CARLETON UNIVERSITY

SCHOOL OF
MATHEMATICS AND STATISTICS

HONOURS PROJECT

TITLE: Coding for Multiple User Access Channels

AUTHOR: Joseph Lentini

SUPERVISOR: Dr. Panario

DATE: July 29, 2019

Coding for Multiple User Access Channels

Giuseppe Lentini

August 7, 2019

Abstract

In this project, we give constructions of linear codes with a complementary dual (LCD) and $\mathcal{T}$-Direct code over $\mathbb{F}_q$. We then show that these families of codes can be used to encode multiple user access channels.

1 Introduction

In 1992, Massey [17] first defined linear codes with a complementary dual (LCD Codes) as a linear code C in which their dual code is the orthogonal complement of C. Massey gave a complete characterization of all LCD codes using generating matrices and proposed a class of LCD codes. It was also shown that LCD codes can be used to encode two-user binary adder channels. Two years later in 1994, Massey and Yang [18] gave the necessary and sufficient condition for a cyclic code to be LCD. However, it took until 2004 for Sendrier [22] to prove that LCD codes were asymptotically good by showing that LCD codes meet the Gilbert-Varshamov Bound.

Recently many authors have constructed new classes of LCD codes. [6], [9], [13], [14], [15]. Furthermore, in [23], the authors have constructed optimal LCD codes using orthogonal matrices. This construction takes removing number of rows from an orthogonal matrix and then takes the matrix product of this matrix with one or multiple diagonal matrices. Finally, in [3], the authors use self-orthogonal codes to construct a new class of Euclidean and Hermitian LCD

codes. The authors also prove that for all $q > 3$, there exists an (n, k) Euclidean Maximum Distance Separable (MDS) LCD code over $\mathbb{F}_q$. This completely solves the Euclidean case.

In addition to two-user binary adder channels, Carlet and Guilley in [4] have shown that LCD codes simultaneously improves the resistance against side-channel attacks and fault injection attacks.

After Massey published his 1992 paper on LCD codes, Vasantha and Raja Durai published in 2002 an analogous paper [25] to Massey's on the subject of $\mathcal{T}$-Direct codes. These codes are a generalization of LCD codes. Similar to Massey, Vasantha and Raja Durai gave a complete characterization of all $\mathcal{T}$-Direct codes using their generating matrices. It was also shown that $\mathcal{T}$-Direct codes can be used to encode the noiseless $\mathcal{T}$-user Binary Adder Channel. However, it was not until 2011 in [20] that the first classes of $\mathcal{T}$-Direct codes were constructed. This $\mathcal{T}$-Direct code which has n constituent codes and hence an n-Direct code is constructed using an n-Direct code in which each constituent code was a Maximum Rank Distance (MRD) code. Using the generator matrices of the MRD constituent codes, they take the Kroenecker product of a certain number of these generator matrices to create matrices that generate a $\mathcal{T}$-Direct code. In 2011, Raja Durai and Devi constructed n-Direct codes and $(2n-1)$-Direct codes over $\mathbb{F}_{2^n}$. In 2018, Raja Durai and Devi in [7], using the same method as in [20], constructed n^3-Direct codes, n^n-Direct codes and n^{3^m}-Direct codes over $\mathbb{F}_{2^n}$.

This report is structured as follows. In Section 2, we present preliminaries which is divided into three subsections. The first subsection, finite fields preliminaries and notation is given.The second subsection provides the linear algebra background on matrices as well as subspaces. The final subsection gives the required coding theory preliminaries. In Section 3, we define LCD codes and $\mathcal{T}$-Direct codes, and then construct classes of these codes. In Section 4, we discuss applications of LCD codes and $\mathcal{T}$-Direct codes to the information theoretic problem of multiple user access channels. Finally, in Section 5, we discuss possible research directions moving forward.

2 Preliminaries

In order to study LCD codes and T-Direct codes, we need to familiarize ourselves with finite fields, matrices, as well as some matrix operations. Finally, we define linear codes. It should be noted that almost all proofs in this section are omitted for brevity.

2.1 Finite Fields

Before we can define a field, we must define two different algebraic structures. The first of which is a group.

2.1.1 Definition [21] Let G be a nonempty set. The function $* : G \times G \to G$ is a *binary operation.*

2.1.2 Definition [16] Let G be a nonempty set and $*$ be a binary operation. $(G, *)$ is a *group* if
1) $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$;
2) for all $a \in G$ there exists some $e \in G$ such that $a * e = e * a = a$;
3) for all $a \in G$ there exists some $b \in G$ such that $a * b = b * a = e$.
Futher, G is *abelian* if
4) $a * b = b * a$ for all $a, b \in G$.

Now that we have a defined a group, we can now define a ring using the definition of a group. Rings are important algebraic since every field is a ring, so all definitions and theorems pertaining to rings apply also to fields.

2.1.3 Definition [16] Let R be a set, and $+$ and $\cdot$ be binary operations.

$(R, +, \cdot)$ is a *ring* if

1) $(R, +)$ is an abelian group;

2) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$;

3) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in R$.

2.1.4 Definition [8],[16] Let $(R, +, \cdot)$ be a ring. If $a \cdot b = b \cdot a$ for all $a, b \in R$, then $(R, +, \cdot)$ is a *commutative ring*. If $(R \setminus \{0\}, \cdot)$ is a group, then $(R, +, \cdot)$ is a *division ring*.

2.1.5 Definition [16] Let $(R, +, \cdot)$ be a commutative division ring. Then $(R, +, \cdot)$ is a *field*.

2.1.6 Definition [8] Let $(R, +, \cdot)$ be a ring and $S \subseteq R$. If $(S, +, \cdot)$ is a ring, then S is a *subring* of R.

2.1.7 Definition [16] Let R be a ring. The least such $n \in \mathbb{Z}$ such that $nr = 0$ for every $r \in R$, if it exists, is the *characteristic* of R and R has characteristic n. If no such n exists, R has characteristic 0.

For the remainder of the report, we denote a group $(G, *)$ by G and a ring $(R, +, \cdot)$ by R. We only use the notation of Definition 2.1.2 and Definition 2.1.3 if we need to specify the binary operations of G and R.

We know define a particular class of subrings that are important in properly defining a finite field.

2.1.8 Definition [16] Let J be a subring of R. J is an *ideal* if $ar, ra \in J$ for every $r \in R$ and every $a \in J$.

2.1.9 Definition [16] Let R be a commutative ring. An ideal J of R is *principal* if there exists an $a \in R$ such that $J = \langle a \rangle = \{ra : r \in R\}$.

We now construct a finite field with p elements for p a prime.

2.1.10 Definition [16] Let $a \in \mathbb{Z}$ and $\langle n \rangle$ be the principal ideal generated by $n \in \mathbb{Z} > 0$. The set $[a] = a + \langle n \rangle$ is the residue class of a modulo n and

$$\mathbb{Z}/\langle n \rangle = \{[0] = 0 + \langle n \rangle, [1] = 1 + \langle n \rangle, \ldots, [n-1] = n - 1 + \langle n \rangle\}.$$

2.1.11 Definition [16] For a prime p, let $\mathbb{F}_p$ be the set $\{0, 1, \ldots, p-1\}$ of integers and let $\varphi : \mathbb{Z}/\langle p \rangle \to \mathbb{F}_p$ be the mapping defined by $\varphi([a]) = a$ for $a = 0, 1, \ldots, p-1$. Then $\mathbb{F}_p$, endowed with the field structure induced by φ, is a finite field called the *Galois field of order p*.

For the remainder of the report we use $\mathbb{F}_p$ to denote the Galois field of order p for p prime and p is a prime number. Not only is $\mathbb{F}_p$ a finite field, it is the foundation for constructing finite fields that do not have a prime number of elements. To do this, first, we need to define a polynomial ring.

2.1.12 Definition [16] Let R be a ring. The *polynomial ring over* R is the set

$$R[x] = \{a_0 + a_1 x + \cdots + a_n x^n : a_0, \ldots a_n \in R\}.$$

2.1.13 Definition [16] Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ with $f(x) \not\equiv 0$. Then n is the *degree* of $f(x)$ and a_n is the *leading coefficient* of f.

2.1.14 Definition [16] Let F be a field. A polynomial $p \in F[x]$ is *irreducible* over F if p has positive degree and $p = bc$ implies b or c is a constant polynomial for $b, c \in F[x]$.

We can now create a class of finite fields with p^n elements using polynomials.

2.1.15 Theorem [24] Let $g \in \mathbb{F}_p[x]$ an irreducible polynomial of degree n.

The residue class ring $F[x]/\langle g\rangle$ is a field with p^n elements.

Now that we have created finite fields with p^n. However using this construction we may have more then one finite field with p^n elements. For example, as noted in [16] there are 18 irreducible polynomials of degree 7 over $\mathbb{F}_2$, so there are at least 18 fields of order 2^7. Before we can proceed, we need to state one more important fact about finite fields of order p^n: the uniqueness property. To do this we need to define one final algebraic structure: a vector space. Vector spaces will also play an important part in the subsections on linear algebra and coding theory.

2.1.16 Theorem [2] Suppose V is a set with the operations of vector addition and scalar multiplication. Then V is a *vector space* over F if the following hold:
1) $\mathbf{u}+\mathbf{v} \in V$ for all $\mathbf{u}, \mathbf{v} \in V$;
2) $\alpha\mathbf{u} \in V$ for all $\alpha \in F$ and $\mathbf{u} \in V$;
3) $\mathbf{u}+\mathbf{v} = \mathbf{v}+\mathbf{u}$ for all $\mathbf{u}, \mathbf{v} \in V$;
4) $\mathbf{u}+(\mathbf{v}+\mathbf{w}) = (\mathbf{u}+\mathbf{v})+\mathbf{w}$ for all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$;
5) For all $\mathbf{u} \in V$, there exists a vector $\mathbf{0}$ such that $\mathbf{u}+\mathbf{0} = \mathbf{u}$;
6) For all $\mathbf{u} \in V$, there exists a vector $-\mathbf{u} \in V$ such that $\mathbf{u}+(-\mathbf{u}) = 0$;
7) $\alpha(\beta\mathbf{u}) = (\alpha\beta)\mathbf{u}$ for all $\alpha, \beta \in F$ and $\mathbf{u} \in V$;
8) $\alpha(\mathbf{u}+\mathbf{v}) = \alpha\mathbf{u}+\alpha\mathbf{v}$ forall $\alpha \in F$ and $\mathbf{u}, \mathbf{v} \in V$;
9) $(\alpha+\beta)\mathbf{u} = \alpha\mathbf{u}+\beta\mathbf{u}$ forall $\alpha, \beta \in F$ and $\mathbf{u} \in V$;
10) $1\mathbf{u} = \mathbf{u}$ for all $\mathbf{u} \in V$.

2.1.17 Definition [2] Let V and W be vector spaces. If $W \subseteq V$, and W and V have the same vector addition and scalar multiplication, then W is a *subspace* V.

2.1.18 Definition [2] Let V be a vector space, $S = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\} \subseteq V$

and F a field. The *span of* S is the set

$$\text{span}(S) = \{\alpha_1\mathbf{u}_1 + \alpha_2\mathbf{u}_2 + \cdots + \alpha_n\mathbf{u}_n : \alpha_1, \ldots, \alpha_n \in F\}.$$

2.1.19 Definition [2] Let V be a vector space. A subset $S \subseteq V$ is a *spanning set* of V if $\text{span}(S) = V$. In this case S *spans* V.

2.1.20 Definition [2] Let V be a vector space, F a field, and $S \subseteq V$ such that $S = \{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$. An equation of the form

$$\alpha_1\mathbf{u}_1 + \cdots + \alpha_n\mathbf{u}_n = 0$$

for $\alpha_1, \ldots, \alpha_n \in F$ is a *relation of linear dependence on* S. If $\alpha_i = 0$ for all $1 \leq i \leq n$, then it is a *trivial relation of linear dependence.*

2.1.21 Definition [2] Suppose V is a vector space and $S = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\} \subseteq V$. S is *linearly independent* if there is a trivial relation of linear dependence.

