LINEAR CODES ON UNITARY SPACE

Mahdieh Hakimi Poroch*
Department of Mathematics
University of Mazandaran
Babolsar, Iran
m.hakimiporoch@stu.umz.ac.ir

Ali Asghar Talebi
Department of Mathematics
University of Mazandaran
Babolsar, Iran
a.talebi@umz.ac.ir

Abstract. Linear codes are an important class of codes. They are the most studied codes from a mathematical point of view. In this work, we propose linear codes in unitary space, then describe a way for finding a new parity check matrix of linear codes in unitary space. In the end, we give a decoding procedure for linear codes in unitary space.

Keywords: linear codes, generator matrix, parity check matrix, unitary space.

1. Introduction

Among all types of codes, linear codes are studied the most. Since linear codes are vector spaces, their algebraic structure often make them easier to describe, encode, and decode than nonlinear codes. The code alphabet for linear codes is a finite field, although sometimes other algebraic structures can be used to define codes that are also called linear.

Let $\mathbb{F}_q^n$ denote the vector space of all n-tuples over the finite field $\mathbb{F}_q$. An (n, M)-code $\mathcal{C}$ over $\mathbb{F}_q$ is a subset of $\mathbb{F}_q^n$ of size M. If $\mathcal{C}$ is a k-dimensional subspace of $\mathbb{F}_q^n$, then $\mathcal{C}$ will be called an $[n, k]$-linear code over $\mathbb{F}_q$. The linear code $\mathcal{C}$ has q^k codewords. If $\mathcal{C}$ has the minimum distance d, then $\mathcal{C}$ is an $[n, k, d]$-linear code over $\mathbb{F}_q$. The Hamming weight of a vector V is the number of its non-zero entries and is denoted by $\mathrm{w}_H(v)$. We have $\mathrm{w}_H(v) = d_H(v, 0)$. The minimum weight of the code $\mathcal{C}$ is the minimum non-zero weight among all codewords of $\mathcal{C}$, $\mathrm{w}_{\min}(\mathcal{C}) = \min_{0 \neq x \in \mathcal{C}}(\mathrm{w}_H(x))$.

It is customary to put the codewords of a basis for a linear code $\mathcal{C}$ into a matrix. A generator matrix for an $[n, k]$-code $\mathcal{C}$ is any $k \times n$ matrix G whose rows form a basis for $\mathcal{C}$. Also a parity check matrix of a linear code $\mathcal{C}$ is a matrix H whose columns form a basis for the dual code $\mathcal{C}^{\perp}$.

∗. Corresponding author

Moreover, a code is of practical use only if an efficeint decoding scheme can be applied to it. For linear codes, syndrome decoding is an efficient way to decode them. In fact, let $\mathcal{C}$ be an $[n, k, d]$-linear code over $\mathbb{F}_q$, then for any $v \in \mathbb{F}_q^n$, the syndrome of v is the word $S(v) = vH^t$.

Now, we want to describe linear codes in unitary space. This paper is organized as follows: In the second section, we mention some notes about linear codes and their minimum distance. In the third section, we introduce unitary space, linear codes in unitary space, then find a new parity-check matrix of linear codes in unitary space. Also we assert syndrome decoding of linear codes in unitary space. Finally we conclude with the summary of the main results of this paper.

2. Preliminaries

A linear code $\mathcal{C}$ of lenght n and dimension k over $\mathbb{F}_q$ is often called a q-ary $[n, k]$-code or an $[n, k]$-code. It is also an (n, q^k)-linear code. If the distance d of $\mathcal{C}$ is known, it is also sometimes referred to as an $[n, k, d]$-linear code.

Definition 2.1. Let x be a word in $\mathbb{F}_q^n$. The (Hamming) weight of x, denoted by $\mathrm{w}(x)$, is defined to be the number of non-zero coordinates in x, i.e. $\mathrm{w}(x) = d(x, 0)$, where 0 is the zero word.

An important invariant of a code is the minimum distance between codewords. The (Hamming) distance $d(x, y)$ between two vectors $x, y \in \mathbb{F}_q^n$ is defined to the number of coordinates in which x and y differ.

