TWMS J. App. Eng. Math. V.9, N.2, 2019, pp. 225-236

DECODING OF ORBIT CODES

M. HAKIMI POROCH[1], A. A. TALEBI[1], §

Abstract. Subspace codes have an important role to correct errors and erasures for random network coding. Orbit codes are a family of constant dimension subspace codes and they are interesting for their error correction. In this work, we want to propose two algorithms for decoding of orbit codes.

Keywords: Subspace codes, Constant dimension subspace codes, Grassmannian, Group action, Orbit codes.

AMS Subject Classification: 11T71, 94B35.

1. Introduction

Subspace codes have gained considerable attention during the last decade due to their crucial role in random network coding. Subspace codes are defined as sets of vector spaces over a finite field. Subspace codes can be used to correct errors and erasures in network with linear network coding. Networks are exposed to noise such that messages can be lost or modified during the transmission of subspace $\mathcal{V}$. Therefore some vectors of $\mathcal{V}$ might be lost and we will received smaller subspace $\mathcal{V}' < \mathcal{V}$. On the other hand, vectors which are not contained in $\mathcal{V}$ might be received. These erroneous vectors span a vector space $\mathcal{E}$, thus $\mathcal{R} = \mathcal{V}' \oplus \mathcal{E}$ will be received. In fact, there are two types of errors that may occur during transmission, a decrease in dimension, which is called an *erasure* and an increase in dimension, called an *insertion*.

The set of all k-dimensional subspaces of $\mathbb{F}_q^n$ is called *Grassmann variety* and denoted by $\mathcal{G}(k, \mathbb{F}_q^n)$. Constant dimension codes are a family of subspace codes where codewords have the same dimension. In fact, constant dimension codes are subsets of $\mathcal{G}(k, \mathbb{F}_q^n)$. Orbit codes are a subclass of constant dimension codes. These are subspace codes that arise as an orbit of a subspace in $\mathbb{F}_q^n$ under a subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$. If the subgroup is cyclic, it is called cyclic orbit code. Also, if the subgroup is irreducible, the code is called an irreducible cyclic orbit code.

In [9], Trautmann et al., present an algebraic construction of cyclic orbit codes. They investigate two algorithms for decoding of cyclic orbit codes. If field size q and the dimension of the vector spaces k are small, the first algorithm is efficient. The second algorithm

[1] Department of Mathematics, University of Mazandaran, Iran, Bobolsar.
e-mail: m.hakimiporoch@stu.umz.ac.ir; ORCID: https://orcid.org/ 0000-0003-4394-1081.
e-mail: a.talebi@umz.ac.ir; ORCID: https://orcid.org/ 0000-0002-2056-0502.

§ Manuscript received: May 28, 2017; accepted: Sep 29, 2017.
TWMS Journal of Applied and Engineering Mathematics, Vol.9, No.2;

explains syndrome decoding of irreducible cyclic orbit codes. The main idea is that the pairwise quotients of the elements of a subspace are invariant for all elements of the same orbit. When the number of quotients is small, this algorithm is more efficient that other known decoding algorithms.
The goal of this paper is to decode orbit codes. The paper is organized as follows: In the second section, we will give some preliminaries about subspace codes, orbit codes and their minimum distance. In the third section, we derive two algorithms for decoding of orbit codes. Finally in section 4, we conclude this work.

2. PRELIMINARIES

Let $\mathbb{F}_q$ be the finite field of size q and let $\mathbb{F}_q^n$ be the vector space of dimension n. The set of all k-dimensional subspaces of $\mathbb{F}_q^n$, called *Grassmann variety* or simply *Grassmannian* and it is denoted by $\mathcal{G}_q(k,n)$. In fact

$$\mathcal{G}_q(k,n) := \{\mathcal{U} \leq \mathbb{F}_q^n \mid \dim(\mathcal{U}) = k\}.$$

The union of all *Grassmann varieties*, *i.e.* the set of all subspaces of $\mathbb{F}_q^n$ is called the *projective space* and it is defined by

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

The set of all $k \times n$-matrices over $\mathbb{F}_q$ is represented by $Mat_{k\times n}$.
Let $U \in Mat_{k\times n}$ be matrix of rank k, then

$$\mathcal{U} = \mathrm{rs}(U) := \mathrm{rowspace}(U) \in \mathcal{G}_q(k,n).$$

For any $\mathcal{U}, \mathcal{V} \in \mathcal{P}_q(n)$, the subspace distance is defined as:

$$\begin{aligned} d_{\mathcal{S}}(\mathcal{U},\mathcal{V}) &= \dim(\mathcal{U}+\mathcal{V}) - \dim(\mathcal{U}\cap\mathcal{V}) \\ &= \dim(\mathcal{U}) + \dim(\mathcal{V}) - 2\dim(\mathcal{U}\cap\mathcal{V}). \end{aligned}$$

Definition 2.1. *A subspace code $\mathcal{C}$ is a subset of $\mathcal{P}_q(n)$ and $\mathcal{C}$ is called a* constant dimension code*, if all codewords of $\mathcal{C}$ have the same dimension.*

The minimum distance of a subspace code $\mathcal{C}$ is defined as:

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

The general linear group of dimension n is the set of all invertible $n \times n$-matrices with entries in $\mathbb{F}_q$ and it is denoted by $\mathrm{GL}_n(\mathbb{F}_q)$.
The $\mathrm{GL}_n(\mathbb{F}_q)$-elements define a group action from the right on the *Grassmannian* as:

$$\begin{aligned} \mathcal{G}_q(k,n) \times \mathrm{GL}_n(\mathbb{F}_q) &\longrightarrow \mathcal{G}_q(k,n) \\ (\mathcal{U}, A) &\longmapsto \mathcal{U}A \end{aligned}$$