2.1.22 Definition [2] Suppose V is a vector space. Then a subset $S \subseteq V$ is a *basis* of V if it is linearly independent and spans V.

2.1.23 Definition [2] Suppose V is a vector space and $\{\mathbf{v}_1, \ldots, \mathbf{v}_t\}$ is a basis of V. Then the *dimension* of V is defined by $\dim(V) = t$. In this case, V is *finite dimensional.* If V has no finite dimension, V is *infinite-dimensional.*

2.1.24 Theorem [1] Let V be a finite-dimensional vector space and U, a subspace of V. If $\dim U = \dim V$, then $U = V$.

The final step before we can give the uniqueness of a finite field is to definite a subfield and a field extension.

2.1.25 Definition [16] Let F be a field and $K \subseteq F$. If K is field under

the operations of F, then K is a *subfield* of F and F is an *extension* of K. If $K \neq F$, K is a *proper subfield*. A field containing no proper subfields is a *prime field*.

2.1.26 Definition [16] Let L be an extension field of K. If L, considered as a vector space over K, is finite-dimensional, then L is a *finite extension* of K. The dimension of the vector space L over K is the *degree* of L over K, denoted $[L : K]$.

2.1.27 Theorem [16] Let F be a finite field. Then F has p^n elements, where the prime p is the characteristic of F and n is the degree of F over its prime subfield.

Now we know that there is only finite fields of prime powers. So there is no finite field with $6, 10, 12, 14, \ldots$ elements.

2.1.28 Definition [16] Let $f \in K[x]$ be of positive degree and F, an extension field of K. Then f *splits* in F if there exists elements $\alpha_1, \ldots, \alpha_n \in F$ such that

$$f(x) = a(x - \alpha_1) \cdots (x - \alpha_n),$$

where a is the leading coefficient of f. The field F is a *splitting field* of f over K if f splits F and if, moreover, $F = K(\alpha_1, \ldots, \alpha_n)$ where $K(\alpha_1, \ldots, \alpha_n)$ is the extension field of F obtained by adjoining $\alpha_1, \ldots, \alpha_n$.

2.1.29 Theorem [16] For every prime p and every positive integer n there exists a finite field with p^n elements. Any finite field with $q = p^n$ elements is isomorphic to the splitting field of $x^q - x$ over $\mathbb{F}_p$.

Now we know that finite fields of order p^n are unique up to isomorphism. Hence, any property that holds over one finite field of order p^n holds over all of

them, so we may unambigously refer to the finite field of order p^n. Therefore we denote $\mathbb{F}_{p^n}$ as the finite field with p^n elements. For the remainder of the report, we let $q = p^n$ in the context of a finite field. So we denote a finite field with q elements by $\mathbb{F}_q$. Further, we use $\mathbb{F}_q^\times$ to denote the set of all nonzero elements of $\mathbb{F}_q$.

Finally, for the section on $\mathcal{T}$-Direct codes, we must define a trace-orthogonal basis and a normal basis.

2.1.30 Definition [16] Let $F = \mathbb{F}_{q^m}$, $K = \mathbb{F}_q$ and $\alpha \in F$. The trace $\mathrm{Tr}_{F/K}(\alpha)$ of α over K is

$$\mathrm{Tr}_{F/K}(\alpha) = \sum_{i=0}^{m-1} \alpha^{q^i}.$$

2.1.31 Definition [16] Let $K = \mathbb{F}_q$ and $F = \mathbb{F}_{q^m}$. Then a basis of F over K of the form $\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$ for $\alpha \in F$ is a *normal basis* of F over K.

2.1.32 Definition [12] Let $B = \{\alpha_1, \ldots, \alpha_n\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. B is a *trace-orthogonal basis* if
i) $\mathrm{Tr}_{F/K}(\alpha_i) = 1$ for all $\alpha_i \in B$;
ii) $\mathrm{Tr}_{F/K}(\alpha_i \alpha_j) = 0$ for all $\alpha_i, \alpha_j \in B$, $i \neq j$.

2.2 Linear Algebra

The first definition we give is that of a matrix. Matrices are a very fundamentally important concept in linear algebra. It also plays an important role in coding theory.

2.2.1 Definition [2] Let F be a field. An $m \times n$ *matrix* is a rectangular layout of elements from F having m rows and n columns. If A is an $m \times n$ matrix, then $[A]_{ij} \in F$ denotes the entry in the ith row and jth column of A.

2.2.2 Definition [2] Let A be an $m \times n$ matrix and B be a $m \times k$ matrix, then $[A|B]$ denotes the $m \times (n+k)$ matrix with the first n being the n columns of A and the last k columns being the columns of B.

One important matrix is the identity matrix.

2.2.3 Definition [2] The $m \times m$ *identity matrix*, I_m is the matrix

$$[I_m]_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

for $1 \leq i, j \leq m$.

The columns of I_n form a set called the standard basis. We denote $\mathbf{e}_i$ as the ith column of I_n. Hence,

$$\begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}$$

where the ith position is a 1 and all the other positions are 0.

We now define a class of matrices that give us a representation of a code as we see in the coding theory background.

2.2.4 Definition [2] Let F be a field. An *n-dimensional vector* is a $1 \times n$ matrix. If $\mathbf{v}$ is an n-dimensional vector, then $v_i \in F$ denotes the ith entry of $\mathbf{v}$ for $1 \leq i \leq n$. The set of all n-dimensional vectors is denoted F^n.

Now we define operations that may be performed on one or multiple matrices.

2.2.5 Definition [2] Let A and B be $m \times n$ matrices, and $\alpha \in F$. The following three operations on matrix are *row operations*.

1) Swap the location of two rows;

2) Multiply each entry of a single row by a $\alpha \neq 0$;

3) Multiply each entry of a row by some $\alpha \neq 0$ and add these values to the entries in the same columns of a second row. Leave the first row the same but replace the second row by these new values.

If B can be obtained from A by a sequence of row operations, A and B are *row equivalent*.

2.2.6 Definition [2] Let A be an $m \times n$ matrix. The *transpose* of A, denoted by A^T, is the $n \times m$ matrix given by

$$[A^T]_{ij} = [A]_{ji}$$

for $1 \leq i \leq n$, $1 \leq j \leq m$.

2.2.7 Definition [2] Let A be an $m \times n$ matrix with columns $\mathbf{A}_1, \ldots, \mathbf{A}_n$ and $\mathbf{u}$ an n-dimensional vector. Then the *matrix-vector product* of A with $\mathbf{u}$ is

$$A\mathbf{u} = u_1 A_1 + \cdots + u_n A_n.$$

2.2.8 Definition [2] Let A be an $m \times n$ matrix and B an $n \times k$ matrix with columns $\mathbf{B}_1, \ldots, \mathbf{B}_k$. Then the *matrix product* of A and B is the $m \times k$ matrix

$$AB = [A\mathbf{B}_1 | \cdots | A\mathbf{B}_k].$$

Now that we have defined a matrix-vector product, we can define another important class of matrices that will be fundamental when studying LCD codes: the class of nonsingular matrices.

2.2.9 Definition [2] Let A be an $n \times n$ matrix. A is *nonsingular* if $A\mathbf{x} = \mathbf{0}$ implies $\mathbf{x} = 0$. Otherwise A is *singular*.

Now that we've defined what a nonsingular matrix, we need ways of determing whether or not a matrix is nonsingular. Fortunately, as we will see shortly, the determinant infact does that.

2.2.10 Definition [2] Let A be an $n \times n$ matrix and $A(i|j)$ be the submatrix obtained by removing the ith row and the jth column. The *determinant* of A, denoted $\det(A)$, is defined recursively by

1. If A is a 1×1 matrix then $\det(A) = [A]_{11}$.
2. If A is an $n \times n$ matrix for $n \geq 2$, then

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+1} [A]_{ii} \det(A(1|i)).$$

We now present a few equivalent definitions of a matrix being nonsingular. This is not an exhaustive list of all nonsingular matrix equivalencies. One may refer to [2] for such a list. Here we only give the ones that is used when proving classes of LCD codes and $\mathcal{T}$-Direct codes.

2.2.11 Theorem [2] Let A be an $n \times n$ matrix. The following are equivalent.

i) A is nonsingular;

ii) A is row equivalent to I_n;

iii) $\det(A) \neq 0$.

Finally, we define one final matrix operation which we use to create classes of $\mathcal{T}$-Direct codes.

2.2.12 Definition [20] Let

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}$$

be an $m \times n$ matrix and B be a $r \times s$ matrix. The *kronecker product* $A \otimes B$ is

the $mr \times ns$ matrix

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix}.$$

2.2.13 Lemma [11] Let A be an $m \times n$ matrix, B, a $k \times l$ matrix, C, an $n \times r$ matrix, D, an $l \times s$ matrix, E, an $n \times n$ matrix and F, an $m \times m$ matrix. Then
1) $(A \otimes B)^T = A^T \otimes B^T$;
2) $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$;
3) $\det(E \otimes F) = \det(E)^m \det(F)^n$.

We now define two sets of matrices which are in fact groups under the operation of matrix multiplication. The group of orthogonal matrices will allow us to create classes of LCD codes.

2.2.14 Definition [8],[23] Let $M_{n\times n}$ be the set of $n \times n$ matrices. The *general linear group* over a field F, denoted $GL(n, F)$, is the set

$$GL(n, F) = \{A \in M_{n\times n} : \det(A) \neq 0\}.$$

The *orthogonal group of index n* over $\mathbb{F}_q$, denoted $\mathcal{O}_n(q)$, is the set

$$\mathcal{O}_n(q) = \{A \in GL(n, \mathbb{F}_q) : AA^T = I_n\}.$$

Any matrix in $\mathcal{O}_n(q)$ is an *orthogonal matrix*.

Next we give a lemma that is used in proofs from the section on LCD codes. Since we have not found this lemma in any of the literature on this subject, we provide a proof.

2.2.15 Lemma Let A be an orthogonal matrix and A_k be the matrix obtained by removing any k rows. Then $A_k A_k^T = I_{n-k}$.

Proof. We proceed by induction on k.

Base case. We begin by removing the ith row of A and call this matrix A_1. Then A_1^T is going to be the matrix A^T with the ith column removed. So we are multiplying an $(n-1) \times n$ matrix by an $n \times (n-1)$ matrix. The resulting product will be an $(n-1) \times (n-1)$ matrix. Hence we only need to show that this matrix is the identity matrix.

Recall that since A is orthogonal, $AA^T = I_n$. If we can show that $A_1 A_1^T$ is obtained from AA^T by removing the ith row and the ith column, then we are done. We know that

$$AA^T = [A(\mathbf{A}^T)_1 | \cdots | A(\mathbf{A}^T)_n]$$

by Definition 2.2.8, but since we removing the ith column of A^T to obtain A_1^T, we have that

$$AA_1^T = [A(\mathbf{A}^T)_1 | \cdots | A(\mathbf{A}^T)_{i-1} | A(\mathbf{A}^T)_{i+1} | \cdots | A(\mathbf{A}^T)_n].$$

and so

$$AA_1^T = [A(\mathbf{A}_1^T)_1 | \cdots | A(\mathbf{A}_1^T)_{n-1}].$$

Next we show that $A_1 A_1^T$ is obtained by removing the ith row of AA_1^T. Let $(\mathbf{A}\mathbf{A}_1^T)_l$ be the lth column of AA_1^T. Then

$$(\mathbf{A}\mathbf{A}_1^T)_l = \begin{cases} A(\mathbf{A}^T)_l & \text{if } 1 \leq l \leq i-1 \\ A(\mathbf{A}^T)_{l+1} & \text{if } i \leq l \leq n-1 \end{cases}$$

If $1 \leq l \leq i-1$, then by Definition 2.2.8

$$(\mathbf{A}\mathbf{A}_1^T)_l = a_{l1}\mathbf{A}_1 + \cdots + a_{ln}\mathbf{A}_n.$$

and if $i \leq l \leq n-1$, then

$$(\mathbf{A}\mathbf{A}_1^T)_l = a_{l+1,1}\mathbf{A}_1 + \cdots + a_{l+1,n}\mathbf{A}_n.$$

In either case, the jth entry of this column vector is going to be a linear combination of the jth row of A. Hence, if we remove the ith row of A, we are

removing the ith entry of $(\mathbf{A}\mathbf{A}_1^T)_l$ from our vector. Since $(\mathbf{A}\mathbf{A}_1^T)_l$ is the lth column of AA_1^T, if we remove the ith row of A, we are also removing the ith row of AA_1^T while all other rows of AA_1^T remain the same. Thus $A_1A_1^T$ is obtained from AA^T by removing the ith row and the ith column.