Lemma 2.2 (5, Lemma 5.1)**.** *If $x, y \in \mathbb{F}_q^n$, then $d(x, y) = \mathrm{w}(x - y)$.*

The (minimum) distance of a code $\mathcal{C}$ is the smallest distance between distinct codewords and is important in determining the error-correcting capability of $\mathcal{C}$. In fact, the (minimum) distance of $\mathcal{C}$ is denoted by $d(\mathcal{C})$, where

$$d(\mathcal{C}) = \min\{d(x, y) \mid x, y \in \mathcal{C},\ x \neq y\}.$$

Theorem 2.3 (7, Theorem 4.3.8)**.** *Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$. Then $d(\mathcal{C}) = \mathrm{w}(\mathcal{C})$.*

Theorem 2.4 (5, Theorem 5.5)**.** *Let G be a generator matrix of an $[n, k]$-code, then G can be transformed to the standard form $[I_k|A]$, where I_k is the $k \times k$ identity matrix and A is a $k \times (n - k)$ matrix.*

Since the generator matrix of a linear code has full row rank, it is quite obvious that any linear code is equivalent to a linear code that has a generator matrix in standard form.

Definition 2.5. Let $\mathcal{C}$ be an $[n, k]$-code over $GF(q)$ and a is any vector in V. Then the set $a + \mathcal{C}$ is defined by $a + \mathcal{C} = \{a + x \mid x \in \mathcal{C}\}$, is called a coset of $\mathcal{C}$.

Theorem 2.6 (5, Theorem 6.4)**.** *Suppose that $\mathcal{C}$ is an $[n,k]$-code over $GF(q)$, then:*

1. *every vector of $V(n,q)$ is in some coset of $\mathcal{C}$,*
2. *every coset contains exactly q^k vectors,*
3. *two cosets either are disjoint or coinside.*

H is the generator matrix of some codes, called the dual or orthogonal of $\mathcal{C}$ and denoted $\mathcal{C}^\perp$. Notice that $\mathcal{C}^\perp$ is an $[n, n-k]$-code. In fact,

$$\mathcal{C}^\perp = \{x \in \mathbb{F}_q^n \mid x.c = 0,\ \forall c \in \mathcal{C}\}.$$

If G is in standard form $[I_k|A]$, one can take $H = [-A^t|I_{n-k}]$. Also we have $HG^t = 0$.

Theorem 2.7 (5, Theorem 7.5)**.** *Let $\mathcal{C}$ be an $[n,k]$-code on $V(n,q)$, then $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.*

3. Linear codes in unitary space

In this section, we want to introduce linear codes in unitary space and some of their properties.

Definition 3.1. A bilinear form on a vector space V over a field $\mathbb{F}$ is a function $<,>: V \times V \longrightarrow \mathbb{F}$ that satisfies

$$< \lambda u + \mu v, w >= \lambda < u, w > +\mu < v, w >,$$
$$< u, \lambda v + \mu w >= \lambda < u, v > +\mu < u, w >,$$

for all $u, v, w \in V$ and $\lambda, \mu \in \mathbb{F}$.

It is symmetric, if $< u, v >=< v, u >$ for all $u, v \in \mathbb{F}$. It is skew-symmetric, if $< u, v >= - < v, u >$, for all $u, v \in \mathbb{F}$. It is also an alternating, if $< v, v >= 0$ for all $v \in \mathbb{F}$.

Definition 3.2. A conjugate symmetric sesquilinear form on V over a field $\mathbb{F}$ that has an automorphism σ of order 2, is a function $<,>: V \times V \longrightarrow \mathbb{F}$ that satisfies $< \lambda u + \mu v, w >= \lambda < u, w > +\mu < v, w >$, and $< u, v >=< v, u >^\sigma$, for all $u, v, w \in V$ and $\lambda, \mu \in \mathbb{F}$.

If $X \subseteq V$, then define the subspace $X^\perp = \{v \in V \mid < x, v >= 0, \forall x \in X\}$. The set $X^\perp$ is called the radical of $<,>$ and is denoted $\mathrm{Rad}(<,>)$. We say that $<,>$ is non-degenerate if $\mathrm{Rad}(<,>) = 0$.

A non-degenerate conjugate symmetric sesquilinear form is called a unitary form. A vector space V together with a unitary form is called unitary space and is denoted by $(V, <,>_U)$.

A vector $v \in V$ is called isotropic if $< v, v >_U = 0$. A subspace W of V is called totally isotropic if $<,>_U$ restricted to W is zero.