Let $\mathcal{U} \in \mathcal{G}_q(k,n)$ be fixed and let G be a subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$, then

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

is called an orbit code [10].
If $G \leq \mathrm{GL}_n(\mathbb{F}_q)$ is cyclic, an orbit code is called cyclic orbit code. The size of code $\mathcal{C}$ is

$$|\mathcal{C}| = \frac{|G|}{|\mathrm{Stab}_G(\mathcal{U})|},$$

where

$$\mathrm{Stab}_G(\mathcal{U}) := \{A \in G \mid \mathcal{U}A = \mathcal{U}\},$$

and its minimum distance of the code $\mathcal{C}$ is

$$d(\mathcal{C}) = \min\{d_{\mathcal{S}}(\mathcal{U},\mathcal{U}A) \mid A \in G,\ A \notin \mathrm{Stab}_G(\mathcal{U})\}.$$

Definition 2.2. *Let $p(x) = p_0 + p_1x + \cdots + p_{n-1}x^{n-1} + x^n \in \mathbb{F}_q[x]$. The companion matrix $p(x)$ is described as:*

$$\mathrm{M}_p := \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ -p_0 & -p_1 & -p_2 & \dots & -p_{n-1} \end{pmatrix}$$

Definition 2.3. *A polynomial $p(x) \in \mathbb{F}_q[x]$ is called irreducible, if it cannot be factored into the product of two non-constant polynomials of $\mathbb{F}_q[x]$. In fact, for any $a(x), b(x) \in \mathbb{F}_q[x]$, we have*

$$p(x) = a(x)b(x) \Longrightarrow \deg(a(x)) = 0 \quad \text{or} \quad \deg(b(x)) = 0.$$

Theorem 2.1. [5] *Let $p(x) = p_0 + p_1x + \cdots + p_{n-1}x^{n-1} + x^n$ be a monic irreducible polynomial of degree n over the finite field $\mathbb{F}_q$ and $\alpha \in \mathbb{F}_{q^n}$ be a root of $p(x)$. Then the extension field $\mathbb{F}_{q^n}$ can be represented by*

$$\mathbb{F}_{q^n} \cong \mathbb{F}_q[x]/p(x) \cong \mathbb{F}_q[\alpha] \cong \mathbb{F}_q[\mathrm{M}_p].$$

Lemma 2.1. [7] *For any finite field $\mathbb{F}_q$, the multiplicative group $\mathbb{F}_q^*$ is cyclic,* i.e. *it can be generated by one element.*

An irreducible polynomial $p(x) \in \mathbb{F}_q[x]$ of degree n is called *primitive*, if any of its roots is a multiplicative generator of $\mathbb{F}_{q^n}^*$.

Lemma 2.2. [7] *If $p(x) \in \mathbb{F}_q[x]$ is a primitive polynomial, then the multiplicative group generated by M_p has order $q^n - 1$.*

Lemma 2.3. [9] *Let $p(x)$ be an irreducible polynomial over $\mathbb{F}_q$ of degree n and M_p its companion matrix. Furthermore, let $\alpha \in \mathbb{F}_{q^n}^*$ be a root of $p(x)$ and ϕ be the canonical homomorphism*

$$\begin{aligned} \phi : \mathbb{F}_q^n &\longrightarrow \mathbb{F}_{q^n} \\ (v_0, \dots, v_{n-1}) &\longmapsto \sum_{i=0}^{n-1} v_i\alpha^i. \end{aligned}$$

Then the multiplication with M_p resp. α commutes with the mapping ϕ, i.e. *for all $v \in \mathbb{F}_q^n$, we get*

$$\phi(v\mathrm{M}_p) = \phi(v)\alpha.$$

Definition 2.4. *A* multiset *is a generalization of the notion of set in which members are allowed to appear more than once. To distinguish it from usual sets $\{x \in X\}$, we will denote multisets by $\{\{x \in X\}\}$. The number of times an element x belongs to the multiset X is the* multiplicity *of that element, denoted by $m_X(x)$.*

Let $p(x) \in \mathbb{F}_q[x]$ be a primitive polynomial of degree n and α be a root of it. Thus α is a primitive element of $\mathbb{F}_{q^n}$. For any non-zero element $u \in \mathbb{F}_q^n$, there exists an $i \in \mathbb{Z}_{q^n-1}$ such that $\phi(u) = \alpha^i$.

Theorem 2.2. [8, Theorem 15] *Over $\mathbb{F}_q$ let $p(x)$ be a primitive polynomial and α a root of it. Assume $\mathcal{U} = \{0, u_1, \ldots, u_{q^k-1}\} \in \mathcal{G}_q(k,n)$,*

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

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

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

has multiplicity less that or equal to $q^d - 1$, 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 M_p of $p(x)$ on $\mathcal{U}$ is an orbit code of cardinality $q^n - 1$ and minimum distance $2k - 2d$.

An orbit code is called *completely reducible*, if its generating group is *completely reducible*. In general, a group is *completely reducible* if it is the direct product of irreducible groups.
Now suppose that our generator matrix M_p is of the type

$$\mathrm{M}_p = \begin{pmatrix} \mathrm{M}_{p_1} & 0 \\ 0 & \mathrm{M}_{p_2} \end{pmatrix}$$

, M_{p_1} and M_{p_2} are companion matrices of the primitive polynomials $p_1(x), p_2(x) \in \mathbb{F}_q[x]$ with $\deg\, p_1(x) = n_1, \deg\, p_2(x) = n_2$ respectively. Let

$$U = (U_1 \quad U_2)$$

be the matrix representation of $\mathcal{U} \in \mathcal{G}_q(k,n)$, where

$$U_1 \in Mat_{k\times n_1}, \quad U_2 \in Mat_{k\times n_2},$$

then $\mathcal{U}\mathrm{M}_p^i = \mathrm{rs}(U_1\mathrm{M}_{p_1}^i \quad U_2\mathrm{M}_{p_2}^i)$.
Also $\phi^{(n_1)} : \mathbb{F}_q^{n_1} \longrightarrow \mathbb{F}_{q^{n_1}}$ and $\phi^{(n_2)} : \mathbb{F}_q^{n_2} \longrightarrow \mathbb{F}_{q^{n_2}}$ are standard vector space isomorphisms.