Induction Assumption. Let A_k be the matrix obtained by removing k rows from A. Then $A_kA_k^T = I_{n-k}$.

Induction Step. Let $\mathbf{A}_{i_1}, \ldots, \mathbf{A}_{i_{n-k}}$ be the $n-k$ rows of A in A_k. By our induction assumption $A_kA_k^T = I_{n-k}$, so if we can show that removing the jth row from A_k results in removing the jth row and jth column from $A_kA_k^T$, then it follows that $A_{k+1}A_{k+1}^T = I_{n-k-1}$. As in the base case, if we remove the jth column from A_k^T, we are also removing the jth entry in each row of $A_kA_k^T$. Also, the jth entry in each column of $A_kA_k^T$ is a linear combination of the jth row of A_k, we are removing the jth row of $A_kA_k^T$ while preserving all other rows. So $A_{k+1}A_{k+1}^T$ is obtained by removing the jth row and jth column from $A_kA_k^T$, as required. □

Since we have layed out a background in matrices, we start using matrices to define two subspaces that is used in the next subsection on coding theory.

2.2.16 Definition [2] Let A be an $m \times n$ matrix with columns $\mathbf{A}_1, \ldots, \mathbf{A}_n$ and F be a field. The *column space* of A, denoted $\mathcal{C}(A)$, is the subset of F containing all linear combinations of the columns of A. The *row space* of A, denoted $\mathcal{R}(A)$, is the column space of A^T, i.e., $\mathcal{R}(A) = \mathcal{C}(A^T)$. The *rank* of A, denoted $r(A)$, is the dimension of the column space of A.

We now define another subspace that will become fundamental in the application of LCD codes and $\mathcal{T}$-Direct codes to multiple user access channels.

2.2.17 Definition [1] Let $U_1, \ldots, U_m$ be subspaces of V. The set

$$U_1 + \cdots + U_m = \{u_1 + \cdots + u_m : u_i \in U_i \text{ for all } 1 \leq i \leq m\}$$

is a *direct sum* if each element of $U_1 + \cdots + U_m$ can be written uniquely as a sum $u_1 + \cdots + u_m$ for $u_i \in U_i$. If $U_1 + \cdots + U_m$ is a direct sum, it is denoted $U_1 \oplus \cdots \oplus U_m$.

2.2.18 Theorem [1] Let U and W be subspaces of a vector space V. Then $U + W$ is a direct sum if and only if $U \cap W = \{0\}$.

2.2.19 Theorem [1] Let V be a vector space and $U_1, \ldots, U_m$, finite-dimensional subspaces of V. If $U_1 + \cdots + U_m$ is a direct sum, then $U_1 \oplus \cdots \oplus U_m$ is finite-dimensional and

$$\dim(U_1 \oplus \cdots \oplus U_m) = \dim U_1 + \cdots + \dim U_m.$$

Finally we define the inner product of two vectors. This is used to define the dual code of a linear code.

2.2.20 Definition [23] Let F be a field and $\mathbf{x}, \mathbf{y} \in F^n$. Then the *Euclidean inner product* of $\mathbf{x}$ and $\mathbf{y}$ is

$$\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i.$$

2.3 Coding Theory

We begin our section on coding theory by defining a linear code.

2.3.1 Definition [16] Let H be an $(n-k) \times n$ matrix of rank $n-k$ with entries in $\mathbb{F}_q$. The set C of all n-dimensional vectors $\mathbf{c} \in \mathbb{F}_q^n$ such that $H\mathbf{c}^T = 0$

is a *linear (n,k) code* over $\mathbb{F}_q$; n is the *length* and k is the *dimension* of the code. The elements of C are *codewords*, and the matrix H is the *parity-check matrix* of C.

It is traditional in coding that $\mathbf{c}$ is actually an $n \times 1$ matrix instead of the $1 \times n$ matrix from Definition 2.2.3. So $\mathbf{c}^T$ is a $1 \times n$ matrix.

Most times when we define a linear code C, we are not defining it by its parity-check matrix. We instead define it using its generator matrix.

2.3.2 Definition [16] Let C be an (n, k) code, G be a $k \times n$ matrix. If $\mathcal{R}(G) = C$, then G is a *generator matrix* of C.

2.3.3 Remark [19] Let C be an (n, k) code, G be the generator matrix, and $\mathbf{u} \in \mathbb{F}_q^k$. Then $\mathbf{u}$ corresponds to the codeword $\mathbf{x} \in C$ under the relation that $\mathbf{x} = \mathbf{u}G$.

Every linear code has a dual code. As van Lint explains in [24], the dual code of C is not necessarily an orthoogonal complement of C. The dual code of C might equal C itself, or it may intersect with C in some other non-trivial way.

2.3.4 Definition [16] Let C be a linear (n, k) code over $\mathbb{F}_q$. Then its *dual code* is defined as

$$C^{\perp} = \{\mathbf{x} \in \mathbb{F}_q^n : \mathbf{x} \cdot \mathbf{y} = 0, \text{ for all } \mathbf{y} \in C\}.$$

2.3.5 Proposition [17] Let C be a linear (n, k) code over $\mathbb{F}_q$. Then $C = (C^{\perp})^{\perp}$.

2.3.6 Proposition [16] Let C be a linear (n,k) code over $\mathbb{F}_q^n$. If G is the generator matrix for C, then G is the parity-check matrix for $C^{\perp}$. Also, if H is the parity-check of C, then H is the generator matrix of $C^{\perp}$.

Apart from the length and the dimension of the code, there is one more parameter that is important to linear codes.

2.3.7 Definition [24] Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$. The *Hamming distance* $d(\mathbf{x}, \mathbf{y})$ of $\mathbf{x}$ and $\mathbf{y}$ is

$$d(\mathbf{x}, \mathbf{y}) := |\{i : 1 \leq i \leq n, x_i \neq y_i\}|.$$

2.3.8 Definition [24] Let $C \subseteq \mathbb{F}_q^n$ be a nontrivial code. The *minimum distance* of C, denoted d is

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

The minimum distance is important because it characterizes the code's error detection and error correction capability. In the sequel, we give an important bound on the minimum distance: the Singleton Bound.

2.3.9 Theorem [24] (*Singleton Bound*) For any (n, k) code C over $\mathbb{F}_q$, we have $d \leq n - k + 1$.

A special case of the singleton bound, is when the minimum distance is equal to the singleton bound.

2.3.10 Definition [19] Let C be an (n, k) code over $\mathbb{F}_q$. If we have $d = n-k+1$, then C is *maximum distance separable (MDS)*.

We conclude the background on coding by defining maximum rank distance (MRD) codes. These codes will be used to generate classes of $\mathcal{T}$-Direct codes.

2.3.11 Definition [20] Let V^n be an n-dimensional vector space over $\mathbb{F}_{q^m}$ for $n \leq m$, $\mathbf{u}_1, \ldots, \mathbf{u}_m$ a fixed basis of $\mathbb{F}_{q^m}$ as a vector over $\mathbb{F}_q$, $\mathbf{x} = (x_1, \ldots, x_n) \in V^n$ for $x_i \in \mathbb{F}_{q^m}$, and A_m^n the collection of all $m \times n$ matrices over $\mathbb{F}_q$. The

$m \times n$ matrix $A(\mathbf{x})$ is defined as

$$A(\mathbf{x}) = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}$$

for $x_i = a_{1i}\mathbf{u}_1 + \cdots + a_{mi}\mathbf{u}_m$. The *rank* of $\mathbf{x}$ over $\mathbb{F}_q$ is the rank of $A(\mathbf{x})$ and is denoted $r(\mathbf{x}; q)$.

2.3.12 Proposition [20] The norm $r(\mathbf{x}; q)$ specifies a rank metric on V^n.

2.3.13 Definition [20] Let V^n be an n-dimensional vector space over $\mathbb{F}_q^m$ for $n \leq m$. A linear (n, k)-code over V^n is a *Rank Distance (RD)* code if it metric is induced by the rank norm. An (n, k) RD code is a *Maximum Rank Distance (MRD)* code if $d = n - k + 1$.

2.3.14 Definition [20] Let G be the generator matrix of an (n, k) MRD code and $\{\alpha^{q^0}, \alpha^{q^1}, \ldots, \alpha^{q^{n-1}}\}$, a normal basis of $\mathbb{F}_{q^n}$. Then

$$G = \begin{bmatrix} \alpha^{q^0} & \alpha^{q^1} & \cdots & \alpha^{q^{n-1}} \\ \alpha^{q^1} & \alpha^{q^2} & \cdots & \alpha^{q^n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{q^{k-1}} & \alpha^{q^k} & \cdots & \alpha^{q^{k+n-2}} \end{bmatrix}.$$

3 LCD Codes

As mentioned in the previous section, the dual code of a linear code C is not necessarily an orthogonal complement of C. As we see throughout the remainder of the report, linear codes that have the property that their dual code is an orthogonal complement are ideal for coding schemes with multiple users. We demonstrate what happens when we restrict our attention to such codes. For

the most part, the proofs will either be similar to the original authors with more detail.

3.1 Definitions and Theorems

We will begin our study of LCD codes by defining what is an LCD code.

3.1.1 Definition [17] Let C be a linear (n, k) code over $\mathbb{F}_q$. Then C is a *linear code with a complementary dual (LCD)* if $C \cap C^{\perp} = \{\mathbf{0}\}$.

An immediate consequence of the definition of an LCD code is the following.

3.1.2 Proposition [17] Let C be a linear (n, k) code over $\mathbb{F}_q$. If C is an LCD code, then $C^{\perp}$ is an LCD code.

Proof. Let C be an LCD code. Then, $C \cap C^{\perp} = \{\mathbf{0}\}$. So, using this fact with Proposition 2.3.5, we get that

$$C^{\perp} \cap (C^{\perp})^{\perp} = C^{\perp} \cap C = \{\mathbf{0}\}.$$

□

To use LCD codes to encode coding schemes with two users, we need to make sure that when the codeword from C and the codeword from $C^{\perp}$ get sent into the common channel, they can be decoded without any ambiguity. The following theorem shows us that we can do this.

3.1.3 Proposition [17] Let C be a linear (n, k) code over $\mathbb{F}_q$. We have that $\mathbb{F}_q^n = C \oplus C^{\perp}$ if and only if C is an LCD code.

Proof. First, suppose $\mathbb{F}_q^n = C \oplus C^{\perp}$, then $C \cap C^{\perp} = \{0\}$ by Theorem 2.2.18. Hence C is an LCD Code.

Now suppose C is an LCD code, then $C \cap C^{\perp} = \{0\}$ and thus $C \oplus C^{\perp}$ is a direct sum. Since $C, C^{\perp} \subseteq \mathbb{F}_q^n$, clearly C and $C^{\perp}$ are subspaces of $\mathbb{F}_q^n$. Recall that $\dim C = k$ and $\dim C^{\perp} = n - k$. Thus

$$\dim(C \oplus C^{\perp}) = \dim C + \dim C^{\perp} = k + n - k = n = \dim \mathbb{F}_q^n$$

by Theorem 2.2.19. Hence, $\mathbb{F}_q^n = C \oplus C^{\perp}$ by Theorem 2.1.24.