Theorem 3.3 (3, Theorem 18.1)**.** *All automorphisms $GF(q^m)$ over $GF(q)$ are $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$, where $\sigma_j(\alpha) = \alpha^{q^j}$, $\alpha \in GF(q^m)$, $0 \leq j \leq m-1$. As a result*

$$\mathrm{Aut}(\frac{GF(q^m)}{GF(q)}) \cong \mathbb{Z}_m.$$

By Theorem 3.3, for non-degenerate unitary space $(V, <, >_U)$ with $\dim(V) = n$ over $\mathbb{F}$, we have $\mathbb{F} = GF(q^2)$ and $\sigma(a) = a^q = \overline{a}$ $(a \in \mathbb{F})$.

Definition 3.4. If V is a unitary space with form $<, >_U$, then an isometry g of V is an invertible linear transformation of V that satisfies $< ug, vg >_U = < u, v >_U$ for all $u, v \in V$.

Definition 3.5. Let $(V, <, >_U)$ be a unitary space and $B = \{v_1, \ldots, v_n\}$ be an ordered basis of V. Then $B = (b_{ij})_{1 \leq i,j \leq n}$ in which $b_{ij} = < v_i, v_j >_U$, $1 \leq i, j \leq n$ is called matrix of form $<, >_U$ related to basis B. Hence for every $x, y \in V$, we can write

$$x = \sum_{i=1}^{n} x_i v_i, \quad y = \sum_{j=1}^{n} y_j v_j.$$

such that $x_i, y_j \in \mathbb{F}$, $1 \leq i, j \leq n$. Therefore

$$\begin{aligned} < x, y >_U &= < \sum_{i=1}^{n} x_i v_i, \sum_{j=1}^{n} y_j v_j >_U = \sum_{i,j=1}^{n} x_i < v_i, v_j >_U {y_j}^{\sigma} \\ &= \sum_{i,j=1}^{n} x_i b_{ij} {y_j}^{\sigma} = x^t B y^{\sigma}. \end{aligned}$$

Proposition 3.6 (6, Proposition 2.3.2)**.** *Let V be a $2n$-dimensional unitary vector space with unitary form $<, >_U$. Then there is a basis $v_1, \ldots, v_n, w_1, \ldots, w_n$ of V such that for all i, j, we have*

$$< v_i, v_j >_U = < w_i, w_j >_U = 0, \quad < v_i, w_j >_U = \delta_{ij}.$$

Such a basis for a unitary vector space V is called a unitary basis.

Definition 3.7. Assume that $(V, <, >_U)$ is a non-degenerate unitary space with $\dim(V) = n$ over field $GF(q^2)$. With choosing unitary basis, a unitary form can be described for $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$, $x, y \in V$ by

$$< x, y >_U = x_1 \overline{y}_1 + x_2 \overline{y}_2 + \cdots + x_n \overline{y}_n = \sum_{i=1}^{n} x_i \overline{y}_i.$$

3.1 The dual code in a non-degenerate unitary space

In a non-degenerate unitary space $V(n,q)$, if for $u,v \in V(n,q)$, $< u,v >_U = 0$, then u and v are called orthogonal.

The dual code of a linear code $\mathcal{C}$ in $V(n,q)$ is denoted by $\mathcal{C}^{\perp_U}$. In fact, it is the set of those vectors of $V(n,q)$ which are orthogonal to every codeword of $\mathcal{C}$, i.e. $\mathcal{C}^{\perp_U} = \{v \in V(n,q) | < u,v >_U = 0, \forall u \in \mathcal{C}\}$. It is easy to check that $\mathcal{C}^{\perp_U}$ is a linear code.

Let G be a generator matrix of $\mathcal{C}$. A vector v of $V(n,q)$ belongs to $\mathcal{C}^{\perp_U}$ if and only if u is orthogonal to every row of G. It means that $v \in \mathcal{C}^{\perp_U}$ if and only if $< v,u >_U = 0$, for every row u of G.

Lemma 3.8. *Let $(V, <,>_U)$ be a non-degenerate unitary space of finite dimension. If W is a subspace of V, then*

$$\dim W^{\perp_U} = \dim V - \dim W$$

Proof. Let V^* be the dual space of vector space V. The map ϕ, where

$$\begin{aligned} \phi : V &\longrightarrow V^* \\ v &\longmapsto \phi_v \end{aligned}$$

and $\phi_v(w) =< v,w >_U$, $\forall w,v \in V$ is a inversable linear transformation.