Theorem 2.3. [9, Theorem 27] *Let α_1, α_2 be primitive elements of $\mathbb{F}_{q^{n_1}}$, $\mathbb{F}_{q^{n_2}}$ respectively, $n_1 + n_2 = n$.*

$$\begin{aligned} \phi^{(n_1,n_2)} : \mathbb{F}_q^n &\longrightarrow \mathbb{F}_{q^{n_1}} \times \mathbb{F}_{q^{n_2}} \\ (u_1, \ldots, u_n) &\longmapsto (\phi^{(n_1)}(u_1, \ldots, u_{n_1}), \phi^{(n_2)}(u_{n_1+1}, \ldots, u_n)) \end{aligned}$$

is a vector space isomorphism. Moreover, $u = v\mathrm{M}_p^i$ for some $u, v \in \mathbb{F}_q^n$ if and only if

(1) $\phi^{(n_1)}(u_1, \ldots, u_{n_1}) = \phi^{(n_1)}(v_1, \ldots, v_{n_1})\alpha_1^i$ and
(2) $\phi^{(n_2)}(u_{n_1+1}, \ldots, u_n) = \phi^{(n_2)}(v_{n_1+1}, \ldots, v_n)\alpha_2^i$.

Suppose that $\phi^{(n_1)}(u_i) \neq 0$ and $\phi^{(n_2)}(u_i) \neq 0$ for all non-zero elements u_i of a given vector space $\mathcal{U} \in \mathcal{G}_q(k,n)$, then we have the following Proposition.

Proposition 2.1. [9, Proposition 28] *Assume $\mathcal{U} = \{0, u_1, \ldots, u_{q^k-1}\} \in \mathcal{G}_q(k,n)$ and for all u_i there exist b_i, b_i' such that*

$$\phi^{(n_1,n_2)}(u_i) = (\alpha_1^{b_i}, \alpha_2^{b_i'}) \quad \forall i = 1, \ldots, q^k - 1.$$

Let δ be minimal such that any element of the multiset

$$D := \{\{(b_m - b_l \pmod{q^{n_1} - 1}, b_m' - b_l' \pmod{q^{n_2} - 1}) \mid m, l \in \mathbb{Z}_{q^k-1},\ m \neq l\}\}$$

has multiplicity less than or equal to $q^\delta - 1$. If $\delta < k$, then the orbit of the group generated by M_p on $\mathcal{U}$ is an orbit code of cardinality $\mathrm{ord}(\mathrm{M}_p) = \mathrm{lcm}(q^{n_1} - 1, q^{n_2} - 1)$ and minimum distance $2k - 2\delta$.

Now, suppose that G is not cyclic. Put

$$G = \{\begin{pmatrix} \mathrm{M}_{p_1}^i & 0 \\ 0 & \mathrm{M}_{p_2}^j \end{pmatrix} \mid \quad 0 \leq i \leq q^{n_1} - 1,\ 0 \leq j \leq q^{n_2} - 1\},$$

thus we can write

$$\mathcal{U}\begin{pmatrix} \mathrm{M}_{p_1}^i & 0 \\ 0 & \mathrm{M}_{p_2}^j \end{pmatrix} = \mathrm{rs}(U_1\mathrm{M}_{p_1}^i \quad U_2\mathrm{M}_{p_2}^j).$$

Note that in Proposition 2.1, if $\deg p_1(x) = \deg p_2(x) = n$, then we have

$$b_m - b_l \equiv b'_m - b'_l \pmod{q^n - 1}.$$

But in the following Proposition, we do not have this limitation for polynomials with same degree.

Proposition 2.2. *Assume $\mathcal{U} = \{0, u_1, \ldots, u_{q^k-1}\} \in \mathcal{G}_q(k, n)$ and for all u_i there exist b_i, b'_i such that*

$$\phi^{(n_1,n_2)}(u_i) = (\alpha_1^{b_i}, \alpha_2^{b'_i}) \quad \forall i = 1, \ldots, q^k - 1.$$

Let d be minimal such that any element of multiset

$$D := \{\{(b_m - b_l \equiv h \pmod{q^{n_1} - 1},\ b'_m - b'_l \equiv h' \pmod{q^{n_2} - 1}) \mid m, l \in \mathbb{Z}_{q^k-1},\ m \neq l\}\}$$

has multiplicity less than or equal to $q^d - 1$. If $d < k$, then the orbit of the group G on $\mathcal{U}$ is an orbit code of cardinality $\mathrm{ord}(G) = (q^{n_1} - 1)(q^{n_2} - 1)$ *and minimum distance $2k - 2d$.*