3.1.4 Proposition [17] Let C be a linear code. The orthogonal projector Π_C from $\mathbb{F}_q^n$ onto C such that

$$\mathbf{v}\Pi_C = \begin{cases} \mathbf{v} & \text{if } \mathbf{v} \in C \\ \mathbf{0} & \text{if } \mathbf{v} \in C^{\perp} \end{cases}$$

exists if and only if C is an LCD code.

The following theorem is the most important characterization we have on LCD codes. This theorem allows to prove whether a linear code, given it's generator matrix, is LCD code.

3.1.5 Proposition [17] Let G be a generator matrix for a linear (n, k) code C. C is an LCD code if and only if the $k \times k$ matrix GG^T is nonsingular.

Before we proceed with the proof, we note that the proof of the statement "If GG^T is nonsingular, C is LCD" is a different proof from what is published in [17]. However, the converse is proven the same way as Massey in [17].

Proof. First suppose GG^T is singular, then there exists a nonzero $\mathbf{a} \in \mathbb{F}_q^k$ such that $\mathbf{a}GG^T = \mathbf{0}$. Since $\mathbf{a} \neq \mathbf{0}$ and $G \neq 0$, we have that $\mathbf{a}G \in C$ is also nonzero. Let's define $\mathbf{u} = \mathbf{a}G$. Since G is the generator matrix of C, for any $\mathbf{v} \in C$, $\mathbf{v} = \mathbf{b}G$ for some $\mathbf{b} \in \mathbb{F}_q^k$, so

$$\mathbf{u} \cdot \mathbf{v} = \mathbf{a}G \cdot \mathbf{b}G = \mathbf{a}G(\mathbf{b}G)^T = \mathbf{a}G(G^T\mathbf{b}^T) = (\mathbf{a}GG^T)\mathbf{b}^T = 0.$$

Thus, $u \in C^{\perp}$ as well. So, $C \cap C^{\perp} \neq \{\mathbf{0}\}$, this, C is not an LCD code.

Now, suppose GG^T is nonsingular and assume that C is not an LCD code. Then, there is a nonzero $\mathbf{c} \in C$ such that $\mathbf{c} \in C^\perp$. Since $\mathbf{c} \in C$, there is some vector $\mathbf{a} \in \mathbb{F}_q^k$ such that $\mathbf{c} = \mathbf{a}G$. Since G is the generator matrix for C, it is also the parity-check matrix for $C^\perp$ by Proposition 2.3.6, therefore, $G\boldsymbol{c}^T = \mathbf{0}$, thus,

$$\mathbf{0} = G\boldsymbol{c}^T = G(\boldsymbol{a}G)^T = GG^T\mathbf{a}^T.$$

But, GG^T is nonsingular, so $\mathbf{a}^T = \mathbf{0}$, and further $\mathbf{a} = \mathbf{0}$, indeed $\mathbf{c} = \mathbf{a}G = \mathbf{0}$, a contradiction. So, C is an LCD code. □

3.1.6 Proposition [17] Let C be a linear (n, k) code. If C is an LCD code, then $\Pi_C = G^T(GG^T)^{-1}G$ is the orthogonal projector from $\mathbb{F}_q^n$ onto C.

We omit the proof of this proposition since the proof given in [17] is already the simplest and most efficient way of proving the proposition.

3.2 Classes of LCD Codes

After the characterization of LCD codes, we present classes of LCD codes. The following two classes of LCD codes where the first ones ever proposed by Massey. When they were originally presented, Corollary 3.2.2 was the main result and then Theorem 3.2.1 was only discussed as a generalization of Corollary 3.2.2 to other fields. However, Corollary 3.2.2 naturally follows from Theorem 3.2.1 that we use it as the main theorem.

3.2.1 Theorem [17] Let P be an $k \times (n-k)$ matrix, $G = [I_k|P]$, a generator matrix of an (n, k) linear code C over $\mathbb{F}_p$ for p prime and $\alpha \in \mathbb{F}_p$ such that $\alpha^2 = -1$. Then

$$G' = [I_k|P|\alpha P]$$

is the generator matrix of a $(2n-k, k)$ LCD code C'.

This theorem was not proved in [17]. So we provide a new proof here. This proof is very similar to the proof in [17] of Corollary 3.2.2 with the details added in.

Proof. Let $m = n - k$, $\alpha^2 = -1$, $G = [I_k|P|\alpha P]$ and

$$P = \begin{bmatrix} p_{11} & \cdots & p_{1m} \\ \vdots & \ddots & \vdots \\ p_{k1} & \cdots & p_{km} \end{bmatrix}.$$

Then

$$P^T = \begin{bmatrix} p_{11} & \cdots & p_{k1} \\ \vdots & \ddots & \vdots \\ p_{1m} & \cdots & p_{km} \end{bmatrix}.$$

By Proposition 3.1.3, we must show that GG^T is nonsingular. We will compute the jth row of GG^T. By Definition 2.2.8, the jth column of GG^T is the matrix-vector product of G with the jth column of G^T so,

$$\begin{aligned}
(\mathbf{GG}^T)_j &= G(\mathbf{G}^T)_j \\
&= [I_k|P|\alpha P] \begin{bmatrix} \mathbf{e}_j \\ p_{j1} \\ \vdots \\ p_{jm} \\ \alpha p_{j1} \\ \vdots \\ \alpha p_{jm} \end{bmatrix} \\
&= \mathbf{e}_j + p_{j1}\mathbf{P}_1 + \cdots + p_{jm}\mathbf{P}_m + \alpha p_{j1}\alpha\mathbf{P}_1 + \cdots + \alpha p_{jm}\alpha\mathbf{P}_m \\
&= \mathbf{e}_j + p_{j1}\mathbf{P}_1 + \cdots + p_{jm}\mathbf{P}_m + \alpha^2 p_{j1}\mathbf{P}_1 + \cdots + \alpha^2 p_{jm}\mathbf{P}_m \\
&= \mathbf{e}_j + p_{j1}\mathbf{P}_1 + \alpha^2 p_{j1}\mathbf{P}_1 + \cdots + p_{jm}\mathbf{P}_m + \alpha^2 p_{jm}\mathbf{P}_m \\
&= \mathbf{e}_j + p_{j1}\mathbf{P}_1 - p_{j1}\mathbf{P}_1 + \cdots + p_{jm}\mathbf{P}_m - p_{jm}\mathbf{P}_m \\
&= \mathbf{e}_j.
\end{aligned}$$

Here, the third equality comes from Definition 2.2.7 and the sixth equality comes from the fact that $\alpha^2 = -1$. Since the jth row is some arbitrary we have that

$$GG^T = [\mathbf{e}_1|\cdots|\mathbf{e}_k] = I_k.$$

Since I_k is trivially row equivalent to I_k, GG^T is nonsingular, as required. □

3.2.2 Corollary [17] Let P be an $k \times (n-k)$ matrix, $G = [I_k|P]$, a generator matrix of an (n,k) linear code C over $\mathbb{F}_2$. Then

$$G' = [I_k|P|P]$$

is the generator matrix of a $(2n-k,k)$ LCD code C'.

Proof. Let $\alpha = 1$. Then

$$\alpha^2 = 1^2 = 1 \equiv -1 \pmod 2.$$

Now apply Theorem 3.2.1. □

Now that we have these two theorems, we can extend an (n,k) linear code to a $(2n-1,k)$ LCD code. However, Theorem 3.2.1 and Corollary 3.2.2 are not the only accomplishing such a task. If one permutes the columns of the sub-matrix $[P|P]$ from Corollary 3.2.2, and computes the resulting linear code, it turns out that we also get a $(2n-1,k)$ LCD code. This is the statement of the following theorem.
It should be noted that to the best of the author's knowledge this theorem has not been published in any previous literature on LCD codes and so is a new result.

3.2.3 Theorem Let P be a $k \times m$ matrix for $m = n-k$, $G = [I_k|P]$, a generator matrix of an (n,k) linear code C over $\mathbb{F}_2$, and A the $k \times 2m$ matrix obtained by swapping two columns of the $k \times 2m$ matrix $[P|P]$. Then the matrix

$$G' = [I_k|A]$$

is the generator matrix of a $(2n-k,k)$ LCD code C'.

Proof. The proof will be broken into three cases. In the first case, we will show that the linear code generated by $G' = [I_k|A|P]$ such that A is the matrix P with the ith and jth columns swapped generates an LCD code. In the second case, we will show the case of $G' = [I_k|P|A]$ where A is as defined in the first case. Finally, the third case, we will show the case of $G' = [I_k|A|B]$ where A is the matrix P with the ith column replaced with the jth column of P and B is the matrix P with the jth column replaced with the ith column of P. i.e., $\mathbf{A}_i = \mathbf{A}_j = \mathbf{P}_j$ and $\mathbf{B}_i = \mathbf{B}_j = \mathbf{P}_i$. In each case we will apply Theorem 3.1.5 by proving that $G'G'^T$ is nonsingular.

Case 1. Let $m = n - k$. By Definition 2.2.8, the lth column of $G'G'^T$ is the

matrix-vector product of G' with the lth column of G'^T so,

$$
\begin{aligned}
(\mathbf{G'G'}^T)_j &= G'(\mathbf{G'}^T)_l \\
&= [I_k|A|P] \begin{bmatrix} \mathbf{e}_l \\ p_{l,1} \\ \vdots \\ p_{l,i-1} \\ p_{l,j} \\ p_{l,i+1} \\ \cdots \\ p_{l,j-1} \\ p_{l,i} \\ p_{l,j+1} \\ \cdots \\ p_{l,m} \\ p_{l,1} \\ \cdots \\ p_{l,m} \end{bmatrix} \\
&= \mathbf{e}_l + p_{l,1}\mathbf{A}_1 + \cdots + p_{l,i-1}\mathbf{A}_{i-1} + p_{l,j}\mathbf{A}_i + p_{l,i+1}\mathbf{A}_{i+1} + \cdots \\
&+ p_{l,j-1}\mathbf{A}_{j-1} + p_{l,i}\mathbf{A}_j + p_{l,j+1}\mathbf{A}_{j+1} + \cdots + p_{l,m}\mathbf{A}_m + p_{l,1}\mathbf{P}_1 \\
&+ \cdots + p_{l,m}\mathbf{P}_m \\
&= \mathbf{e}_l + p_{l,1}\mathbf{P}_1 + \cdots + p_{l,i-1}\mathbf{P}_{i-1} + p_{l,j}\mathbf{P}_j + p_{l,i+1}\mathbf{P}_{i+1} + \cdots \\
&+ p_{l,j-1}\mathbf{P}_{j-1} + p_{l,i}\mathbf{P}_i + p_{l,j+1}\mathbf{P}_{j+1} + \cdots + p_{l,m}\mathbf{P}_m + p_{l,1}\mathbf{P}_1 \\
&+ \cdots + p_{l,m}\mathbf{P}_m \\
&= \mathbf{e}_l + 2p_{l,1}\mathbf{P}_1 + \cdots + 2p_{l,m}\mathbf{P}_m \\
&= \mathbf{e}_l.
\end{aligned}
$$

Here, the third equality comes from Definition 2.2.7, the fourth equality comes from the hypothesis, and the fifth comes from commuting the terms. Since $\mathbf{e}_l$

is the lth row of $G'G'^T$, we have that

$$G'G'^T = [\mathbf{e}_1|\cdots|\mathbf{e}_k] = I_k.$$

Since I_k is trivially row equivalent to I_k, $G'G'^T$ is nonsingular, as required.

Case 2. Analogous to Case 1.

