A complete characterization of irreducible cyclic orbit codes

Trautmann, A L ; Rosenthal, J

A Complete Characterization of Irreducible Cyclic Orbit Codes*

Anna-Lena Trautmann and Joachim Rosenthal

Institute of Mathematics
University of Zurich, Switzerland
www.math.uzh.ch/aa

Abstract. Constant dimension codes are subsets of the finite Grassmann variety. The study of constant dimension codes with good distances have been central in random linear network coding theory.
Orbit codes represent a subclass of constant dimension codes. They are characterized that the elements of the code can be viewed as the orbit under a group action.
The paper gives a complete characterization of orbit codes that are generated by an irreducible cyclic group, i.e. an irreducible group having one generator. We show how some of the basic properties of these codes, the cardinality and the minimum distance, can be derived using the isomorphism of the vector space and the extension field.

1 Introduction

In network coding one is looking at the transmission of information through a directed graph with possibly several senders and several receivers [1]. One can increase the throughput by linearly combining the information vectors at intermediate nodes of the network. If the underlying topology of the network is unknown we speak about *random linear network coding*. Since linear spaces are invariant under linear combinations, they are what is needed as codewords [5]. It is helpful (e.g. for decoding) to constrain oneself to subspaces of a fixed dimension, in which case we talk about *constant dimension codes*.

The set of all k-dimensional subspaces of a vector space V is often referred to as the Grassmann variety (or simply Grassmannian) and denoted by $\mathcal{G}(k, V)$. *Constant dimension codes* are subsets of $\mathcal{G}(k, \mathbb{F}_q^n)$, where $\mathbb{F}_q$ is some finite field.

The general linear group $GL(V)$ consisting of all invertible transformations acts naturally on the Grassmannian $\mathcal{G}(k, V)$. If $\mathfrak{G} \leq GL(\mathbb{F}_q^n) = GL_n$ is a subgroup then one has an induced action of $\mathfrak{G}$ on the finite Grassmannian $\mathcal{G}(k, \mathbb{F}_q^n)$. Orbits under the $\mathfrak{G}$-action are called *orbit codes* [10]. The set of orbit codes comes with nice algebraic properties. E.g. for the computation of the distance of an orbit code it is enough to compute the distance between the base point and any of its orbit elements. This is in analogy to linear block codes where the distance can also be computed from the weights of the non-zero code words.

Orbit codes can be classified according to the groups used to construct the orbit. In this work we characterize orbit codes generated by irreducible cyclic subgroups of the general linear group.

The paper is structured as follows: The second section gives some preliminaries, first of random network coding and orbit codes. Then some facts on irreducible polynomials are stated and the representation of finite vector spaces as Galois extension fields is explained in 2.2. In part 2.3 we introduce irreducible matrix groups and give some properties, with a focus on the cyclic ones. The main body of the paper is Section 3, where we study the behavior of orbit codes

* Research partially supported by Swiss National Science Foundation Project no. 126948

generated by these groups and compute the cardinality and minimum distances of them. We begin by characterizing primitive orbit codes and then study the non-primitive irreducible ones. Finally we give a conclusion and an outlook in Section 4.

2 Preliminaries

2.1 Random Network Codes

Let $\mathbb{F}_q$ be the finite field with q elements (where $q = p^r$ and p prime). For simplicity we will denote the Grassmannian $\mathcal{G}(k, \mathbb{F}_q^n)$ by $\mathcal{G}(k, n)$. The general linear group of dimension n, GL_n, is the set of all invertible $n \times n$-matrices with entries in $\mathbb{F}_q$. Moreover, the set of all $k \times n$-matrices over $\mathbb{F}_q$ is denoted by $Mat_{k\times n}$.