Proof. The proof is similar to Proposition 2.1 and the only difference is about the set of D, so we focus on it.
We consider $\mathcal{U} \cap \mathcal{U}\begin{pmatrix} \mathrm{M}_{p_1}^i & 0 \\ 0 & \mathrm{M}_{p_2}^j \end{pmatrix}$ for $0 \leq i \leq q^{n_1} - 1$, $0 \leq j \leq q^{n_2} - 1$. A non-zero element $u_m \in \mathcal{U}$ is in $\mathcal{U}\begin{pmatrix} \mathrm{M}_{p_1}^i & 0 \\ 0 & \mathrm{M}_{p_2}^j \end{pmatrix}$ if only if $\alpha_1^{b_m} = \alpha_1^{b_l+h}$ and $\alpha_2^{b'_m} = \alpha_2^{b'_l+h'}$, for some l, $1 \leq l \leq q^k - 1$. Then it results that

$$b_m - b_l \equiv h \pmod{q^{n_1} - 1}, \quad b'_m - b'_l \equiv h' \pmod{q^{n_2} - 1}.$$

Hence, it is sufficient to write

$$D := \{\{(b_m - b_l \pmod{q^{n_1} - 1}, b'_m - b'_l \pmod{q^{n_2} - 1}) \mid m, l \in \mathbb{Z}_{q^k-1}, m \neq l\}\}.$$

Since $d < k$, it leads that all elements of the orbit code are distinct, so the cardinality of the code is $\mathrm{ord}(G) = (q^{n_1} - 1)(q^{n_2} - 1)$. □

3. Decoding of orbit codes

When we have at most 1 error, we want to consider two algorithms for decoding of orbit codes.
First we define an algorithm for an irreducible cyclic orbit code $\mathcal{C} = \mathcal{U} < \mathrm{M}_p >$ where $\mathcal{U} \in \mathcal{G}_q(k, n)$ and M_p is the companion matrix of an irreducible polynomial $p(x) \in \mathbb{F}_q[x]$ of degree n. Also $\mathcal{R} \in \mathcal{G}_q(k', n)$ is a received vector.

Algorithm: Decoding algorithm for irreducible cyclic orbit codes in $\mathcal{G}_q(k, n)$

Require: Code $\mathcal{C} = \mathcal{U} < \mathrm{M}_p > \subseteq \mathcal{G}_q(k, n)$, received vector space $\mathcal{R} \in \mathcal{P}_q(n)$,$\dim(\mathcal{R}) = k'$, $k' =: k + 1$, the quotient set $S = \{\frac{u_l}{u_m} \mid u_l, u_m \in \mathcal{U} \setminus \{0\},\ u_l \neq u_m\}$ in extension field representation, vector space $\mathcal{W}$ with $\dim(\mathcal{W}) = k$ inside $\mathcal{R}$, all $(k-1)$-dimensional subspaces $\mathcal{W}_j$ of $\mathcal{W}$, $j = 1, \ldots, \frac{(q^n-1)(q^{n-1}-1)\ldots(q^2-1)}{(q^{n-1}-1)(q^{n-2}-1)\ldots(q-1)}$

for each subspace $\mathcal{W}_j$ **do**

for each $r_j \in \mathcal{W}_j \setminus \{0\}$ **do**
for each $s_j \in \mathcal{W}_j \setminus \{0, r_j\}$ **do**
compute the quotient $c_{r_j,s_j} := \frac{r_j}{s_j}$ in extension field representation
end for
end for
for c_{r_j,s_j} be in S **do**
find $\theta(\alpha) = \alpha^i$ such that $\exists\, x, y \in \mathcal{U}$: $x\theta(\alpha) = r_j$, $y\theta(\alpha) = s_j$
compute $\mathcal{U}\mathrm{M}_p^i$
end for
if $\mathcal{U}\mathrm{M}_p^i$ is a subspace of $\mathcal{R}$ **then**
find k-th linearly independent vector from $\mathcal{U}\mathrm{M}_p^i$
return $\mathcal{W}_j$ with k-th linearly independent vector
end if
end for

Example 3.1. *Consider $\mathcal{G}_2(3,6)$ and the primitive polynomial $p(x) = x^6 + x + 1$ in $\mathbb{F}_2[x]$. Let α be a root of $p(x)$. Assume that*

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

Indeed

$$\begin{aligned} \mathcal{U} \;=\; & \{(0,0,0,0,0,0),(0,1,1,0,1,0),(1,0,0,1,0,1),(0,1,1,0,0,0),(1,1,1,1,1,1),\\ & (1,1,1,1,0,1),(0,0,0,0,1,0),(1,0,0,1,1,1)\}. \end{aligned}$$

Moreover

$$\mathrm{M}_p = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

We observe that

$$\begin{aligned} &\phi^6(u_2) = \alpha^{36}, \quad \phi^6(u_3) = \alpha^{23}, \quad \phi^6(u_4) = \alpha^{7}, \quad \phi^6(u_5) = \alpha^{58},\\ &\phi^6(u_6) = \alpha^{40}, \quad \phi^6(u_7) = \alpha^{4}, \quad \phi^6(u_8) = \alpha^{60}. \end{aligned}$$

It results that

$$b_2 = 36, \quad b_3 = 23, \quad b_4 = 7, \quad b_5 = 58, \quad b_6 = 40, \quad b_7 = 4, \quad b_8 = 60.$$

Due to the definition of D, we have

$$D = \pm\{13, 29, 41, 59, 32, 39, 16, 28, 26, 19, 46, 12, 30, 3, 10, 18, 54, 61, 36, 43, 7\}.$$

Hence $d = 1$ and $\mathcal{C} = \mathcal{U} < \mathrm{M}_p >$ has minimum distance

$$2k - 2d = 2 \times 3 - 2 \times 1 = 4.$$

Because the minimum distance is 4, it can correct at most 1 error. We try to correct the error.

