Xaro Soler-Escrivà

June 9, 2021

miguelangel.np@ua.es