Let $U \in Mat_{k\times n}$ be a matrix of rank k and

$$\mathcal{U} = \mathrm{rs}(U) := \text{row space}(U) \in \mathcal{G}(k, n).$$

One can notice that the row space is invariant under GL_k-multiplication from the left, i.e. for any $T \in GL_k$

$$\mathcal{U} = \mathrm{rs}(U) = \mathrm{rs}(TU).$$

Thus, there are several matrices that represent a given subspace. A unique representative of these matrices is the one in reduced row echelon form. Any $k \times n$-matrix can be transformed into reduced row echelon form by a $T \in GL_k$.

The *subspace distance* is a metric on $\mathcal{G}(k, n)$ given by

$$\begin{aligned} d_S(\mathcal{U}, \mathcal{V}) =& 2(k - \dim(\mathcal{U} \cap \mathcal{V})) \\ =& 2 \cdot \mathrm{rank} \begin{bmatrix} U \\ V \end{bmatrix} - 2k \end{aligned}$$

for any $\mathcal{U}, \mathcal{V} \in \mathcal{G}(k, n)$ and some respective matrix representations U and V. It is a suitable distance for coding over the erasure channel [5, 9].

A *constant dimension code* $\mathcal{C}$ is simply a subset of the Grassmannian $\mathcal{G}(k, n)$. The minimum distance is defined in the usual way. A code $\mathcal{C} \subset \mathcal{G}(k, n)$ with minimum distance $d_S(\mathcal{C})$ is called an $[n, d_S(\mathcal{C}), |\mathcal{C}|, k]$-code.

In the case that k divides n one can construct *spread codes* [7], i.e. optimal codes with minimum distance $2k$. These codes are optimal because they reach the Singleton-like bound, which means they have $\frac{q^n-1}{q^k-1}$ elements.

Given $U \in Mat_{k\times n}$ of rank k, $\mathcal{U} \in \mathcal{G}(k, n)$ its row space and $A \in GL_n$, we define

$$\mathcal{U}A := \mathrm{rs}(UA).$$

Let $U, V \in Mat_{k\times n}$ be matrices such that $\mathrm{rs}(U) = \mathrm{rs}(V)$. Then one readily verifies that $\mathrm{rs}(UA) = \mathrm{rs}(VA)$ for any $A \in GL_n$.

This multiplication with matrices from GL_n actually defines a group operation from the right on the Grassmannian:

$$\begin{array}{ccc} \mathcal{G}(k, n) \times GL_n & \longrightarrow & \mathcal{G}(k, n) \\ (\mathcal{U}, A) & \longmapsto & \mathcal{U}A \end{array}$$

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

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

is called an *orbit code* [10]. Since

$$\mathcal{G}(k,n) \cong GL_n/Stab(\mathcal{U}),$$

where $Stab(\mathcal{U}) := \{A \in GL_n | \mathcal{U}A = \mathcal{U}\}$, it is possible that different subgroups generate the same orbit code. An orbit code is called *cyclic* if it can be defined by a cyclic subgroup $\mathfrak{G} \leq GL_n$.

2.2 Irreducible Polynomials and Extension Fields

Let us state some known facts on irreducible polynomials over finite fields (cf. [6] Lemmas 3.4 - 3.6):

Lemma 1 *Let $p(x)$ be an irreducible polynomial over $\mathbb{F}_q$ of degree n, $p(0) \neq 0$ and α a root of it. Define the order of a polynomial $p(x) \in \mathbb{F}_q[x]$ with $p(0) \neq 0$ as the smallest integer e for which $p(x)$ divides $x^e - 1$. Then*

1. *the order of $p(x)$ is equal to the order of α in $\mathbb{F}_{q^n} \backslash \{0\}$.*
2. *the order of $p(x)$ divides $q^n - 1$.*
3. *$p(x)$ divides $x^c - 1$ iff the order of $p(x)$ divides c (where $c \in \mathbb{N}$).*

There is an isomorphism between the vector space $\mathbb{F}_q^n$ and the Galois extension field $\mathbb{F}_{q^n} \cong \mathbb{F}_q[\alpha]$, for α a root of an irreducible polynomial $p(x)$ of degree n over $\mathbb{F}_q$. If in addition $p(x)$ is primitive, then

$$\mathbb{F}_q[\alpha] \backslash \{0\} = \langle \alpha \rangle = \{\alpha^i | i = 0, ..., q^n - 2\}$$

i.e. α generates multiplicatively the group of invertible elements of the extension field.