Case 3. Again we let $m = n - k$. By Definition 2.2.8, the lth column of

$G'G'^T$ is the matrix-vector product of G' with the lth column of G'^T so,

$$
\begin{aligned}
(\mathbf{G'G'}^T)_l &= G'(\mathbf{G'}^T)_l \\
&= [I_k|A|P] \begin{bmatrix} \mathbf{e}_l \\ p_{l,1} \\ \vdots \\ p_{l,i-1} \\ p_{l,j} \\ p_{l,i+1} \\ \cdots \\ p_{l,m} \\ p_{l,1} \\ \cdots \\ p_{l,j-1} \\ p_{l,i} \\ p_{l,j+1} \\ \cdots \\ p_{l,m} \end{bmatrix} \\
&= \mathbf{e}_l + p_{l,1}\mathbf{A}_1 + \cdots + p_{l,i-1}\mathbf{A}_{i-1} + p_{l,j}\mathbf{A}_i + p_{l,i+1}\mathbf{A}_{i+1} + \cdots \\
&+ p_{l,m}\mathbf{A}_m + p_{l,1}\mathbf{B}_1 + \cdots + p_{l,j-1}\mathbf{B}_{j-1} + p_{l,i}\mathbf{B}_j + p_{l,j+1}\mathbf{B}_{j+1} \\
&+ \cdots + p_{l,m}\mathbf{B}_m \\
&= \mathbf{e}_l + p_{l,1}\mathbf{P}_1 + \cdots + p_{l,i-1}\mathbf{P}_{i-1} + p_{l,j}\mathbf{P}_j + p_{l,i+1}\mathbf{P}_{i+1} + \cdots \\
&+ p_{l,m}\mathbf{P}_m + p_{l,1}\mathbf{P}_1 + \cdots + p_{l,j-1}\mathbf{P}_{j-1} + p_{l,i}\mathbf{P}_i + p_{l,j+1}\mathbf{P}_{j+1} \\
&+ \cdots + p_{l,m}\mathbf{P}_m \\
&= \mathbf{e}_l + 2p_{l,1}\mathbf{P}_1 + \cdots + 2p_{l,m}\mathbf{P}_m \\
&= \mathbf{e}_l.
\end{aligned}
$$

Here, the third equality comes from Definition 2.2.7, the fourth equality comes from the hypothesis, and the fifth comes from commuting the terms. Since $\mathbf{e}_l$

is the lth row of $G'G'^T$, we have that

$$G'G'^T = [\mathbf{e}_1|\cdots|\mathbf{e}_k] = I_k.$$

Since I_k is trivially row equivalent to I_k, $G'G'^T$ is nonsingular, as required. $\square$

Recently, it has been discovered by Sok, Shi, and Sole in [23] that by taking submatrices of orthogonal matrices, we can construct LCD codes. We will only prove the first class of LCD codes.

3.2.4 Theorem [23] Let $A \in \mathcal{O}_n(q)$ and A_k a submatrix obtained from A by keeping any k rows. Then for any $\lambda_1, \ldots, \lambda_k \in \mathbb{F}_q \setminus \{0\}$, the matrix

$$G = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_k \end{bmatrix} A_k$$

generates an LCD code.

Proof. By Proposition 3.1.5, we must prove that GG^T is nonsingular. We

proceed to compute GG^T using Lemma 2.2.15.

$$
\begin{aligned}
GG^T &= \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_k \end{bmatrix} A_k \left(\begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_k \end{bmatrix} A_k \right)^T \\
&= \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_k \end{bmatrix} A_k A_k^T \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_k \end{bmatrix}^T \\
&= \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_k \end{bmatrix} I_k \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_k \end{bmatrix} \\
&= \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_k \end{bmatrix} \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_k \end{bmatrix}^T \\
&= \begin{bmatrix} \lambda_1^2 & 0 & \cdots & 0 \\ 0 & \lambda_2^2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_k^2 \end{bmatrix}
\end{aligned}
$$

If we apply the row operation of multiplying the ith row by $\frac{1}{\lambda_i^2}$ for each $1 \leq i \leq k$, then we obtain the that GG^T is row equivalent to I_k since $\lambda_1, \ldots, \lambda_k$ are all nonzero. Hence, by Theorem 2.2.11, GG^T is nonsingular, as required. □

3.2.5 Theorem [23] Let $A \in \mathcal{O}_n(q)$ and A_k a submatrix obtained from A by keeping any k rows, with k being even. Let $\alpha_i, \beta_i \in \mathbb{F}_q \setminus \{0\}$ for $1 \leq i \leq \frac{k}{2}$

such that $\alpha_i^2 + \beta_i^2 \neq 0$ and

$$D_i = \begin{bmatrix} \alpha_i & \beta_i \\ -\beta_i & \alpha_i \end{bmatrix}.$$

Then for any $\lambda_1, \ldots, \lambda_k \in \mathbb{F}_q \setminus \{0\}$, the matrix

$$G = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_k \end{bmatrix} \begin{bmatrix} D_1 & 0 & \cdots & 0 \\ 0 & D_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & D_{\frac{k}{2}} \end{bmatrix} A_k$$

generates an LCD code. Moreover, if k is odd, the matrix

$$G' = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_k \end{bmatrix} \begin{bmatrix} D_1 & 0 & \cdots & 0 & 0 \\ 0 & D_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & D_{\frac{k}{2}} & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix} A_k$$

generates an LCD code.

3.2.6 Theorem [23] Let C be an (n, k) LCD code over $\mathbb{F}_q$ with its generator matrix G being rows of an orthogonal matrix. Suppose that there exist $a, b \in \mathbb{F}_q \setminus \{0\}$ such that $a^2 + b^2 \equiv 0 \pmod{q}$. Then for any $\lambda_1 \leq \cdots \leq \lambda_n \in \mathbb{F}_q$

$$G' = \begin{bmatrix} & \lambda_1 a & \lambda_1 b \\ & \lambda_2(-b) & \lambda_2 a \\ G & \vdots & \vdots \\ & \lambda_{2i-1} a & \lambda_{2i-1} b \\ & \lambda_{2i}(-b) & \lambda_{2i} a \\ & \vdots & \vdots \end{bmatrix}$$

generates an $(n+2, k)$ LCD code.

3.3 $\mathcal{T}$-Direct Codes

Now we generalize LCD codes. One may notice that Definition 3.3.1 is similar to Definition 3.1.1, Proposition 3.3.2 is similar to Proposition 3.1.4 and Proposition 3.3.3 is similar to Propositions 3.1.5 and 3.1.6.

3.3.1 Definition [25] Let $\Gamma_1, \ldots, \Gamma_{\mathcal{T}}$ be $(n, k_1), \ldots, (n, k_{\mathcal{T}})$ linear codes over $\mathbb{F}_q$ for $k_1 + \cdots + k_{\mathcal{T}} \leq n$ and $\Gamma_i^{\perp}$ the dual code of Γ_i with respect to $\Lambda = \Gamma_1 \oplus \cdots \oplus \Gamma_{\mathcal{T}}$. If $\Gamma_i \cap \Gamma_i^{\perp} = \{\mathbf{0}\}$ for all $1 \leq i \leq \mathcal{T}$, then $(\Gamma_1, \ldots, \Gamma_{\mathcal{T}})$ is a *$\mathcal{T}$-Direct code*. Each Γ_i is a *constituent code*.

3.3.2 Proposition [25] The orthogonal projector Π_{Γ_i} from Λ onto Γ_i such that

$$\mathbf{v}\Pi_{\Gamma_i} = \begin{cases} \mathbf{v} & \text{if } \mathbf{v} \in \Gamma_i \\ \mathbf{0} & \text{if } \mathbf{v} \in \Gamma_i^{\perp} \end{cases}$$

for each $i = 1, \ldots T$ exists if and only if $(\Gamma_1, \ldots, \Gamma_T)$ is a $\mathcal{T}$-Direct code.

Similar to how Proposition 3.1.5 is the most important characterization we have on LCD codes, the following theorem is the most important characterization we have on $\mathcal{T}$-Direct codes and will be used in proving that a set of constituent codes form a $\mathcal{T}$-Direct code.

3.3.3 Proposition [25] Let Γ_i be a (n, k_i) linear code over $\mathbb{F}_q$ the generator matrix G_i such that $G_i G_j^T = 0$ for each $i, j = 1, \ldots, T$ with $i \neq j$. Then $(\Gamma_1, \ldots, \Gamma_T)$ is a $\mathcal{T}$-Direct code if and only if the $k_i \times k_i$ matrix $G_i G_i^T$ is nonsingular for every i. Further, if $(\Gamma_1, \ldots, \Gamma_T)$ is a $\mathcal{T}$-Direct code, then $\Pi_{\Gamma_i} = G_i^T (G_i G_i^T)^{-1} G_i$ is the orthogonal projector from Λ onto Γ_i for each i.

It should be noted that all proofs in this section will be similar from the proofs given by Durai and Devi in [20] and [7] with two differences. First, we will fill in the details that Durai and Devi omit. Finally, with respect to proving that

$G_i G_i^T$ is nonsingular, instead of proving that $G_i G_i^T = I_k$, we will instead show that the determinant of $G_i G_i^T$ is nonzero which is equivalent to proving that it is nonsingular.

Now that we have defined a $\mathcal{T}$-Direct code and have a characterization for such codes, we may now begin to find classes of $\mathcal{T}$-Direct codes. Combining Lemma 3.3.4 with Theorem 3.3.5 gives us an n-Direct code.

3.3.4 Lemma [20] Let $\{\alpha_1, \ldots, \alpha_n\}$ be a trace-orthogonal basis and $(\Gamma_1, \ldots, \Gamma_n)$, an n-Direct code over $\mathbb{F}_{2^n}$ such that Γ_i is a (n, k_i) MRD code generated by

$$G_i = \begin{bmatrix} \alpha_1^{q^{k_1+\cdots+k_{i-1}+1}} & \alpha_2^{q^{k_1+\cdots+k_{i-1}+1}} & \cdots & \alpha_n^{q^{k_1+\cdots+k_{i-1}+1}} \\ \alpha_1^{q^{k_1+\cdots+k_{i-1}+2}} & \alpha_2^{q^{k_1+\cdots+k_{i-1}+2}} & \cdots & \alpha_n^{q^{k_1+\cdots+k_{i-1}+2}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{q^{k_1+\cdots+k_{i-1}+k_i}} & \alpha_2^{q^{k_1+\cdots+k_{i-1}+k_i}} & \cdots & \alpha_n^{q^{k_1+\cdots+k_{i-1}+k_i}} \end{bmatrix}$$

for $k_1 + \cdots + k_n \leq n$. Then $G_i' = G_n \otimes G_i$ defines an $(n^2, k_n k_i)$ code.

Durai does not prove this Lemma in [20], so this is new proof.

Proof. We know that G_i a $k_i \times n$ matrix and G_n is a $k_n \times n$ matrix. Then by Definition 2.2.12, $G_i' = G_n \otimes G_i$ is a $k_n k_i \times n^2$ matrix, so by Definition 2.3.2, G_i' generates an $(n^2, k_n k_i)$ code. □

3.3.5 Theorem [20] Let G_i' be defined as in Lemma 3.3.4 and $\Gamma_1', \ldots, \Gamma_n'$ be $(n^2, k_1 k_n), \ldots, (n^2, k_n k_n)$ codes generated by $G_1', \ldots, G_n'$ respectively. Then $(\Gamma_1', \ldots, \Gamma_n')$ is an n-Direct code.

Proof. By Proposition 3.3.3, we must show that $G_i' G_j'^T = 0$ for $1 \leq i, j \leq n$

when $i \neq j$ and $G'_i G'^T_i$ is nonsingular. Applying Lemma 2.2.13, we get

$$\begin{aligned} G'_i G'^T_j &= (G_n \otimes G_i)(G_n \otimes G_j)^T \\ &= (G_n \otimes G_i)(G_n^T \otimes G_j^T) \\ &= (G_n G_n^T) \otimes (G_i G_j^T) \end{aligned}$$

If $i \neq j$, then since G_i and G_j generate consituent codes of an n-Direct code, $G_i G_j^T = 0$ and hence, $G'_i G'^T_j = 0$.
If $i = j$, then $G'_i G'^T_i = (G_n G_n^T) \otimes (G_i G_i^T)$. Since $G_n G_n^T$ is nonsingular, by Theorem 2.2.11, $\det(G_n G_n^T) \neq 0$. Similarly, $\det(G_i G_i^T) \neq 0$. So by Lemma 2.2.13, $\det(G'_i G'^T_i) \neq 0$ and hence $G'_i G'^T_i$ is nonsingular. □

3.3.6 Theorem [20] Let $(\Gamma'_1, \ldots, \Gamma'_n)$ be an n-Direct code where Γ'_i is an $(n^2, k_i k_n)$ code generated by G'_i as defined in Lemma 3.3.4. The orthogonal projector mapping $\Lambda' = \Gamma'_1 \oplus \cdots \oplus \Gamma'_n$ onto Γ'_i is

$$\Pi_{\Gamma'_i} = (G_n^T G_n) \otimes (G_i^T G_i).$$

Now we have a code that can be used to encode a coding scheme with n users. But suppose we want to be able to accomadate more then n users without having to choose a larger n. The following class of codes takes our current n-Direct code and uses it to create a $(2n-1)$-Direct code. This doubles the number of users ours coding scheme can accomadate.

