*Manila Journal of Science 9 (2016), pp. 67-82*

# On the Construction of Some LCD Codes over Finite Fields

Eusebio R. Lina, Jr.*, Ederlina G. Nocon
Mathematics Department, De La Salle University, 2401 Taft Avenue, Manila 0922, Philippines

(*Corresponding Author) Email: eusebio_lina@dlsu.edu.ph

## ABSTRACT

Linear codes with complementary duals (LCD codes) are linear codes that intersect with their duals trivially. In this paper, we construct some families of LCD codes using Massey's characterization of an LCD code. In particular, we obtain some classes of binary LCD codes using the permutation matrix and the all-one matrix. We also explicitly construct generator matrices of LCD codes using the generator matrices of self-dual codes and binary Hamming codes. For $3 \leq r \leq 7,$ the binary LCD codes obtained using the Hamming matrix $H_r$ are optimal. We also consider some known methods of combining two or more codes such as the direct product, direct sum, and Plotkin sum. We show that the direct product and the direct sum of two LCD codes are also LCD. We also prove that the permutation equivalence of codes preserves the LCD-ness of linear codes.

**Keywords:** LCD codes, complementary dual codes, construction of LCD codes, binary LCD codes, LCD codes from known linear codes

## 1. INTRODUCTION

Error-correcting codes play an important role in digital communication. All real systems that work with digitally represented data, such as CD players, TVs, fax machines, the internet, satellites, and mobile phones, require the use of error-correcting codes. Among all types of codes, linear codes are studied the most. Because of their algebraic structure, they are easier to describe, encode, and decode than nonlinear codes. In this paper, we study a subclass of linear codes known as LCD codes. Massey (1992) defined a linear code with complementary dual (LCD code) to be a linear code $C$ such that $C \cap C^{\perp} = \{0\}$. These codes have practical utility since they provide an optimum linear coding solution for a two-user binary adder channel. They also play an important role in counter measures to passive and active side-channel analyses on embedded cryptosystems (Carlet & Guilley, 2015).

Massey (1992) pointed out that the class of LCD codes is rich enough to contain asymptotically good codes. Sendrier (2004) confirmed this by showing that LCD codes meet the Gilbert-Varshamov bound.

Dougherty et al. (2015) derived a linear programming bound on the largest size of an LCD code of given length and minimum distance. In the same paper, some combinatorial relations on the parameters of LCD codes were introduced. Some methods of constructing LCD codes were also given in Dougherty et al. (2015). Yang and Massey (1994) gave a necessary and sufficient condition for a cyclic code to have a complementary dual. Esmaeli and Yari (2009) derived necessary and sufficient conditions for some classes of quasi-cyclic codes to be LCD codes. Recently, LCD codes over finite chain rings were studied in Liu and Liu (2015).

In this paper, we construct LCD codes by applying Massey's characterization of LCD codes. This is organized in the following way. Section 2 collects the background material that we need. Section 3 contains the result that the permutation equivalence of linear codes preserves the property of being LCD. Section 4 provides the construction of LCD codes using special types of matrices while Section 5 discusses construction of LCD codes using generator matrices of self-dual codes and binary Hamming codes. Section 6 recalls some classic ways of combining two linear codes and examines whether these constructions involving LCD codes will give rise to new LCD codes.

## 2. PRELIMINARIES

Let $F_q$ be a finite field of order $q$. For a positive integer $n$, let $F_q^n$ denote the vector space of all $n$-tuples over $F_q$. A *linear code* $C$ of length $n$ and dimension $k$ over $F_q$ is a $k$-dimensional subspace of the vector space $F_q^n$. The code $C$ is called an $[n, k]$ linear code over $F_q$.

Let $x = (x_1, x_2, ..., x_n)$ and $y = (y_1, y_2, ..., y_n)$ be vectors in $F_q^n$. The *(Hamming) distance, d(x,y)*, between $x$ and $y$ is the number of coordinates in which the vectors $x$ and $y$ differ, i.e.,

$$d(x, y) = \left|\{i \mid x_i \neq y_i\}\right|.$$

The *(Hamming) weight, wt(x)*, of a vector $x$ is the number of nonzero components in $x$. We define the *minimum weight* of a code $C$ to be the weight of the nonzero vector of smallest weight in $C$, i.e.,

$$wt(C) = min\{wt(c) \mid c \in C, c \neq 0\}.$$

It is easy to see that $d(x, y) = wt(x - y)$. The *minimum distance* of a code $C$ is defined by

$$d = d(C) = \min_{x,y \in C, x \neq y} \{d(x, y)\}.$$

For a linear code $C$, the minimum distance is also the minimum weight. We use the $[n, k, d]_q$ code as the notation for a $k$-dimensional linear code of length $n$ over $F_q$ with minimum distance $d$.