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

Proof. Since $k|n$ it holds that $c \in \mathbb{N}$. Moreover, it holds that $(\alpha^c)^{q^k-1} = \alpha^{q^n-1} = 1$ and $(\alpha^c)^{q^k-2} = \alpha^{-c} \neq 1$, hence the order of α^c is $q^k - 1$. It is well-known that if k divides n the field $\mathbb{F}_{q^n}$ has exactly one subfield $\mathbb{F}_{q^k}$. Thus the group generated by α^c has to be $\mathbb{F}_{q^k} \backslash \{0\}$, which again is isomorphic to $\mathbb{F}_q^k$ as a vector space. □

2.3 Irreducible Matrix Groups

Definition 3 *1. A matrix $A \in GL_n$ is called* irreducible *if $\mathbb{F}_q^n$ contains no non-trivial A-invariant subspace, otherwise it is called* reducible.
2. A subgroup $\mathfrak{G} \subseteq GL_n$ is called irreducible *if $\mathbb{F}_q^n$ contains no $\mathfrak{G}$-invariant subspace, otherwise it is called* reducible.
3. An orbit code $\mathcal{C} \subseteq \mathcal{G}(k,n)$ is called irreducible *if $\mathcal{C}$ can be viewed as the orbit under the group action of an irreducible group.*

A cyclic group is irreducible if and only if its generator matrix is irreducible. Moreover, an invertible matrix is irreducible if and only if its characteristic polynomial is irreducible.

Example 4 *Over $\mathbb{F}_2$ the only irreducible polynomial of degree 2 is $p(x) = x^2 + x + 1$. The irreducible matrices in GL_2 must have trace and determinant equal to 1 and hence are*

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

We can say even more about irreducible matrices with the same characteristic polynomial. For this, note that the definition of an irreducible matrix G implies the existence of a so called *cyclic vector* $v \in \mathbb{F}_q^n$ having the property that

$$\{v, vG, vG^2, \ldots, vG^{n-1}\}$$

forms a basis of $\mathbb{F}_q^n$. Let $S \in GL_n$ be the basis transformation which transforms the matrix G into this new basis. Then it follows that

$$SGS^{-1} = \begin{pmatrix} 0 & 1 & 0 \ldots & 0 \\ 0 & 0 & 1 \ldots & 0 \\ \vdots & \vdots & \vdots \ddots & \vdots \\ 0 & 0 & 0 \ldots & 1 \\ -c_0 & -c_1 & \ldots & -c_{n-1} \end{pmatrix}.$$

The matrix appearing on the right is said to be in *companion form*. By convention we will use row vectors and accordingly companion matrices where the coefficients of the corresponding polynomials are in the last row (instead of the last column).

One readily verifies that

$$p(x) := x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$$

is the characteristic polynomial of both G and SGS^{-1}. It follows that every irreducible matrix in GL_n is similar to the companion matrix of its characteristic polynomial. Hence all irreducible matrices with the same characteristic polynomial are similar.

Furthermore, we can say something about the order of a matrix when viewed as an element of the finite group GL_n. For this assume that $G \in GL_n$ is an invertible matrix having $p(x)$ as characteristic polynomial. Then one readily verifies that the order of G is equal to the order of $p(x)$. Hence G is a primitive element of GL_n if and only if its characteristic polynomial is primitive.