Suppose that we received vector space $\mathcal{R}$. *Since we have at most* 1 *error, we can have a* 4*-dimensional subspace* $\mathcal{R}$ *in the form*

$$\mathcal{R} = \mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Choose a 3*-dimensional subspace* $\mathcal{W}$ *inside* $\mathcal{R}$. *In fact*

$$\mathcal{W} = \mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

We make seven of 2*-dimenstional subspaces of* $\mathcal{W}$ *which are:*

$$\mathcal{W}_1 = \mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix} \cong \{0, \alpha^{48}, \alpha^{46}, \alpha^{58}\},$$

$$\mathcal{W}_2 = \mathrm{rs}\begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix} \cong \{0, \alpha^{46}, \alpha^{7}, \alpha^{50}\},$$

$$\mathcal{W}_3 = \mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix} \cong \{0, \alpha^{48}, \alpha^{7}, \alpha^{35}\},$$

$$\mathcal{W}_4 = \mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \cong \{0, \alpha^{48}, \alpha^{50}, \alpha^{60}\},$$

$$\mathcal{W}_5 = \mathrm{rs}\begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix} \cong \{0, \alpha^{46}, \alpha^{35}, \alpha^{60}\},$$

$$\mathcal{W}_6 = \mathrm{rs}\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \cong \{0, \alpha^{7}, \alpha^{58}, \alpha^{60}\},$$

$$\mathcal{W}_7 = \mathrm{rs}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix} \cong \{0, \alpha^{58}, \alpha^{35}, \alpha^{50}\}.$$

Because these sets are pairwise distinct, it is enough to compute the quotient of only one pair of them. So we have

$$c_1 := \frac{\alpha^{48}}{\alpha^{46}} = \alpha^{\pm 2}, \quad c_2 := \frac{\alpha^{46}}{\alpha^{7}} = \alpha^{\pm 39}, \quad c_3 := \frac{\alpha^{48}}{\alpha^{7}} = \alpha^{\pm 41},$$
$$c_4 := \frac{\alpha^{48}}{\alpha^{50}} = \alpha^{\pm 61}, \quad c_5 := \frac{\alpha^{46}}{\alpha^{35}} = \alpha^{\pm 11}, \quad c_6 := \frac{\alpha^{7}}{\alpha^{51}} = \alpha^{\pm 12},$$
$$c_7 := \frac{\alpha^{58}}{\alpha^{35}} = \alpha^{\pm 23}.$$

In addition

$$\begin{aligned} S \;=\; \{&\alpha^{\pm 13}, \alpha^{\pm 29}, \alpha^{\pm 22}, \alpha^{\pm 4}, \alpha^{\pm 32}, \alpha^{\pm 24}, \alpha^{\pm 16}, \alpha^{\pm 35}, \alpha^{\pm 17}, \alpha^{\pm 19}, \alpha^{\pm 37}, \alpha^{\pm 51}, \alpha^{\pm 33}, \\ &\alpha^{\pm 3}, \alpha^{\pm 53}, \alpha^{\pm 18}, \alpha^{\pm 54}, \alpha^{\pm 2}, \alpha^{\pm 36}, \alpha^{\pm 20}, \alpha^{\pm 56}\}. \end{aligned}$$

We see that c_i, $(i = 1, 2, 3, 4, 6)$ *are in the set of* S, *thus we try to get a third linearly independent vector from them.*
For $\mathcal{W}_1$, *we have*

$$\{\alpha^{48-i}, \alpha^{46-i}\} = \{\alpha^{60}, \alpha^{58}\}.$$

So

$$48 - 60 \equiv i \pmod{63}, \quad 46 - 58 \equiv i \pmod{63} \Longrightarrow i = 51.$$

Similary for $\mathcal{W}_2$,

$$\{\alpha^{46-i}, \alpha^{7-i}\} = \{\alpha^{36}, \alpha^{60}\},$$

and

$$46 - 36 \equiv i \pmod{63}, \quad 7 - 60 \equiv i \pmod{63} \Longrightarrow i = 10.$$

From $\mathcal{W}_3$, *we can write*

$$\{\alpha^{48-i}, \alpha^{7-i}\} = \{\alpha^{36}, \alpha^{58}\},$$

where

$$48 - 36 \equiv i \pmod{63}, \quad 7 - 58 \equiv i \pmod{63} \Longrightarrow i = 12.$$

Also for $\mathcal{W}_4$,

$$\{\alpha^{48-i}, \alpha^{50-i}\} = \{\alpha^{60}, \alpha^{58}\},$$

and

$$48 - 58 \equiv i \pmod{63}, \quad 50 - 60 \equiv i \pmod{63} \Longrightarrow i = 53.$$

At the end, for $\mathcal{W}_6$, *we have*

$$\{\alpha^{7-i}, \alpha^{58-i}\} = \{\alpha^{7}, \alpha^{58}\},$$

thus

$$7 - 7 \equiv i \pmod{63}, \quad 58 - 58 \equiv i \pmod{63} \Longrightarrow i = 0.$$

After calculating $\mathcal{U}\mathrm{M}_p^{51}$, $\mathcal{U}\mathrm{M}_p^{10}$, $\mathcal{U}\mathrm{M}_p^{12}$ *and* $\mathcal{U}\mathrm{M}_p^{53}$, *we see that from* $\mathcal{U}\mathrm{M}_p^{10}$, *we can get a third linearly independent vector which is in* $\mathcal{R}$. *So we decode to codeword*

$$H = \mathrm{rs}\begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Now we describe an algorithm for decoding of an orbit code $\mathcal{C} = \mathcal{U}G$, where

$$G = \{\begin{pmatrix} \mathrm{M}_{p_1}^i & 0 \\ 0 & \mathrm{M}_{p_2}^j \end{pmatrix} \mid \quad 0 \le i \le q^{n_1} - 1,\ 0 \le j \le q^{n_2} - 1\},$$