Let $\{w_1, w_2, \ldots, w_k\}$ be a basis for W. We claim that the elements of $\phi_{w_i} \in V^*$, $1 \leq i \leq k$ are independent. Assume that

$$\sum_{i=1}^{k} \lambda_i \phi_{w_i} = 0, \quad \lambda_i \in \mathbb{F},$$

then

$$\sum_{i=1}^{k} \lambda_i \phi_{w_i}(v) = \sum_{i=1}^{k} \lambda_i < w_i, v >_U = < \sum_{i=1}^{k} \lambda_i w_i, v >_U = 0, \quad \forall v \in V.$$

Since $(V, <,>_U)$ is non-degenerate, it follows that

$$\sum_{i=1}^{k} \lambda_i w_i = 0 \Longrightarrow \lambda_i = 0, \quad \text{for} \ \ 1 \leq i \leq n.$$

Therefore the elements of ϕ_{w_i}, $(1 \leq i \leq k)$ are distinct independent. As a result

$$\begin{aligned} W^{\perp_U} &= \{x \in V \mid < w_i, x >_U = 0, \ \ \forall w_i, \ 1 \leq i \leq k\} \\ &= \{x \in V \mid \phi_{w_i}(x) = 0, \ \ \forall w_i, \ 1 \leq i \leq k\} \\ &= \{x \in V \mid x \in \ker \phi_{w_i}, \ \ \forall w_i, \ 1 \leq i \leq k\} \\ &= \bigcap_{i=1}^{k} \ker \phi_{w_i}. \end{aligned}$$

But ϕ_{w_i} is a non-zero functional and the dimension of its kernel is $\dim V - 1$. Because ϕ_{w_i}, $(1 \leq i \leq k)$ are independent, it yields that

$$\dim\left(\bigcap_{i=1}^{k}\ker\phi_{w_i}\right)=\dim V-k.$$

The proof is complete. □

If $\mathcal{C}$ is an $[n,k]$-code on $V(n,q)$, then $\mathcal{C}^{\perp_U}$ is an $[n,n-k]$-code.

Theorem 3.9. *Let $\mathcal{C}$ be an $[n,k]$-code on $V(n,q)$, then $(\mathcal{C}^{\perp_U})^{\perp_U}=\mathcal{C}$.*

Proof. Since every vector of $\mathcal{C}$ is orthogonal to every vector of $\mathcal{C}^{\perp_U}$, so $\mathcal{C}\subseteq(\mathcal{C}^{\perp_U})^{\perp_U}$. On the other hand,

$$\dim\left((\mathcal{C}^{\perp_U})^{\perp_U}\right)=n-\dim\left(\mathcal{C}^{\perp_U}\right)=n-(n-k)=k=\dim\left(\mathcal{C}\right),$$

thus $(\mathcal{C}^{\perp_U})^{\perp_U}=\mathcal{C}$. □

For a vector $u\in V(n,q)$ and a $(l\times n)$ matrix B with rows $r_1,r_2,\ldots,r_l$, we define $u.B=(<u,r_1>_U,<u,r_2>_U,\ldots,<u,r_l>_U)$.

Definition 3.10. A parity check matrix H_U for an $[n,k]$-code $\mathcal{C}$ on $V(n,q)$ is a generator matrix of $\mathcal{C}^{\perp_U}$.

H_U is an $(n-k)\times n$ matrix satisfying $<h,g>_U=0$ for every row h of H_U and row g of generator matrix G, i.e. $g.H_U=0$.

From Lemma 3.8 and Theorem 3.9, if H_U is a parity check matrix of an $[n,k]$-code $\mathcal{C}$, then $\mathcal{C}=\{x\in V(n,q)\mid x.H_U=0\}$

Theorem 3.11. *If $G=[I_k|A]$ is the generator matrix of an $[n,k]$-code $\mathcal{C}$, then a parity check matrix of $\mathcal{C}$ is $H_U=[B|I_{n-k}]$ where $A=(a_{ij})_{k\times(n-k)}$, $B=(b_{kt})_{(n-k)\times k}$ and $b_{kt}=-\overline{a_{tk}}$.*

Proof. H_U has the size required of a parity-check matrix and its rows are linearly independent. It is enough to show that every row of H_U is orthogonal to every row of G.