The next fact is a well-known group theoretic result:

Lemma 5 *(cf. [6] Theorem 1.15.) In a finite cyclic group $\mathfrak{G} = \langle G \rangle$ of order m, the element G^l generates a subgroup of order $\frac{m}{\gcd(l,m)}$. Hence each element G^l with $\gcd(l, m) = 1$ is a generator of $\mathfrak{G}$.*

Lemma 6 *(cf. [8] Theorem 7) All irreducible cyclic groups generated by matrices with a characteristic polynomial of the same order are conjugate to each other.*

Example 7 *Over $\mathbb{F}_2$ the irreducible polynomials of degree 4 are $p_1(x) = x^4 + x + 1$, $p_2(x) = x^4 + x^3 + 1$ and $p_3(x) = x^4 + x^3 + x^2 + x + 1$, where $ord(p_1) = ord(p_2) = 15$ and $ord(p_3) = 5$. Let P_1, P_2, P_3 be the respective companion matrices: One verifies that $\langle P_1 \rangle$ and $\langle P_2 \rangle$ are conjugate to each other but $\langle P_3 \rangle$ is not conjugate to them.*

One can describe the action of an irreducible matrix group via the Galois extension field isomorphism.

Theorem 8 *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 ϕ be the canonical homomorphism*

$$\begin{aligned} \phi : \mathbb{F}_q^n &\longrightarrow \mathbb{F}_{q^n} \\ (v_1, \ldots, v_n) &\longmapsto \sum_{i=1}^{n} v_i \alpha^{i-1}. \end{aligned}$$

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

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

If P is a companion matrix of a primitive polynomial the group generated by P is also known as a *Singer group*. This notation is used e.g. by Kohnert et al. in their network code construction (see [2], [4]). Elsewhere P is called *Singer cycle* or *cyclic projectivity* (e.g. in [3]).

3 Irreducible Cyclic Orbit Codes

The irreducible cyclic subgroups of GL_n are exactly the groups generated by the companion matrices of the irreducible polynomials of degree n and their conjugates. Moreover, all groups generated by companion matrices of irreducible polynomials of the same order are conjugate.

It is sufficient to characterize the orbits of cyclic groups generated by companion matrices of irreducible polynomials of degree n. The following theorem shows that the results are then carried over to any irreducible cyclic orbit code via the choice of a starting point of the orbit.

Theorem 9 *Let G be an irreducible matrix, $\mathfrak{G} = \langle G\rangle$ and $\mathfrak{H} = \langle S^{-1}GS\rangle$ for an $S \in GL_n$. Moreover, let $\mathcal{U} \in \mathcal{G}(k,n)$ and $\mathcal{V} := \mathcal{U}S$. Then the orbit codes*

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

have the same cardinality and minimum distance.

Proof. Trivially the cardinality of both codes is the same. It remains to be shown that the same holds for the minimum distance.

The following diagram commutes:

$$\begin{array}{ccc} \mathcal{U} & \xrightarrow{G} & \mathcal{U}G \\ S\downarrow & & \downarrow S \\ \mathcal{V} & \xrightarrow[S^{-1}GS]{} & \mathcal{U}GS \end{array}$$

Since the subspace distance is invariant under GL_n-action and $(S^{-1}GS)^i = S^{-1}G^iS$ it holds that

$$d_S(\mathcal{U},\mathcal{U}G^i) = d_S(\mathcal{V},\mathcal{U}G^iS)$$

hence the minimum distances of the codes defined by $\mathfrak{G}$ and by $\mathfrak{H}$ are equal. □

3.1 Primitive Generator

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

Lemma 10 *For every $\beta \in \mathbb{F}_{q^n}$ the set*

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

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

Proof.

$$\begin{aligned}\varphi_\beta : \ \mathbb{F}_{q^n} &\longrightarrow \mathbb{F}_{q^n}\\ u &\longmapsto \beta u\end{aligned}$$

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

Theorem 11 *The set*

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

defines a spread code.

Proof. By a simple counting argument it is enough to show that the subspace $\alpha^i \cdot \mathbb{F}_{q^k}$ and $\alpha^j \cdot \mathbb{F}_{q^k}$ have only trivial intersection whenever $0 \leq i < j \leq c-1$. For this assume that there are field elements $c_i, c_j \in \mathbb{F}_{q^k}$, such that

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

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

We now translate this result into a matrix setting. For this let ϕ denote the canonical homomorphism as defined in Theorem 8.