M_{p_1} and M_{p_2} are companion matrices of the primitive polynomials of $p_1(x), p_2(x) \in \mathbb{F}_q[x]$ with $\deg\, p_1(x) = n_1$, $\deg\, p_2(x) = n_2$ and $n = n_1 + n_2$.
In addition, $U = (U_1 \quad U_2)$ is the matrix representation of $\mathcal{U} \in \mathcal{G}_q(k, n)$, so

$$\mathcal{U}\begin{pmatrix} \mathrm{M}_{p_1}^i & 0 \\ 0 & \mathrm{M}_{p_2}^j \end{pmatrix} = \mathrm{rs}(U_1\mathrm{M}_{p_1}^i \quad U_2\mathrm{M}_{p_2}^j).$$

Moreover, $R = (R_1 \quad R_2)$ is the matrix representation of a received vector $\mathcal{R} \in \mathcal{G}_q(k', n)$, where $R_1 \in Mat_{k' \times n_1}$ and $R_2 \in Mat_{k' \times n_2}$.

Algorithm: Decoding algorithm for orbit codes $\mathcal{C} = \mathcal{U}G$ in $\mathcal{G}_q(k, n)$

Require: Code $\mathcal{C} = \mathcal{U}G$, recived vector space $\mathcal{R} \in \mathcal{P}_q(n)$, $\dim(\mathcal{R}) = k'$,
$k' := k + 1$, the quotient set

$$S = \{(\tfrac{u_l}{u_m}, \tfrac{u'_l}{u'_m}) \mid u_l, u_m, u'_l, u'_m \in \mathcal{U} \setminus \{0\},\ u_l \ne u_m,\ u'_l \ne u'_m\}$$

in extension field representation, vector space $\mathcal{W}$ with $\dim(\mathcal{W}) = k$ inside $\mathcal{R}$, all $(k-1)$-dimensional subspaces $\mathcal{W}_f$ of $\mathcal{W}$, $f = 1, \ldots, \frac{(q^n-1)(q^{n-1}-1)\ldots(q^2-1)}{(q^{n-1}-1)(q^{n-2}-1)\ldots(q-1)}$

for each subspace $\mathcal{W}_f$ **do**
  for each $r = (r_f \ r'_f) \in \mathcal{W}_f \setminus \{0\}$ **do**
    for each $s = (s_f \ s'_f) \in \mathcal{W}_f \setminus \{0, r\}$ **do**

compute $c_{r_f,s_f} := \frac{r_f}{s_f}$, $c'_{r'_f,s'_f} := \frac{r'_f}{s'_f}$ in extension field representation
end for
end for
for $(c_{r_f,s_f}, c'_{r'_f,s'_f})$ be in S **do**
find $\theta(\alpha) = \alpha^i$ such that $\exists\ x, y \in \mathcal{U}$: $x\theta(\alpha) = r_f$, $y\theta(\alpha) = s_f$
find $\theta'(\alpha) = \alpha^j$ such that $\exists\ x', y' \in \mathcal{U}$: $x'\theta'(\alpha) = r'_f$, $y'\theta'(\alpha) = s'_f$
compute $U_1\mathrm{M}^i_{p_1}$ and $U_2\mathrm{M}^j_{p_2}$
store $\mathrm{rs}(U_1\mathrm{M}^i_{p_1} \quad U_2\mathrm{M}^j_{p_2})$
end for
if $\mathrm{rs}(U_1\mathrm{M}^i_{p_1} \quad U_2\mathrm{M}^j_{p_2})$ is a subspace of $\mathcal{R}$ **then**
find k-th linearly independent vector from $\mathrm{rs}(U_1\mathrm{M}^i_{p_1} \quad U_2\mathrm{M}^j_{p_2})$
return $\mathcal{W}_f$ with k-th linearly independent vector
end if
end for

Example 3.2. *Consider $\mathcal{U} \in \mathcal{G}_2(3,8)$ and primitive polynomials $p_1(x) = 1 + x + x^4$ and $p_2(x) = 1 + x^3 + x^4$ in $\mathbb{F}_2[x]$. Let α_1, α_2 be roots of $p_1(x)$ and $p_2(x)$, respectively. We have*

$$\mathrm{M}_{p_1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}, \qquad \mathrm{M}_{p_2} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

Assume that

$$\mathcal{U} = \mathrm{rs}\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \end{array}\right).$$

In fact

$$\begin{aligned} \mathcal{U} \;=\; & \{(0,0,0,0,0,0,0,0), (1,0,0,0,1,0,0,0), (1,1,0,0,0,0,1,0), (0,0,1,0,0,1,1,0), \\ & (0,1,0,0,1,0,1,0), (1,1,1,0,0,1,0,0), (1,0,1,0,1,1,1,0), (0,1,1,0,1,1,0,0)\}. \end{aligned}$$

We observe that

$$\begin{aligned} & \phi^{(4,4)}(u_2) = (1,1), \quad \phi^{(4,4)}(u_3) = (\alpha_1^4, \alpha_2^2), \quad \phi^{(4,4)}(u_4) = (\alpha_1^2, \alpha_2^{13}), \quad \phi^{(4,4)}(u_5) = (\alpha_1, \alpha_2^9), \\ & \phi^{(4,4)}(u_6) = (\alpha_1^{10}, \alpha_2), \quad \phi^{(4,4)}(u_7) = (\alpha_1^8, \alpha_2^7), \quad \phi^{(4,4)}(u_8) = (\alpha_1^5, \alpha_2^{12}). \end{aligned}$$

Therefore

$$\begin{aligned} & b_2 = 0,\ b'_2 = 0, \quad b_3 = 4,\ b'_3 = 2, \quad b_4 = 2,\ b'_4 = 13, \quad b_5 = 1,\ b'_5 = 9, \\ & b_6 = 10,\ b'_6 = 1, \quad b_7 = 8,\ b'_7 = 7, \quad b_8 = 5,\ b'_8 = 12. \end{aligned}$$