Let u be the ith row of H_U and v is the jth row of G. Then

$$v=(0,\ldots,0,\overbrace{1}^{j\text{th}},0,\ldots,0,a_{j\times1},a_{j\times2},\ldots,a_{j\times(n-1)},a_{j\times n}),$$

$$u=(-\overline{a_{1\times i}},-\overline{a_{2\times i}},\ldots,-\overline{a_{j\times i}},\ldots,-\overline{a_{k\times i}},0,\ldots,\overbrace{1}^{(k+i)\text{th}},0,\ldots,0).$$

Therefore $<v,u>_U=-a_{j\times i}+a_{j\times i}=0$. For other rows of H_U and G, it is similar. □

3.2 Syndrome decoding

Let Let H_U be a parity check matrix of an $[n,k]$-code $\mathcal{C}$. Then for any vector $v \in V(n,q)$, the $1 \times (n-k)$ row vector $S(v) = vH_U$ is called the syndrome of v.

If the columns of H_U are $H_1, H_2, \ldots, H_{n-k}$, then

$$S(v) = (< v, H_1 >_U, < v, H_2 >_U, \ldots, < v, H_{n-k} >_U).$$

Also $S(v) = 0$ if and only if $v \in \mathcal{C}$.

Proposition 3.12. *Two vectors u and v are in the same coset of $\mathcal{C}$ if and only if they have the same syndrome.*

Proof. For two arbitrary vectors u and v in $V(n,q)$, u and v are in the same coset

$$\begin{aligned}
&\iff u + \mathcal{C} = v + \mathcal{C} \\
&\iff u - v \in \mathcal{C} \\
&\iff (u-v)H_U = 0 \\
&\iff (< u-v, H_1 >_U, \ldots, < u-v, H_{n-k} >_U) = 0, \\
&\qquad H_i \ (1 \le i \le n-k) \text{ is } i\text{th column of } H_U \\
&\iff (< u, H_1 >_U, \ldots, < u, H_{n-k} >_U) = (< v, H_1 >_U, \ldots, < v, H_{n-k} >_U) \\
&\iff uH_U = vH_U \\
&\iff S(u) = S(v).
\end{aligned}$$

□

Theorem 3.13. *Let $\mathcal{C}$ be an $[n,k]$-code with parity check matrix H_U. For each codeword of Hamming weight t, there exist t-columns of H_U which are linearly dependent. Conversely if there exist t-columns linearly dependent of H_U, then there exists a codeword of Hamming weight t in $\mathcal{C}$.*

Proof. Assume that the parity check matrix H_U is in the form $H_U = (H_1, H_2, \ldots, H_n)$, where H_i represents the ith column of H_U. Given a codeword $v = (v_1, v_2, \ldots, v_n) \in \mathcal{C}$, we have $0 = vH_U = (v_1\overline{H}_1, v_2\overline{H}_2, \ldots, v_n\overline{H}_n)^t$. This implies that $\mathcal{C}$ has a vector v of weight t if and only if H_U has t-columns linearly dependent. □

Corollary 3.14. *Let $\mathcal{C}$ be an $[n,k]$-code with the parity check matrix H_U, then the minimum distance of $\mathcal{C}$ is equal to the smallest number of columns of H_U that are linearly independent.*

The vector having minimum weight in a coset is called the coset leader.

From group theory, we know that if $\mathcal{C}$ is an $[n,k]$-code over $GF(q)$, then $V(n,q)$ is partitioned into disjoint cosets of $\mathcal{C}$ as follows: $V(n,q) = (0+\mathcal{C}) \cup (e_1+\mathcal{C}) \cup \ldots \cup (e_r+\mathcal{C})$, where $r = q^{n-k} - 1$.

We may choose $0, e_1, \ldots, e_r$ to be the coset leader.

Now we present a method to partition the 2^n vectors of $V(n,q)$ to $\frac{2^n}{2^k} = 2^{n-k}$ cosets. We place the elements of $\mathcal{C}$ in a row with the vector 0 as left most element. Select from the remaining vector, a vector e_1 of minimum weight, then form the second row by placing e_1 under 0 and e_1+x under x for each $x \in \mathcal{C}$. We continue this process untill we have used all elements of $V(n,q)$. Now we have an array of rows and columns. This is called a standard array of $\mathcal{C}$.

If $v_1 = 0, v_2, \ldots, v_{2^k}$ are the codewords of $\mathcal{C}$, in Figure 1, we show a standard array of $\mathcal{C}$.