3.3.7 Theorem [20] Let $\{\alpha_1, \ldots, \alpha_n\}$ be a trace-orthogonal basis in $\mathbb{F}_{2^n}$ and $(\Gamma_1, \ldots, \Gamma_n)$, an n-Direct code where Γ_i is an $(n, 1)$ code generated by

$$G_i = \begin{bmatrix} \alpha_1^{2^i} & \alpha_2^{2^i} & \cdots & \alpha_n^{2^i} \end{bmatrix}.$$

Further let $\mathcal{A}_i = G_n \otimes G_i$ for $1 \leq i \leq n-1$ and $\mathcal{B}_i = G_i \otimes G_i$ for $1 \leq i \leq n$. If $\Gamma'_1, \ldots, \Gamma'_{2n-1}$ are $(n^2, 1)$ codes such that $\Gamma'_1, \ldots, \Gamma'_{n-1}$ is generated by $\mathcal{A}_1, \ldots, \mathcal{A}_{n-1}$, respectively, and $\Gamma'_n, \ldots, \Gamma'_{2n-1}$ is generated by $\mathcal{B}_1, \ldots, \mathcal{B}_n$, respectively, then $(\Gamma'_1, \ldots, \Gamma'_{2n-1})$ is a $(2n-1)$-Direct code.

Proof. By Proposition 3.3.3, we must first show that $\mathcal{A}_i\mathcal{A}_j^T = 0$ for $1 \leq i, j \leq n-1$ and $\mathcal{B}_i\mathcal{B}_j^T = 0$ for $1 \leq i, j \leq n$ when $i \neq j$ and nonsingular when $i = j$. We must also show that $\mathcal{A}_i\mathcal{B}_j^T = 0$ for $1 \leq i \leq n-1$ and $1 \leq j \leq n$. First we consider $\mathcal{A}_i\mathcal{A}_j^T$. Applying Lemma 2.2.13, we get

$$\begin{aligned} \mathcal{A}_i\mathcal{A}_j^T &= (G_n \otimes G_i)(G_n \otimes G_j)^T \\ &= (G_n \otimes G_i)(G_n^T \otimes G_j^T) \\ &= (G_nG_n^T) \otimes (G_iG_j^T) \end{aligned}$$

If $i \neq j$, then since G_i and G_j generate consituent codes of an n-Direct code, by Proposition 3.3.3, $G_iG_j^T = 0$ and hence, $\mathcal{A}_i\mathcal{A})_j^T = 0$.

If $i = j$, then $\mathcal{A}_i\mathcal{A}_j^T = (G_nG_n^T) \otimes (G_iG_i^T)$. Since $G_nG_n^T$ is nonsingular, by Theorem 2.2.11, $\det(G_nG_n^T) \neq 0$. Similarly, $\det(G_iG_i^T) \neq 0$. So by Lemma 2.2.13, $\det(\mathcal{A}_i\mathcal{A}_i^T) \neq 0$ and hence $\mathcal{A}_i\mathcal{A}_i^T$ is nonsingular.

Now we consider $\mathcal{B}_i\mathcal{B}_j^T$. Again applying Lemma 2.2.13, we get

$$\begin{aligned} \mathcal{B}_i\mathcal{B}_j^T &= (G_i \otimes G_i)(G_j \otimes G_j)^T \\ &= (G_i \otimes G_i)(G_j^T \otimes G_j^T) \\ &= (G_iG_j^T) \otimes (G_iG_j^T) \end{aligned}$$

If $i \neq j$, then since G_i and G_j generate consituent codes of an n-Direct code, by Proposition 3.3.3, $G_iG_j^T = 0$ and hence, $\mathcal{B}_i\mathcal{B}_j^T = 0$.

If $i = j$, then $\mathcal{B}_i\mathcal{B}_j^T = (G_iG_i^T) \otimes (G_iG_i^T)$. Since $G_iG_i^T$ is nonsingular, by Theorem 2.2.11, $\det(G_iG_i^T) \neq 0$. So by Lemma 2.2.13, $\det(\mathcal{B}_i\mathcal{B}_i^T) \neq 0$ and hence $\mathcal{B}_i\mathcal{B}_i^T$ is nonsingular.

Finally, using Lemma 2.2.11, we get

$$\begin{aligned} \mathcal{A}_i\mathcal{B}_j^T &= (G_n \otimes G_i)(G_j \otimes G_j)^T \\ &= (G_n \otimes G_i)(G_j^T \otimes G_j^T) \\ &= (G_nG_j^T) \otimes (G_iG_j^T) \end{aligned}$$

If $i \neq j$, then since G_n and G_j generate consituent codes of an n-Direct code, by Proposition 3.3.3, $G_nG_j^T = 0$ and hence, $\mathcal{A}_i\mathcal{B}_j^T = 0$. □

Now that we can encode a coding scheme with $2n-1$ users, we can actually do a little bit better.

3.3.8 Theorem [7] Let $\{\alpha_1, \ldots, \alpha_n\}$ be a trace-orthogonal basis in $\mathbb{F}_{2^n}$ and $(\Gamma_1, \ldots, \Gamma_n)$, an n-Direct code where Γ_i is an $(n, 1)$ MRD code generated by

$$G_i = \begin{bmatrix} \alpha_1^{2^i} & \alpha_2^{2^i} & \cdots & \alpha_n^{2^i} \end{bmatrix}.$$

Further, let $i, j, k \in \{1, \ldots, n\}$. If Γ'_{ijk} are $(n^3, 1)$ codes generated by

$$\mathcal{G}_{ijk} = G_i \otimes G_j \otimes G_k,$$

then $(\Gamma'_{ijk})_{i,j,k=1}^{n}$ is an n^3-Direct code.

Proof. Since $(\Gamma_1, \ldots, \Gamma_n)$ is an n-Direct code where each Γ_i is generated by

$$G_i = \begin{bmatrix} \alpha_1^{2^i} & \alpha_2^{2^i} & \cdots & \alpha_n^{2^i} \end{bmatrix}.$$

for $1 \leq i \leq n$, $G_i G_j^T = 0$ for $1 \leq j \leq n$ and $i \neq j$, and $G_i G_i^T$ is nonsingular for each i, by Proposition 3.3.3. To show that $(\Gamma'_{ijk})_{i,j,k=1}^{n}$ is an n^3-Direct code, we must show that for each $\mathcal{G}_{ijk}\mathcal{G}_{rst}^T = 0$ whenever $(i, j, k) \neq (r, s, t)$ and $\mathcal{G}_{ijk}\mathcal{G}_{rst}^T$ is nonsingular otherwise. Applying Lemma 2.2.13, we get

$$\begin{aligned} \mathcal{G}_{ijk}\mathcal{G}_{rst}^T &= (G_i \otimes G_j \otimes G_k)(G_r \otimes G_s \otimes G_t)^T \\ &= (G_i \otimes G_j \otimes G_k)(G_r^T \otimes G_s^T \otimes G_t^T) \\ &= (G_i G_r^T) \otimes (G_j G_s^T) \otimes (G_k G_t^T) \end{aligned}$$

If $(i, j, k) \neq (r, s, t)$, then either $i \neq r$, $j \neq s$, or $k \neq t$. In either case one of $(G_i G_r^T)$, $(G_j G_s^T)$, or $(G_k G_t^T)$ is zero, hence, $\mathcal{G}_{ijk}\mathcal{G}_{rst}^T = 0$.
Now suppose $(i, j, k) = (r, s, t)$. Then $i = r$, $j = s$, $k = t$. So $\mathcal{G}_{ijk}\mathcal{G}_{rst}^T = (G_i G_i^T) \otimes (G_j G_j^T) \otimes (G_k G_k^T)$. By Proposition 3.3.3, $G_i G_i^T$, $G_j G_j^T$, and $G_k G_k^T$ are all nonsingular. Hence $\det(G_i G_i^T) \neq 0$, $\det(G_j G_j^T) \neq 0$ and $\det(G_k G_k^T) \neq 0$. Thus, by multiple applications of Lemma 2.2.13, we have that $\det(\mathcal{G}_{ijk}\mathcal{G}_{rst}^T) \neq 0$.

Thus, by Theorem 2.2.11. $\mathcal{G}_{ijk}\mathcal{G}_{rst}^T$ is nonsingular. Thus $(\Gamma'_{ijk})_{i,j,k=1}^n$ is an n^3-Direct code. $\square$

Now we can encode a coding environment for n^3 users. However, if we modify the design we have for n^3-Direct codes, we create a Direct code with even more constituent codes.

3.3.9 Theorem [7] Let $\{\alpha_1, \ldots, \alpha_n\}$ be a trace-orthogonal basis in $\mathbb{F}_{2^n}$ and $(\Gamma_1, \ldots, \Gamma_n)$, an n-Direct code where Γ_i is an $(n, 1)$ MRD code generated by

$$G_i = \left[\alpha_1^{2^i} \quad \alpha_2^{2^i} \quad \cdots \quad \alpha_n^{2^i}\right].$$

Further, let $i_1, \ldots, i_n \in \{1, \ldots, n\}$. If $\Gamma'_{i_1 i_2 \cdots i_n}$ are $(n^n, 1)$ codes generated by

$$\mathcal{G}_{i_1 i_2 \cdots i_n} = G_{i_1} \otimes \cdots \otimes G_{i_n},$$

then $(\Gamma'_{i_1 i_2 \cdots i_n})_{i_1,\ldots,i_n=1}^n$ is an n^n-Direct code.