Corollary 12 *Assume $k|n$. Then there is a subspace $\mathcal{U} \in \mathcal{G}(k,n)$ such that the cyclic orbit code obtained by the group action of a a primitive companion matrix is a code with minimum distance $2k$ and cardinality $\frac{q^n-1}{q^k-1}$. Hence this irreducible cyclic orbit code is a spread code.*

Proof. In the previous theorem represent $\mathbb{F}_{q^k} \subset \mathbb{F}_{q^n}$ as the rowspace of a $k \times n$ matrix over $\mathbb{F}_q$ and using the same basis over $\mathbb{F}_q$ represent the primitive α with a primitive companion matrix P. The orbit code defined in this way has then all the desired properties. □

Example 13 *Over the binary field let $p(x) := x^6 + x + 1$ be primitive, α a root of $p(x)$ and P its companion matrix.*

1. *For the 3-dimensional spread compute $c = \frac{63}{7} = 9$ and construct a basis for the starting point of the orbit:*

$$\begin{aligned}u_1 &= \phi^{-1}(\alpha^0) = \phi^{-1}(1) = (100000)\\ u_2 &= \phi^{-1}(\alpha^c) = \phi^{-1}(\alpha^9) = \phi^{-1}(\alpha^4 + \alpha^3) = (000110)\\ u_3 &= \phi^{-1}(\alpha^{2c}) = \phi^{-1}(\alpha^{18}) = \phi^{-1}(\alpha^3 + \alpha^2 + \alpha + 1) = (111100)\end{aligned}$$

   The starting point is

$$\mathcal{U} = \mathrm{rs}\begin{bmatrix}1&0&0&0&0&0\\0&0&0&1&1&0\\1&1&1&1&0&0\end{bmatrix} = \mathrm{rs}\begin{bmatrix}1&0&0&0&0&0\\0&1&1&0&1&0\\0&0&0&1&1&0\end{bmatrix}$$

   and the orbit of the group generated by P on $\mathcal{U}$ is a spread code.
2. *For the 2-dimensional spread compute $c = \frac{63}{3} = 21$ and construct the starting point*

$$\begin{aligned}u_1 &= \phi^{-1}(\alpha^0) = \phi^{-1}(1) = (100000)\\ u_2 &= \phi^{-1}(\alpha^c) = \phi^{-1}(\alpha^{21}) = \phi^{-1}(\alpha^2 + \alpha + 1) = (111000)\end{aligned}$$

   The starting point is

$$\mathcal{U} = \mathrm{rs}\begin{bmatrix}1&0&0&0&0&0\\1&1&1&0&0&0\end{bmatrix} = \mathrm{rs}\begin{bmatrix}1&0&0&0&0&0\\0&1&1&0&0&0\end{bmatrix}$$

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

The following fact has been formulated by Kohnert and Kurz in [4]:

Lemma 14 *Over the binary field let $p(x)$ be a primitive polynomial and α a root of it. Assume $k > 1$ and $\mathcal{U} = \{0, u_1, \ldots, u_{2^k-1}\} \in \mathcal{G}(k, n)$ such that*

$$\phi(u_i) = \alpha^{b_i} \qquad \forall i = 1, \ldots, 2^k - 1$$

and the set

$$\{b_m - b_l \mod 2^n - 1 | l, m \in \mathbb{Z}_{2^k-1}, l \neq m\}$$

has no multiple elements, i.e. all quotients in the field representation are pairwise different. Then the orbit of the group generated by the companion matrix P of $p(x)$ on $\mathcal{U}$ is an orbit code of cardinality $2^n - 1$ and minimum distance $2k - 2$.