It results that

$$\begin{aligned} D \;=\; & \pm\{(11,13), (13,2), (14,6), (5,14), (7,8), (10,3), (2,4), (3,8), (9,1), (11,10), (14,5), \\ & (1,4), (7,12), (9,6), (12,1), (6,8), (8,2), (11,12), (2,9), (5,4), (3,10)\}. \end{aligned}$$

So $d = 1$ and the minimum distance of orbit code $\mathcal{C} = \mathcal{U}G$ is 4.
Since the minimum distace is 4, it can correct at most 1 error. Assume that we recived

vector $\mathcal{R}$ *with* $\dim(\mathcal{R}) = 4$. *Let*

$$\mathcal{R} = \mathrm{rs}\left(\begin{array}{cccc|cccc} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right).$$

Choose a 3*-dimensional subspace* $\mathcal{W}$ *inside* $\mathcal{R}$ *in the form*

$$\mathcal{W} = \mathrm{rs}\left(\begin{array}{cccc|cccc} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \end{array}\right).$$

We make seven of 2*-dimenstional subspaces of* $\mathcal{W}$ *which are*

$$\mathcal{W}_1 = \mathrm{rs}\left(\begin{array}{cccc|cccc} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \end{array}\right) \cong \{0, (\alpha_1^4, \alpha_2^2), (\alpha_1^{10}, \alpha_2), (\alpha_1^2, \alpha_2^{13})\},$$

$$\mathcal{W}_2 = \mathrm{rs}\left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \end{array}\right) \cong \{0, (\alpha_1^{10}, \alpha_2), (\alpha_1^9, \alpha_2^5), (\alpha_1^{13}, \alpha_2^4)\},$$

$$\mathcal{W}_3 = \mathrm{rs}\left(\begin{array}{cccc|cccc} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \end{array}\right) \cong \{0, (\alpha_1^4, \alpha_2^2), (\alpha_1^9, \alpha_2^5), (\alpha_1^{14}, \alpha_2^6)\},$$

$$\mathcal{W}_4 = \mathrm{rs}\left(\begin{array}{cccc|cccc} 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \end{array}\right) \cong \{0, (\alpha_1^2, \alpha_2^{13}), (\alpha_1^9, \alpha_2^5), (\alpha_1^{11}, \alpha_2^{11})\},$$

$$\mathcal{W}_5 = \mathrm{rs}\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \end{array}\right) \cong \{0, (\alpha_1^{14}, \alpha_2^6), (\alpha_1^{10}, \alpha_2), (\alpha_1^{11}, \alpha_2^{11})\},$$

$$\mathcal{W}_6 = \mathrm{rs}\left(\begin{array}{cccc|cccc} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \cong \{0, (\alpha_1^4, \alpha_2^2), (\alpha_1^{13}, \alpha_2^4), (\alpha_1^{11}, \alpha_2^{11})\},$$

$$\mathcal{W}_7 = \mathrm{rs}\left(\begin{array}{cccc|cccc} 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \cong \{0, (\alpha_1^2, \alpha_2^{13}), (\alpha_1^{13}, \alpha_2^4), (\alpha_1^{14}, \alpha_2^6)\}.$$

Since these sets are pairwise distinct, it is enough to compute the quotient of only one pair of these sets. Therefore we have

$$c_1 := \frac{\alpha_1^4}{\alpha_1^{10}} = \alpha_1^{\pm 9},\ c_1' := \frac{\alpha_2^2}{\alpha_2} = \alpha_2^{\pm 1}, \quad c_2 := \frac{\alpha_1^{10}}{\alpha_1^9} = \alpha_1^{\pm 1},\ c_2' := \frac{\alpha_2}{\alpha_2^5} = \alpha_2^{\pm 11},$$
$$c_3 := \frac{\alpha_1^4}{\alpha_1^9} = \alpha_1^{\pm 10},\ c_3' := \frac{\alpha_2^2}{\alpha_2^5} = \alpha_2^{\pm 12}, \quad c_4 := \frac{\alpha_1^2}{\alpha_1^9} = \alpha_1^{\pm 8},\ c_4' := \frac{\alpha_2^{13}}{\alpha_2^5} = \alpha_2^{\pm 8},$$
$$c_5 := \frac{\alpha_1^{14}}{\alpha_1^{10}} = \alpha_1^{\pm 4},\ c_5' := \frac{\alpha_2^6}{\alpha_2} = \alpha_2^{\pm 5}, \quad c_6 := \frac{\alpha_1^4}{\alpha_1^{13}} = \alpha_1^{\pm 6},\ c_6' := \frac{\alpha_2^2}{\alpha_2^4} = \alpha_2^{\pm 13},$$
$$c_7 := \frac{\alpha_1^2}{\alpha_1^{13}} = \alpha_1^{\pm 4},\ c_7' := \frac{\alpha_2^{13}}{\alpha_2^4} = \alpha_2^{\pm 9}.$$