Proof. Since $(\Gamma_1, \ldots, \Gamma_n)$ is an n-Direct code where each Γ_i is generated by

$$G_i = \left[\alpha_1^{2^i} \quad \alpha_2^{2^i} \quad \cdots \quad \alpha_n^{2^i}\right].$$

for $1 \leq i \leq n$, $G_i G_j^T = 0$ for $1 \leq j \leq n$ and $i \neq j$, and $G_i G_i^T$ is nonsingular for each i, by Proposition 3.3.3. To show that $(\Gamma'_{i_1 i_2 \cdots i_n})_{i_1 i_2 \cdots i_n=1}^n$ is an n^n-Direct code, we must show that $\mathcal{G}_{i_1 \cdots i_n}\mathcal{G}_{j_1 \cdots j_n}^T = 0$ whenever $(i_1, \ldots i_n) \neq (j_1, \ldots, j_n)$ and $\mathcal{G}_{i_1 \cdots i_n}\mathcal{G}_{j_1 \cdots j_n}^T$ is nonsingular otherwise. Applying Lemma 2.2.13, we get

$$\begin{aligned}
\mathcal{G}_{i_1 \cdots i_n}\mathcal{G}_{j_1 \cdots j_n}^T &= (G_{i_1} \otimes \cdots \otimes G_{i_n})(G_{j_1} \otimes \cdots \otimes G_{i_n})^T \\
&= (G_{i_1} \otimes \cdots \otimes G_{i_n})(G_{j_1}^T \otimes \cdots \otimes G_{j_n}^T) \\
&= (G_{i_1} G_{j_1}^T) \otimes \cdots \otimes (G_{i_n} G_{j_n}^T).
\end{aligned}$$

If $(i_1, \ldots, i_n) \neq (j_1, \ldots, j_n)$, then either there exists some $1 \leq k \leq n$ such that $i_k \neq j_k$ and thus for such k, $G_{i_k} G_{j_k}^T = 0$. Hence, $\mathcal{G}_{i_1 \cdots i_n}\mathcal{G}_{j_1 \cdots j_n}^T = 0$.
Now suppose $(i_1, \ldots, i_n) = (j_1, \ldots, j_n)$. Then $i_k = j_k$ for all $1 \leq k \leq n$. So

$\mathcal{G}_{i_1\cdots i_n}\mathcal{G}^T_{j_1\cdots j_n} = (G_{i_1}G^T_{i_1})\otimes\cdots\otimes(G_{i_n}G^T_{i_n})$. By Proposition 3.3.3, each $G_{i_k}G^T_{i_k}$ for $1 \leq k \leq n$ is nonsingular. Hence, by Theorem 2.2.11, for each k, $\det(G_{i_k}G^T_{i_k}) \neq 0$. And so, by multiple applications of Lemma 2.2.13, $\det(\mathcal{G}_{i_1\cdots i_n}\mathcal{G}^T_{j_1\cdots j_n}) \neq 0$. Hence, $\mathcal{G}_{i_1\cdots i_n}\mathcal{G}^T_{j_1\cdots j_n}$ is nonsingular. Thus $(\Gamma'_{i_1\cdots i_n})^n_{i_1,\ldots,i_n=1}$ is an n^n-Direct code. □

From Theorem 3.3.8, we have a method for generating an n^3-Direct code and from Theorem 3.3.9, we have a method for generating an n^n-Direct code. A natural question that is omitted from [7] is whether or not we can create an n^4-Direct code, an n^5-Direct code, ..., an n^{n-1}-Direct code. The following is a new theorem that to the author's knowledge is not published in any literature on $\mathcal{T}$-Direct codes, and answers that question.

3.3.10 Theorem Let $\{\alpha_1, \ldots, \alpha_n\}$ be a trace-orthogonal basis in $\mathbb{F}_{2^n}$ and $(\Gamma_1, \ldots, \Gamma_n)$, an n-Direct code where Γ_i is an $(n, 1)$ MRD code generated by

$$G_i = \begin{bmatrix} \alpha_1^{2^i} & \alpha_2^{2^i} & \cdots & \alpha_n^{2^i} \end{bmatrix}.$$

Further, let $i_1, \ldots, i_k \in \{1, \ldots, n\}$ for $2 \leq k \leq n$. If $\Gamma'_{i_1\cdots i_k}$ are $(n^k, 1)$ codes generated by

$$\mathcal{G}_{i_1\cdots i_k} = G_{i_1} \otimes \cdots \otimes G_{i_k},$$

then $(\Gamma'_{i_1 i_2\cdots i_k})^n_{i_1,\ldots,i_k=1}$ is an n^k-Direct code.

Proof. Since $(\Gamma_1, \ldots, \Gamma_n)$ is an n-Direct code where each Γ_i is generated by

$$G_i = \begin{bmatrix} \alpha_1^{2^i} & \alpha_2^{2^i} & \cdots & \alpha_n^{2^i} \end{bmatrix}.$$

for $1 \leq i \leq n$, $G_iG^T_j = 0$ for $1 \leq j \leq n$ and $i \neq j$, and $G_iG^T_i$ is nonsingular for each i, by Proposition 3.3.3. To show that $(\Gamma'_{i_1 i_2\cdots i_k})^n_{i_1 i_2\cdots i_k=1}$ is an n^k-Direct code, we must show that $\mathcal{G}_{i_1\cdots i_k}\mathcal{G}^T_{j_1\cdots j_k} = 0$ whenever $(i_1, \ldots i_k) \neq (j_1, \ldots, j_k)$

and $\mathcal{G}_{i_1\cdots i_k}\mathcal{G}^T_{j_1\cdots j_k}$ is nonsingular otherwise. Applying Lemma 2.2.13, we get

$$\begin{aligned}\mathcal{G}_{i_1\cdots i_k}\mathcal{G}^T_{j_1\cdots j_k} &= (G_{i_1}\otimes\cdots\otimes G_{i_k})(G_{j_1}\otimes\cdots\otimes G_{i_k})^T\\ &= (G_{i_1}\otimes\cdots\otimes G_{i_k})(G^T_{j_1}\otimes\cdots\otimes G^T_{j_k})\\ &= (G_{i_1}G^T_{j_1})\otimes\cdots\otimes(G_{i_k}G^T_{j_k}).\end{aligned}$$

If $(i_1,\ldots,i_k)\neq(j_1,\ldots,j_k)$, then either there exists some $1\leq l\leq k$ such that $i_l\neq j_l$ and for such l, $G_{i_l}G^T_{j_l}=0$. Hence, $\mathcal{G}_{i_1\cdots i_k}\mathcal{G}^T_{j_1\cdots j_k}=0$.
Now suppose $(i_1,\ldots,i_k)=(j_1,\ldots,j_k)$. Then $i_l=j_l$ for all $1\leq l\leq k$. So $\mathcal{G}_{i_1\cdots i_k}\mathcal{G}^T_{j_1\cdots j_k}=(G_{i_1}G^T_{i_1})\otimes\cdots\otimes(G_{i_k}G^T_{i_k})$. By Proposition 3.3.3, for each $i\leq l\leq k$, $G_{i_l}G^T_{i_l}$ is nonsigular. Thus, by Theorem 2.2.11, for each l, $\det(G_{i_l}G^T_{i_l})\neq 0$. Hence, by multiple applications of Lemma 2.2.13, $\det(\mathcal{G}_{i_1\cdots i_k}\mathcal{G}^T_{j_1\cdots j_k})\neq 0$. Therefore, $\mathcal{G}_{i_1\cdots i_k}\mathcal{G}^T_{j_1\cdots j_k}$ is nonsingular, and so, $(\Gamma'_{i_1\cdots i_k})^n_{i_1,\ldots,i_k=1}$ is an n^k-Direct code. □

As a consequence of the previous theorem, we can generate an n^2-Direct code as follows.

3.3.11 Corollary Let $\{\alpha_1,\ldots,\alpha_n\}$ be a trace orthogonal basis in $\mathbb{F}_{2^n}$ and $(\Gamma_1,\ldots,\Gamma_n)$, an n-Direct code where Γ_i is an $(n,1)$ MRD code generated by

$$G_i=\begin{bmatrix}\alpha_1^{2^i} & \alpha_2^{2^i} & \cdots & \alpha_n^{2^i}\end{bmatrix}.$$

Further, let $i,j\in\{1,\ldots,n\}$. If Γ'_{ij} are $(n^2,1)$ codes generated by

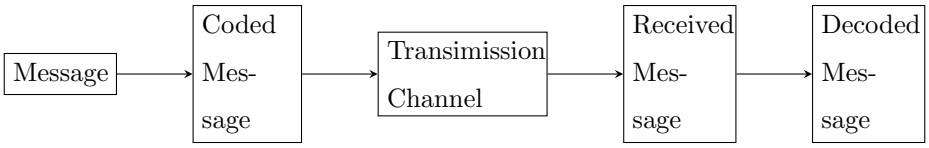
$$\mathcal{G}_{ij}=G_i\otimes G_j,$$

then $(\Gamma'_{ij})^n_{i,j=1}$ is an n^2-Direct code.

Proof of this corollary will be omitted since the result is immediate from Theorem 3.3.10.

4 Applications

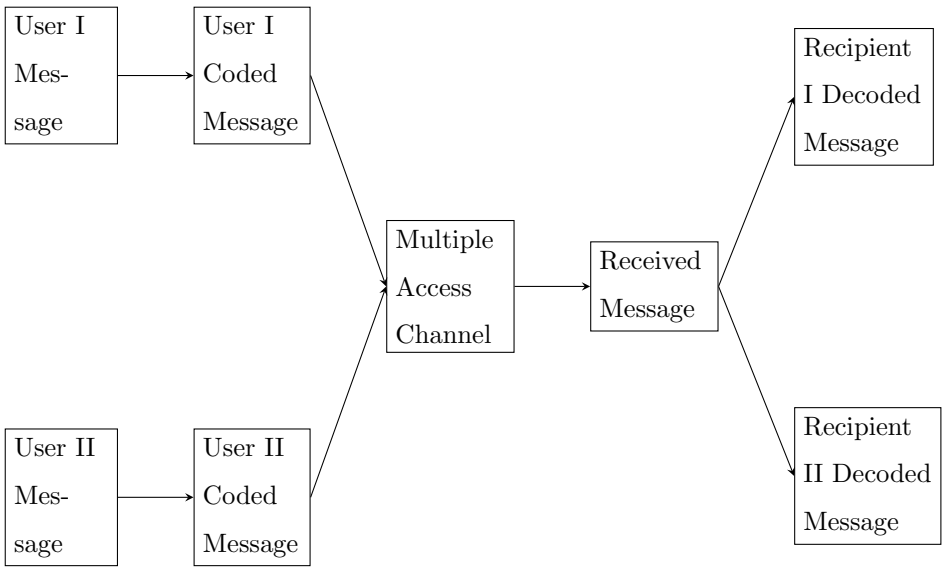
Most coding schemes require encoding information through a device such that there is one sender and one receiver. Such a device can be a CD, a satellite, a camera, etc. In each case some information is encoded into the device and then as it passes through the transmission channel it is decoded and the receiver can then listen, watch, or view the information. Mathematically speaking, the user sends a message $\mathbf{a} \in \mathbb{F}_q^k$. This message gets encoded using a function $f : \mathbb{F}_q^k \to \mathbb{F}_q^n$ which maps $\mathbf{a} \in \mathbb{F}_q^k$ to $\mathbf{c} \in \mathbb{F}_q^n$ with $k \leq n$. In this case, $\mathbf{c}$ is going to be a codeword in some code C. Once the message is encoded it is send to the recipient through the transmission channel and received as a word that may or may not contain an error. This word is then decoded using a function $g : \mathbb{F}_q^n \to \mathbb{F}_q^k$. This scenario which is descrbed in further detail in [16], is illustrated below.



In the decoding process we are concerned with being able to detect and correct any errors that may have occured in transmission. In the single user case, as long as the received message contains less errors than what the code can correct, the receiver will receive the information without any errors.

A natural extension would be to consider a case where there are two senders and two receivers which is discussed in [10]. Let $k \leq n$ and suppose we have two users that send a message through the same channel. Both senders send a message in $\mathbb{F}_q^k$. The first sender uses the code $C_1 \subseteq \mathbb{F}_q^n$ to encode their message and the second sender uses the code $C_2 \subseteq \mathbb{F}_q^n$ to encode their message and both messages get sent through the same communication channel. Once the two messages have passed through the channel they will be decoded so that the first recipient receives the message sent by the first sender and the second recipient

receives the message received by the second sender. This scenario is illustrated below.



As with the single user case, we need to ensure that the received information contains fewer errors than what each code can correct. However, we also need to ensure the received information can be decoded in one unique way.