Proof. In field representation the elements of the orbit code are:

$$\begin{aligned} C_0 &= \{\alpha^{b_1}, \alpha^{b_2}, \ldots, \alpha^{b_{2^k-1}}\} \\ C_1 &= \{\alpha^{b_1+1}, \alpha^{b_2+1}, \ldots, \alpha^{b_{2^k-1}+1}\} \\ &\vdots \\ C_{q^n-2} &= \{\alpha^{b_1+q^n-2}, \ldots, \alpha^{b_{2^k-1}+q^n-2}\} \end{aligned}$$

We show that the intersection between any two code words is at most one element. Therefore, assume w.l.o.g. that the first element of C_h is equal to the second element of C_j:

$$\alpha^{b_1+h} = \alpha^{b_2+j} \iff h \equiv b_2 - b_1 + j \mod 2^n - 1$$

To have another element in common it has to hold

$$b_y + h \equiv b_z + j \mod 2^n - 1$$

for some $y \neq 1$ (or $z \neq 2$). Insert h from above:

$$b_y + b_2 - b_1 + j \equiv b_z + j \iff b_2 - b_1 \equiv b_z - b_y \mod 2^n - 1$$

By condition the only solution for this equation is $y = 1, z = 2$. Thus there is no second element in the intersection.

On the other hand one can always find $h \neq j$ such that there is a solution to

$$b_y + h \equiv b_z + j \mod 2^n - 1,$$

hence, the minimum distance is exactly $2k - 2$. □

As can be found in [2], a subspace fulfilling the condition of Lemma 14 exists for any k, n. Moreover, it is shown how to combine different orbits to a network code of minimum distance $2k - 2$ and how one-error-correcting decoding can be done.

The result and proof from above can be carried over to arbitrary finite fields and any starting point $\mathcal{U} \in \mathcal{G}(k, n)$ in the following way:

Theorem 15 *Over $\mathbb{F}_q$ let $p(x)$ be a primitive polynomial and α a root of it. Assume $\mathcal{U} = \{0, u_1, \ldots, u_{q^k-1}\} \in \mathcal{G}(k, n)$,*

$$\phi(u_i) = \alpha^{b_i} \qquad \forall i = 1, \ldots, q^k - 1$$

and $d < k$ be minimal such that any element of the set

$$\{b_m - b_l \mod q^n - 1 | l, m \in \mathbb{Z}_{q^k-1}, l \neq m\}$$

has multiplicity less than $q^d - 1$, i.e. a quotient of two elements in the field representation appears at most $q^d - 1$ times in the set of all pairwise quotients. Then the orbit of the group generated by the companion matrix P of $p(x)$ on $\mathcal{U}$ is an orbit code of cardinality $q^n - 1$ and minimum distance $2k - 2d$.

Proof. In analogy to the proof of Lemma 14, to have another element in common it has to hold

$$b_2 - b_1 \equiv b_z - b_y \mod q^n - 1.$$

By condition there are up to $q^d - 1$ solutions in (y, z) for this equation, including $y = 1, z = 2$. Thus the intersection of C_i and C_j has at most $q^d - 1$ elements. On the other hand, since d is minimal, one can always find $h \neq j$ such that there are $q^d - 1$ solutions to

$$b_y + h \equiv b_z + j \mod q^n - 1,$$

hence, the minimum distance is exactly $2k - 2d$. □

If $d = k$, i.e. all quotients are the same, one gets elements with full intersection which means they are the same element. This can only happen if $k|n$ (since $k|n$ if and only if $q^k - 1|q^n - 1$). In this case one can construct spread codes as explained in Corollary 12.

3.2 Non-Primitive Generator

Theorem 16 *Let P be an irreducible non-primitive companion matrix, $\mathfrak{G}$ the group generated by it and denote by $v\mathfrak{G}$ and $\mathcal{U}\mathfrak{G}$ the orbits of $\mathfrak{G}$ on $v \in \mathbb{F}_q^n$ and $\mathcal{U} \in \mathcal{G}(k, n)$, respectively. If $\mathcal{U} \in \mathcal{G}(k, n)$ such that*

$$v \neq w \implies v\mathfrak{G} \neq w\mathfrak{G} \quad \forall\, v, w \in \mathcal{U},$$

then $\mathcal{U}\mathfrak{G}$ on is an orbit code with minimum distance $2k$ and cardinality $\mathrm{ord}(P)$.