On the other hand

$$\begin{aligned} S = \{&(\alpha_1^{\pm 11}, \alpha_2^{\pm 13}), (\alpha_1^{\pm 13}, \alpha_2^{\pm 2}), (\alpha_1^{\pm 14}, \alpha_2^{\pm 6}), (\alpha_1^{\pm 5}, \alpha_2^{\pm 14}), (\alpha_1^{\pm 7}, \alpha_2^{\pm 8}), (\alpha_1^{\pm 10}, \alpha_2^{\pm 3}), (\alpha_1^{\pm 2}, \alpha_2^{\pm 4}), \\ &(\alpha_1^{\pm 3}, \alpha_2^{\pm 8}), (\alpha_1^{\pm 9}, \alpha_2^{\pm 1}), (\alpha_1^{\pm 11}, \alpha_2^{\pm 10}), (\alpha_1^{\pm 14}, \alpha_2^{\pm 5}), (\alpha_1^{\pm 1}, \alpha_2^{\pm 4}), (\alpha_1^{\pm 7}, \alpha_2^{\pm 12}), (\alpha_1^{\pm 9}, \alpha_2^{\pm 6}), \\ &(\alpha_1^{\pm 12}, \alpha_2^{\pm 1}), (\alpha_1^{\pm 6}, \alpha_2^{\pm 8}), (\alpha^{\pm 8}, \alpha^{\pm 2}), (\alpha_1^{\pm 11}, \alpha_2^{\pm 12}), (\alpha_1^{\pm 2}, \alpha_2^{\pm 9}), (\alpha_1^{\pm 5}, \alpha_2^{\pm 4}), (\alpha_1^{\pm 3}, \alpha_2^{\pm 10})\}. \end{aligned}$$

We see that (c_1, c_1') *and* (c_5, c_5') *are in the set of* S.
From (c_1, c_1'), *we have*

$$\{\alpha_1^{4-i}, \alpha_1^{10-i}\} = \{\alpha_1^4, \alpha_1^{10}\} \Longrightarrow 4-i \equiv 4 \pmod{15}, \quad 10-i \equiv 10 \pmod{15}.$$
$$\{\alpha_2^{2-j}, \alpha_2^{1-j}\} = \{\alpha_2^2, \alpha_2\} \Longrightarrow 2-j \equiv 2 \pmod{15}, \quad 1-j \equiv 1 \pmod{15}.$$

So $(i, j) = (0, 0)$.
Also for (c_5, c_5'), *we can write*

$$\{\alpha_1^{14-i}, \alpha_1^{10-i}\} = \{\alpha_1^8, \alpha_1^4\} \Longrightarrow 14-i \equiv 8 \pmod{15}, \quad 10-i \equiv 4 \pmod{15}.$$
$$\{\alpha_2^{6-j}, \alpha_2^{1-j}\} = \{\alpha_2^7, \alpha_2^2\} \Longrightarrow 6-j \equiv 7 \pmod{15}, \quad 1-j \equiv 2 \pmod{15}.$$

Thus $(i, j) = (6, 14)$. *We calculate* $\mathrm{rs}(U_1\mathrm{M}_{p_1}^6 \quad U_2\mathrm{M}_{p_2}^{14})$.
It shows that we can get a third linearly independent vector from $\mathrm{rs}(U_1\mathrm{M}_{p_1}^6 \quad U_2\mathrm{M}_{p_2}^{14})$ *which is in* $\mathcal{R}$. *So we decode to the codeword*

$$K = \mathrm{rs}\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{array}\right).$$

4. Conclusion

First, we presented an overwiev of subspace codes, orbit codes and the minimum distance of them. Furthermore, when we have at most 1 error, we investigated how to decode irreducible cyclic orbit code $\mathcal{C} = \mathcal{U} < \mathrm{M}_p >$ and orbit code $\mathcal{C} = \mathcal{U}G$. The complexity of these two algorithms depend mainly on the number of quotients. When k is small, the number of quotients is small. While when k is big, it gets more difficult to compute all quotients. Therefore, if the dimension of vector spaces k is small, these two algorithms are efficient.

References

[1] Elsenhans, A., Kohnert, A. and Wassermann, A., (2010), Construction of codes for network coding, Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems-MTNS (Budapest, Hungary), pp. 1811-1814.

[2] Ghatak, A., (2014), Construction of Singer Subgroup Orbit Codes Based on Cyclic Different Sets, 20 national conference on communications.

[3] Gluesing-Luerssen, H., Morrison, K. and Troha, C., (2014), Cyclic orbit codes and stabilizer subfields. arXiv:1403.1218.

[4] Herstein, I. N., (1975), Topics in algebra. 2nd ed. Lexington, Mass.: Xerox College Publishing.

[5] Jungnickel, D., (1993), Finite fields, structure and arithmetic, BI-Wiss.-Verl.

[6] Kerber, A., (1999), Applied Finite Group Actions, Algorithms and Combinatorics, Vol. 19, Springer-Verlag.

[7] Lidl, R. and Niederreiter, H., (1994), Introduction to Finite Fields and their applications. Cambridge University Press, Cambridge, London, Revised edition.

[8] Trautmann, A. L. and Rosenthal, J., (2011), A Complete Characterization of Irreducible Cyclic Orbit Codes. In Proceedings of the Seventh International Workshop on Coding and Cryptography-WCC 2011, pp. 219-228.

[9] Trautmann, A. L., Manganiello, F., Braun, M. and Rosenthal, J., (2013), Cyclic Orbit Codes. IEEE Transactions on Information Theory, no. 99, pp. 1-18.

[10] Trautmann, A. L., Manganiello, F. and Rosenthal, J., (2010), Orbit codes-a new concept in the area of network coding. In IEEE Information Theory Workshop, Dublin, Ireland, pp. 1-4.

Mahdieh Hakimi Poroch received her B.Sc. degree from Alzahra University, M.Sc. degree from K. N. Toosi University of Technology and Ph.D. degree from University of Mazandaran, all in mathematics. Her research interests include algebraic graph theory, network coding theory and cryptography.

Ali Asghar Talebi is assistant professor in the University of Mazandaran. He received his B.Sc. degree from University of Birjand, M.Sc. degree from Ferdowsi University of Mashhad and Ph.D. degree from Iran University of Science and Technology. His current research interests inculde algebraic graph theory, coding theory and fuzzy graph theory.