4.1 Definition [10] Let $\mathbf{u}, \mathbf{v} \in \mathbb{F}_2^n$, further let $E : \mathbb{F}_2^n \to \{0, 1, \xi\}^n$, $E_1, \ldots, E_n : \mathbb{F}_2 \to \{0, 1, \xi\}$ and define

$$E(\mathbf{u}, \mathbf{v}) = (E_1(u_1, v_1), E_2(u_2, v_2), \ldots, E_n(u_n, v_n))$$

where

$$\begin{cases} E_i(u_i, v_i) = u_i = v_i & u_i = v_i, \\ E_i(u_i, v_i) = \xi & u_i \neq v_i. \end{cases}$$

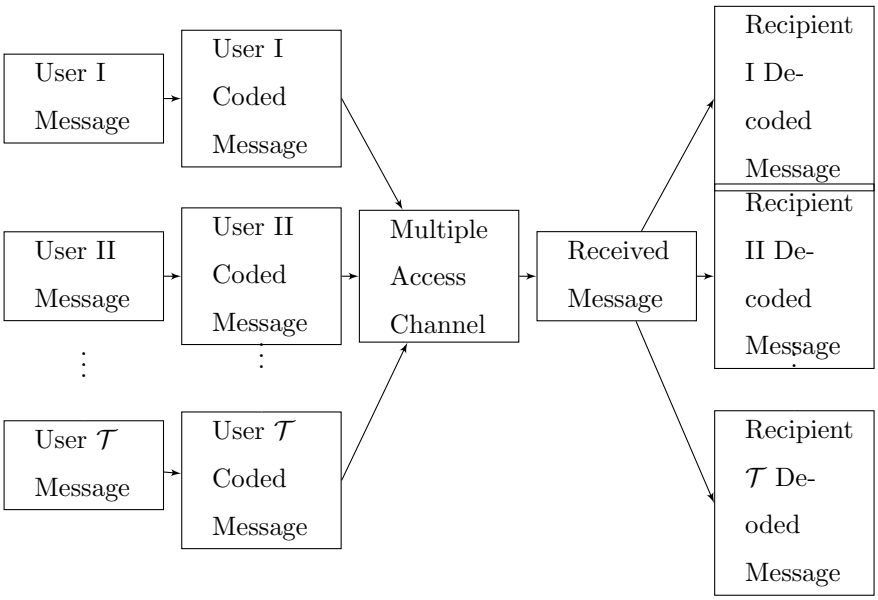
Suppose $C_1 \subseteq \mathbb{F}_2^n$ and $C_2 \subseteq \mathbb{F}_2^n$. Then (C_1, C_2) is *uniquely decodable* if and only if for any $(\mathbf{u}, \mathbf{v}), (\mathbf{u'}, \mathbf{v'}) \in C_1 \times C_2$ with $(\mathbf{u}, \mathbf{v}) \neq (\mathbf{u'}, \mathbf{v'})$, it is the case that $E(\mathbf{u}, \mathbf{v}) \neq E(\mathbf{u'}, \mathbf{v'})$.

The next proof is different then the one given by Massey.

4.2 Theorem [17] Let $C \subseteq \mathbb{F}_2^n$ be an LCD code. $(C, C^\perp)$ is uniquely decodable.

Proof. Let C be an LCD code, $\mathbf{u}, \mathbf{u'} \in C$ and $\mathbf{v}, \mathbf{v'} \in C^\perp$ such that $\mathbf{u} \neq \mathbf{u'}$ and $\mathbf{v} \neq \mathbf{v'}$. We must show that $E(\mathbf{u}, \mathbf{v}) \neq E(\mathbf{u'}, \mathbf{v'})$. By construction, $E_i(u_i, v_i) = u_i$ if $u_i = v_i$ and $E_i(u_i, v_i) = \xi$ if $u_i \neq v_i$. If $u_i = v_i$, then $u_i - v_i = 0$. Similarly if $u_i \neq v_i$, then $u_i - v_i = 1$ since $u_i, v_i \in \mathbb{F}_2$. It should be noted that if $\mathbf{u} - \mathbf{v} \neq \mathbf{u'} - \mathbf{v'}$, then $E(\mathbf{u}, \mathbf{v}) \neq E(\mathbf{u'}, \mathbf{v'})$ because if $\mathbf{u} - \mathbf{v} \neq \mathbf{u'} - \mathbf{v'}$ WLOG, there exists some j for $1 \leq j \leq n$ such that $u_j - v_j = 0$ and $u' - v' = 1$. In this case, $E_j(u_j, v_j) = 0$ or 1 and $E_j(u'_j, v'_j) = \xi$, so clearly, $E(\mathbf{u}, \mathbf{v}) \neq E(\mathbf{u'}, \mathbf{v'})$. Therefore, we must show that $\mathbf{u} - \mathbf{v} \neq \mathbf{u'} - \mathbf{v'}$. Since we are in $\mathbb{F}_2^n$, $\mathbf{u} - \mathbf{v} = \mathbf{u} + \mathbf{v}$ and similarly, $\mathbf{u'} - \mathbf{v'} = \mathbf{u'} + \mathbf{v'}$. Further, by Proposition 3.1.3, $\mathbb{F}_2^n = C \oplus C^\perp$, so each $\mathbf{x} \in \mathbb{F}_2^n$ there exists a unique, $\mathbf{y} \in C$ and $\mathbf{z} \in C^\perp$ such that $\mathbf{x} = \mathbf{y} + \mathbf{z}$. Since $(\mathbf{u}, \mathbf{v}) \neq (\mathbf{u'}, \mathbf{v'})$ either $\mathbf{u} \neq \mathbf{u'}$ or $\mathbf{v} \neq \mathbf{v'}$, hence, $\mathbf{u} + \mathbf{v} \neq \mathbf{u'} + \mathbf{v'}$. And so $E(\mathbf{u}, \mathbf{v}) \neq E(\mathbf{u'}, \mathbf{v'})$. Thus, $(C, C^\perp)$ is uniquely decodable. □

However we can extend this even further to a case with $\mathcal{T}$ senders and $\mathcal{T}$ receivers which is discussed in [5]. Let $k \leq n$ and suppose we have two users that send a message through the same channel. All senders send a message from $\mathbb{F}_q^k$. The first sender uses the code $C_1 \subseteq \mathbb{F}_q^n$ to encode their message and the second sender uses the code $C_2 \subseteq \mathbb{F}_q^n$ to encode their message and so on until the $\mathcal{T}$th sender uses the code $C_\mathcal{T}$ to encode their message. All $\mathcal{T}$ messages get sent through the same communication channel. Once the all the messages have passed through the channel it will be decoded so that the first recipient receives the message sent by the first sender and the second recipient receives the message received by the second sender, and so on until the $\mathcal{T}$th recipient receives the message sent by the $\mathcal{T}$th sender. This scenario is illustrated below.



4.3 Definition [5] Let $(C_1, \ldots, C_T)$ be code with T constituent codes. Then the code $(C_1, \ldots, C_T)$ is *uniquely decodable* if all sums consisting of one codeword from each constituent code are distinct.

4.4 Theorem [25] Let $(\Gamma_1, \ldots, \Gamma_\mathcal{T})$ be a $\mathcal{T}$-Direct code over $\mathbb{F}_2$. Then the code $(\Gamma_1, \ldots, \Gamma_\mathcal{T})$ is uniquely decodable.

It should be noted that the proof given for this theorem is different then that of Vasantha and Raja Durai.

Proof.

Suppose $(\Gamma_1, \ldots, \Gamma_\mathcal{T})$ is a $\mathcal{T}$-Direct code. By Definition 3.3.1, $\Lambda = \Gamma_1 \otimes \cdots \otimes \Gamma_\mathcal{T} \subseteq \mathbb{F}_2^n$. Since Λ is a direct product, by Definition 2.2.17, each sum consisting of one codeword from each constituent code are distinct. Hence, $(\Gamma_1, \ldots, \Gamma_\mathcal{T})$ is uniquely decodable. □

5 Conclusion

In this project we have defined LCD codes and $\mathcal{T}$-Direct codes as well as giving a complete characterization of these families of codes. Next, we presented constructions of LCD codes over $\mathbb{F}_q$ and of $\mathcal{T}$-Direct codes over $\mathbb{F}_{2^n}$ including a new class of each. The first few constructions of LCD codes were constructed by adjoining smaller matrices to the generating matrix of a linear code, not necessarily LCD. The final constructions of LCD codes were constructed from orthogonal matrices. The $\mathcal{T}$-Direct codes, on the other hand, were constructed by taking the Kronecker product of generating matrices of MRD codes. Finally, we have shown applications of each to noiseless multiple-user access channels. Going forward, the goal is to construct $\mathcal{T}$-Direct codes over any finite field, not only those of characteristic 2, and to find constructions of $\mathcal{T}$-Direct codes without deriving them from MRD code. Also, it is the intention of the author to find ways of encoding the noisy multiple-user access channels and two-way multiple-user access channels.

References

[1] S. Axler, *Linear Algebra Done Right*. Springer, 3rd edition, 2015.

[2] R. Beezer, *A First Course in Linear Algebra*. http://linear.ups.edu/html/fcla.html (Retrieved July 4, 2019).

[3] C. Carlet, S. Mesnager, C. Tang, Y. Qi. *Euclidean and Hermitian LCD MDS codes*. Designs, Codes and Cryptography, 86 (2018), 2605-2618.

[4] C. Carlet, S. Guilley. *Complementary Dual Codes for Counter-Measures to Side-Channel Attacks*. https://eprint.iacr.org/2015/603.pdf (Retrieved July 4, 2019).

[5] S. Chang, E.J. Weldon Jr., *Coding for T-User Multiple-Access Channels*. IEEE Transactions on Information Theory, 25 (1979), 684-691.

[6] B. Chen, H .Liu, *New Constructions of MDS Codes With Complementary Duals*. IEEE Transactions on Information Theory, 64 (2018) 5776-5782.

[7] M. Devi, R.S. Raja Durai, H. Xu, *Design of $\mathcal{T}$-Direct codes over $GF(2^{\mathcal{N}})$ with increased users*. Finite Fields and Their Applications, 55 (2019), 202-215.

[8] J. Gallian, *Comtemporary Abstract Algebra*. Cengage Learning, 9th edition, 2017.

[9] L. Jin, *Construction of MDS Codes With Complementary Duals*. IEEE Transactions on Information Theory, 63 (2017) 2843-2847.

[10] T. Kasami, S. Lin, *Coding for Multiple-Access Channel*. IEEE Transactions on Information Theory, IT-22 (2) (1976) 129-137.

[11] A. Laub, *Matrix Analysis for Scientists and Engineers*. Society for Industrial and Applied Mathematics, 2005.

[12] A. Lempel, *Matrix Factorization over $GF(2)$ and Trace-Orthogonal Bases of $GF(2^n)$*. SIAM Journal on Computing, 4 (1975) 175-186.

[13] C. Li, C. Ding, S. Li, *LCD Cyclic Codes Over Finite Fields*. IEEE Transactions on Information Theory, 63 (2017) 4344-4356.

[14] X. Liu, Y. Fan, H. Liu, *Galois LCD codes over finite fields*. Finite Fields and Their Applications, 49 (2018) 227-242.

[15] X. Liu, H. Liu, *Matrix-product complementary dual codes*. https://arxiv.org/pdf/1604.03774.pdf (Retrieved July 4, 2019)

[16] R. Lidl, H. Niederreiter, *Introduction to Finite fields and their Applications*. Cambridge University Press, 2nd edition, 1994.

[17] J.L. Massey, *Linear codes with complementary duals*. Discrete Mathematics, 106-107 (1992) 337-342.

[18] J.L. Massey, W. Yang, *The condition for a cyclic code to have a complementary dual*. Discrete Mathematics, 126 (1994) 391-393.

[19] F.J. MacWilliams, N.J.A Sloane, *The Theory of Error-Correcting Codes*. Elsevier B.V., 1st edition, 1977.

[20] R.S. Raja Durai, M. Devi, *Construction of ($\mathcal{N}$ + $\mathcal{M}$)-Direct codes in $GF(2^{\mathcal{N}})$*. in: Proceedings of the 2011 World Congress on Information and Communication Technologies, Mumbai (India), 2011, pp. 766-771.

[21] J. Rotman, *An Introduction to the Theory of Groups*. Springer-Verlag, 4th edition, 1995.

[22] N. Sendrier, *Linear codes with complementary duals meet the Gilbert-Varshamov bound*. Discrete Mathematics, 285 (2004) 345-347.

[23] M. Shi, L. Sok, P. Solé, *Construction of optimal LCD codes over large finite fields*. Finite Fields and Their Applications, 50 (2018) 138-153.

[24] J.H. van Lint, *Introduction to Coding Theory*. Springer-Verlag, 2nd edition, 1992.

[25] W.B. Vasantha, R.S. Raja Durai *T-Direct Codes: An Application to T-user BAC*. in: Proceedings of the 2002 IEEE Information Theory Workshop, Bangalore (India), 2002, pp. 214.