Coset Leader					
v_1=0	v_2	$\ldots$	v_j	$\ldots$	v_{2^k}
e_2	e_2+v_2	$\ldots$	e_2+v_j	$\ldots$	$e_2+v_{2^k}$
e_3	e_3+v_2	$\ldots$	e_3+v_j	$\ldots$	$e_3+v_{2^k}$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
$e_{2^{n-k}}$	$e_{2^{n-k}}+v_2$	$\ldots$	$e_{2^{n-k}}+v_j$	$\ldots$	$e_{2^{n-k}}+v_{2^k}$

Figure 1. Standard array for an $[n,k]-$code.

We know that the syndrome of a vector in $V(n,q)$ is an $(n-k)$-tuple and there is one to one correspondence between a coset leader and a syndrome. We form a decoding table which consists of 2^{n-k} coset leaders and their corresponding syndromes. The steps of the decoding of a received vectors are as follows:

1. Get the syndrome of v, vH_U,
2. Determind the coset leader e_l whose its syndrome is vH_U,
3. Decode the received vector v into $v - e_l$.

Example 3.15. Write $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$. Let $\mathcal{C}$ be the $\mathbb{F}_4$-linear code with generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & \alpha & \alpha \\ 0 & 1 & 0 & \alpha & 1 & \alpha \\ 0 & 0 & 1 & \alpha & \alpha & 1 \end{pmatrix}.$$

Since $\sigma(\alpha) = \alpha^2 = \overline{\alpha}$, the parity check matrix of $\mathcal{C}$ is

$$H_U = \left(\begin{array}{ccc|ccc} -1 & -\alpha^2 & -\alpha^2 & 1 & 0 & 0 \\ -\alpha^2 & -1 & -\alpha^2 & 0 & 1 & 0 \\ -\alpha^2 & -\alpha^2 & -1 & 0 & 0 & 1 \end{array}\right).$$

By Corollary 3.14, the minimum distance of the code is 3, so it is possible to correct the error patterns of weight 1 or 0. Hence all vectors of weight 1 or 0 can

be used as coset leader. The correcable error patterns and their corresponding syndromes are given in Table 1.

Syndrome	Coset Leader
$(1,\alpha,\alpha)$	(1,0,0,0,0,0)
$(\alpha,1,\alpha)$	(0,1,0,0,0,0)
$(\alpha,\alpha,1)$	(0,0,1,0,0,0)
(1,0,0)	(0,0,0,1,0,0)
(0,1,0)	(0,0,0,0,1,0)
(0,0,1)	(0,0,0,0,0,1)

Table 1: Decoding Table for the $\mathbb{F}_4$-linear code $\mathcal{C}$.

Assume that the codeword $v = (0,1,0,\alpha,1,\alpha)$ is transmitted and $w = (0,1,1,\alpha,1,\alpha)$ is received. We compute the syndrome of w. We have

$$wH_U = (0,1,1,\alpha,1,\alpha)\left(\begin{array}{ccc|ccc} -1 & -\alpha^2 & -\alpha^2 & 1 & 0 & 0 \\ -\alpha^2 & -1 & -\alpha^2 & 0 & 1 & 0 \\ -\alpha^2 & -\alpha^2 & -1 & 0 & 0 & 1 \end{array}\right) = (\alpha,\alpha,1).$$

From Table 1, we see that $(\alpha,\alpha,1)$ is the syndrome of the coset leader $e = (0,0,1,0,0,0)$. Hence $(0,0,1,0,0,0)$ is assumed to be the error pattern and w is decoded into: $v = w - e = (0,1,1,\alpha,1,\alpha) - (0,0,1,0,0,0) = (0,1,0,\alpha,1,\alpha)$.

Example 3.16. Let $\mathcal{C}$ be a code over $GF(9)$ with parity check matrix

$$H_U = \left(\begin{array}{cccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{array}\right).$$

Suppose that $v = (v_1, v_2, \ldots, v_8)$ is the codeword transmitted and $w = (w_1, w_2, \ldots, w_8)$ is the received vector.