Proof. The cardinality follows from the fact that each element of $\mathcal{U}$ hast its own orbit of length $\mathrm{ord}(P)$. Moreover, no code words intersect non-trivially, hence the minimum distance is $2k$. □

Note that, if the order of P is equal to $\frac{q^n-1}{q^k-1}$, these codes are again spread codes.

Example 17 *Over the binary field let $p(x) = x^4 + x^3 + x^2 + x + 1$, α a root of $p(x)$ and P its companion matrix. Then $\mathbb{F}_{2^4}\backslash\{0\}$ is partitioned into*

$$\{\alpha^i | i = 0, \ldots, 4\} \cup \{\alpha^i(\alpha + 1) | i = 0, \ldots, 4\} \cup \{\alpha^i(\alpha^2 + 1) | i = 0, \ldots, 4\}.$$

Choose

$$\begin{aligned} u_1 &= \phi^{-1}(1) = \phi^{-1}(\alpha^0) = (1000) \\ u_2 &= \phi^{-1}(\alpha^3 + \alpha^2) = \phi^{-1}(\alpha^2(\alpha + 1)) = (0011) \\ u_3 &= u_1 + u_2 = \phi^{-1}(\alpha^3 + \alpha^2 + 1) = \phi^{-1}(\alpha^3(\alpha^2 + 1)) = (1011) \end{aligned}$$

such that each u_i is in a different orbit of $\langle P \rangle$ and $\mathcal{U} = \{0, u_1, u_2, u_3\}$ is a vector space. Then the orbit of $\langle P \rangle$ on $\mathcal{U}$ has minimum distance 4 and cardinality 5, hence it is a spread code.

Proposition 18 *Let P and $\mathfrak{G}$ be as before and $\mathcal{U} = \{0, v_1, \ldots, v_{q^k-1}\} \in \mathcal{G}(k,n)$. Let $O_1, ..., O_l$ be the different orbits of $\mathfrak{G}$ in $\mathbb{F}_q^n$. Assume that $m < q^k - 1$ elements of $\mathcal{U}$ are in the same orbit, say O_1, and all other elements are in different orbits each, i.e.*

$$v_i\mathfrak{G} = v_j\mathfrak{G} = O_1 \quad \forall\, i,j \leq m,$$

$$v_i \neq v_j \implies v_i\mathfrak{G} \neq v_j\mathfrak{G} \quad \forall\, i,j \geq m.$$

Apply the theory of Section 3.1 to the orbit O_1 and find d_1 fulfilling the conditions of Theorem 15. Then the orbit of $\mathfrak{G}$ on $\mathcal{U}$ is a code of length $\mathrm{ord}(P)$ *and minimum distance* $2k - 2d_1$.

Proof. 1. Since there is at least one orbit O_i that contains exactly one element of $\mathcal{U}$, each element of O_i is in exactly one code word. Hence the cardinality of the code is $\mathrm{ord}(\mathfrak{G}) = \mathrm{ord}(P)$.
2. In analogy to Theorem 16 the only possible intersection is inside O_1, which can be found according to the theory of cyclic primitive groups.

□

We generalize these results to any possible starting point $\in \mathcal{G}(k,n)$:

Theorem 19 *Let $P, \mathfrak{G}, \mathcal{U}$ and the orbits $O_1, ..., O_l$ be as before. Assume that m_i elements of $\mathcal{U}$ are in the same orbit O_i $(i = 1, \ldots, l)$. Apply the theory of Section 3.1 to each orbit O_i and find the corresponding d_i from Theorem 15. Then the following cases can occur:*

1. *No intersections of two different orbits coincide. Define $d_{\max} := \max_i d_i$. Then the orbit of $\mathfrak{G}$ on $\mathcal{U}$ is a code of length* $\mathrm{ord}(P)$ *and minimum distance* $2k - 2d_{max}$.
2. *Some intersections coincide among some orbits. Then the corresponding d_i's add up and the maximum of these is the maximal intersection number $d_{\max}$.*