Assume that a single error has occurred such that the error magnitude is k and the error position is l. Then $(w_1, w_2, \ldots, w_8) = (v_1, \ldots, v_{l-1}, v_l + k, v_{l+1}, \ldots, v_8)$. The syndrome is

$$\begin{aligned}(s_1, s_2) = wH_U &= (\overline{1}w_1 + \overline{1}w_2 + \overline{1}w_3 + \overline{1}w_4 + \overline{1}w_5 + \overline{1}w_6 + \overline{1}w_7 + \overline{1}w_8, \\ &\quad \overline{1}w_1 + \overline{2}w_2 + \overline{3}w_3 + \overline{4}w_4 + \overline{5}w_5 + \overline{6}w_6 + \overline{7}w_7 + \overline{8}w_8).\end{aligned}$$

$$\begin{aligned} s_1 &= \overline{1}w_1 + \overline{1}w_2 + \overline{1}w_3 + \overline{1}w_4 + \overline{1}w_5 + \overline{1}w_6 + \overline{1}w_7 + \overline{1}w_8 \\ &= \overline{1}v_1 + \overline{1}v_2 + \overline{1}v_3 + \overline{1}v_4 + \overline{1}v_5 + \overline{1}v_6 + \overline{1}v_7 + \overline{1}v_8 + k \equiv k \pmod 9 \\ s_2 &= \overline{1}w_1 + \overline{2}w_2 + \overline{3}w_3 + \overline{4}w_4 + \overline{5}w_5 + \overline{6}w_6 + \overline{7}w_7 + \overline{8}w_8 \\ &= \overline{1}v_1 + \overline{2}v_2 + \overline{3}v_3 + \overline{4}v_4 + \overline{5}v_5 + \overline{6}v_6 + \overline{7}v_7 + \overline{8}v_8 + \overline{l}k \equiv \overline{l}k \pmod 9. \end{aligned}$$

Since $\sigma(\alpha) = \alpha^2 = \overline{\alpha}$, we have

$$\begin{aligned} s_1 &= w_1 + w_2 + w_3 + w_4 + w_5 + w_6 + w_7 + w_8 \\ &= v_1 + v_2 + v_3 + v_4 + v_5 + v_6 + v_7 + w_8 + k \equiv k \pmod 9 \\ s_2 &= w_1 + 4w_2 + 7w_4 + 7w_5 + 7w_7 + w_8 \\ &= v_1 + 4v_2 + 7v_4 + 7v_5 + 7v_7 + v_8 + \overline{l}k \equiv \overline{l}k \pmod 9. \end{aligned}$$

With simple computation, we see that the error position l is given by $(\overline{\frac{s_2}{s_1}})$ and the error magnitude k is given by s_1.

After calculating the syndrome (s_1, s_2), the decoding scheme is as follows:

1. If $(s_1, s_2) = (0, 0)$, then w is a codeword and we assume that there is no errors,

2. Suppose $s_1 \neq 0$, $s_2 \neq 0$. We assume that a single error has occurred which is corrected by subtracting s_1 from the $(\overline{\frac{s_2}{s_1}})$th entry of w,

3. If $s_1 = 0$ or $s_2 = 0$ but not both, it follows that there are at least two errors.

For example, if received vector is $w = 21513412$, we get $s_1 = 1$ and $s_2 = 7$, so $(\overline{\frac{s_2}{s_1}}) = 4$. Thus the 4th digit should have been $1 - 1 = 0$, *i.e.* transmitted vector is 21503412.

4. Conclusion

In this work, we investigated unitary space and linear codes in unitary space. Also, we mentioned a new parity check matrix of linear codes in unitary space and syndrome decoding of linear codes. For further research, it would be natural to generalized our presented results for linear codes in orthogonal space.

References

[1] A. Bereczky, *Maximal overgroups of singer elements in classical groups*, Journal of Algebra, 234 (2000), 187-206.

[2] T. Brookfield, *Overgroups of a linear singer cyclic in classical groups*, School of Mathematics the University of Birmingham, Sep 2014.

[3] M. R. Darafsheh, *Linear groups*, Tehran University, 1998.

[4] R. H. Dye, *Maximal subgroups of finite orthogonal and unitary groups stabilizing anisotropic subspaces*, Math. Zeit., 189 (1985), 111-129.

[5] R. Hill, *A first course in coding theory*, Oxford Applied Mathematics and Computing Science Series, University of Salford, 1986.

[6] P. B. Kleidman and M. W. Liebeck, *The subgroup structure of the finite classical groups*, 129, Cambridge University Press, 1990.

[7] S. Ling, C. Xing, *Coding theory*, National University of Singapore, 2004.

Accepted: 22.10.2017