Mathematically formulated: Assume $b_{(j,1)}, \ldots, b_{(j,\mathrm{ord}(P)-1)}$ are the exponents of the field representation of elements of $\mathcal{U}$ on O_j. Define

$$a_{(i,\mu,\lambda)} := b_{(i,\mu)} - b_{(i,\lambda)}$$

and denote by $m^{\mu,\lambda}(a)$ the multiplicity of an element a in the (multi-)set $\{a_{(i,\mu,\lambda)} \mid i = 1, \ldots, l\}$ for given μ and λ. Moreover, let

$$\delta_{(\mu,\lambda)} := \max\{a_{(i,\mu,\lambda)} \cdot m^{\mu,\lambda}(a_{(i,\mu,\lambda)}) \mid i = 1, \ldots, l\},$$

$$d_{\max} := \max\{\delta_{(\mu,\lambda)} \mid \mu, \lambda \in \mathbb{Z}_{\mathrm{ord}(P)-1}\}.$$

Then the orbit of $\mathfrak{G}$ on $\mathcal{U}$ is a code of length $\mathrm{ord}(P)$ *and minimum distance* $2k - 2d_{\max}$.

Note that in the case that the minimum distance of the code is 0 one has double elements in the orbit. Then one has to consider the set of different code words and compute the cardinality and minimum distance again.

4 Conclusion

We listed all possible irreducible cyclic orbit codes and showed that it suffices to investigate the groups generated by companion matrices of irreducible polynomials. Moreover, polynomials of the same degree and same order generate codes with the same cardinality and minimum distance. These two properties of the code depend strongly on the choice of the starting point in the Grassmannian. We showed how one can deduce the size and distance of an orbit code for a given subgroup of GL_n from the starting point $\mathcal{U} \in \mathcal{G}(k,n)$. For primitive groups this is quite straight-forward while the non-primitive case is more difficult.

Subsequently one can use this theory of irreducible cyclic orbit codes to characterize all cyclic orbit codes.

References

1. R. Ahlswede, N. Cai, S.-Y.R. Li, and R.W. Yeung. Network information flow. *IEEE Trans. Inform. Theory*, 46:1204–1216, July 2000.
2. A. Elsenhans, A. Kohnert, and Alfred Wassermann. Construction of codes for network coding. In *Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems – MTNS*, pages 1811–1814, Budapest, Hungary, 2010.
3. J. W. P. Hirschfeld. *Projective Geometries over Finite Fields*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, second edition, 1998.
4. A. Kohnert and S. Kurz. Construction of large constant dimension codes with a prescribed minimum distance. In Jacques Calmet, Willi Geiselmann, and Jörn Müller-Quade, editors, *MMICS*, volume 5393 of *Lecture Notes in Computer Science*, pages 31–42. Springer, 2008.
5. R. Kötter and F.R. Kschischang. Coding for errors and erasures in random network coding. *Information Theory, IEEE Transactions on*, 54(8):3579–3591, August 2008.
6. R. Lidl and H. Niederreiter. *Introduction to Finite Fields and their Applications*. Cambridge University Press, Cambridge, London, 1986.
7. F. Manganiello, E. Gorla, and J. Rosenthal. Spread codes and spread decoding in network coding. In *Proceedings of the 2008 IEEE International Symposium on Information Theory*, pages 851–855, Toronto, Canada, 2008.
8. F. Manganiello, A.-L. Trautmann, and J. Rosenthal. On conjugacy classes of subgroups of the general linear group and cyclic orbit codes. *arXiv:1102.3350v1*, [cs.IT], 2011.
9. D. Silva, F.R. Kschischang, and R. Kötter. A rank-metric approach to error control in random network coding. *Information Theory, IEEE Transactions on*, 54(9):3951–3967, Sept. 2008.
10. A.-L. Trautmann, F. Manganiello, and J. Rosenthal. Orbit codes - a new concept in the area of network coding. In *Information Theory Workshop (ITW), 2010 IEEE*, pages 1 –4, Dublin, Ireland, August 2010.