A code is called *t-error-correcting* if any received word which had $t$ or fewer errors in transmission is correctly decoded by some maximum likelihood decoding scheme. (The method of decoding a received vector to the closest code vector is called *maximum likelihood decoding*.) For a code to be good, $t$ should be large enough relative to the length $n$ of the code. A code with minimum distance $d$ can correct $\left\lfloor \frac{1}{2}(d-1) \right\rfloor$ errors and can detect $\left\lfloor \frac{d}{2} \right\rfloor$ errors, where $\lfloor r \rfloor$ denotes the greatest integer less than or equal to $r$ (Pless, 1998).

The *inner product* of $x$ and $y$ is defined by $x \bullet y = x_1 y_1 + \ldots + x_n y_n$. The *dual code* or *orthogonal code* $C^{\perp}$ of a code $C$ is the set of all vectors of length $n$ that are orthogonal to all codewords of $C$, i.e.,

$$C^{\perp} = \{x \in F_q^n \mid x \bullet y = 0 \text{ for all } y \in C\}.$$

A code $C$ is *self-orthogonal* provided $C \subseteq C^{\perp}$ and *self-dual* provided $C = C^{\perp}$.

We can describe a linear code as a row space or as a null space of a matrix. A $k \times n$ matrix $G$ whose rows form a basis for an $[n, k]$ linear code $C$ is called a *generator matrix* of the code $C$. If $G$ is a generator matrix for $C$, then $C = \{aG \mid a \in F_q^k\}$. A code has a unique generator matrix of the form $[I_k : A]$, where $I_k$ is the $k \times k$ identity matrix. Such a generator matrix is in *standard form*. A *parity check matrix* for $C$ is an $(n-k) \times n$ matrix $H$ such that $c \in C$ if and only if $cH^T = 0$ .

**Definition 1.** A linear code with complementary dual (LCD) is a linear code $C$ satisfying $C \cap C^{\perp} = \{0\}$.

*Remark.* Let $C$ be a linear code.

i. If $C$ is an LCD code, then so is $C^{\perp}$ since $(C^{\perp})^{\perp} = C$.
ii. If $C$ is an LCD code of length $n$ over $F_q$ then $F_q^n = C \oplus C^{\perp}$.

Let $\Pi_C$ be the *orthogonal projector* from $F_q^n$ onto $C$, i.e., the linear mapping from $F_q^n$ onto $F_q^n$ defined by

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

The following theorem gives a complete characterization of LCD codes.

**Theorem 1.** (Massey, 1992) *If G is a generator matrix for the linear code C, then C is an LCD code if and only if the* $k \times k$ *matrix* $GG^T$ *is nonsingular. Moreover, if C is an LCD code, then* $\Pi_C = G^T (GG^T)^{-1} G$ *is the orthogonal projector from* $F_q^n$ *onto C.*

The following corollary to Theorem 1 follows from the fact that the dual code $C^{\perp}$ of $C$ is LCD whenever $C$ is LCD.

**Corollary 2.** *Let C be a linear code and let H be a parity-check matrix of C. Then C is an LCD code if and only if* $HH^T$ *is invertible.*

Recall that the determinant of a matrix $A$, denoted by det($A$), is nonzero if and only if $A$ is nonsingular. Thus, the following corollary is easy to see.

**Corollary 3.** *Let C be a linear code and let G and H be respectively a generator matrix and a parity-check matrix of C. Then the following statements are equivalent:*

C is an LCD code.

*i. C is an LCD code.*
*ii.* $\det(GG^T) \neq 0$.
*iii.* $\det(HH^T) \neq 0$.

## 3. LCD CODES AND PERMUTATION EQUIVALENCE

Often we are interested in properties of codes, such as weight distribution, that remain unchanged when passing from one code to another that is essentially the same. Since linear codes are vector spaces over $F_q$, we might be tempted to look at codes as "essentially the same" if they are isomorphic as vector spaces. Though vector space isomorphism preserves linearity and dimension, under this case, the concept of weight, which is important in the study and use of codes, is lost. Codewords of one weight may be sent to codewords of a different weight via isomorphism. The term *equivalence* is used when comparing two codes that are "essentially the same." In this section, we recall the simplest form of equivalence, called *permutation equivalence*, and prove that it preserves the LCD-ness of linear codes.

**Definition 2.** Two codes $C$ and $C'$ of length $n$ are said to be permutation equivalent provided there is a permutation of coordinates which sends $C$ to $C'$. Equivalently, $C$ and $C'$ are permutation equivalent if there exists a permutation $\sigma$ of the $n$ symbols *{1, 2, …, n}* such that $c' \in C'$ if and only if $c' = \sigma(c)$ for some $c \in C$, where

$$\sigma(c) = \sigma(c_1, c_2, ..., c_n) = (c_{\sigma(1)}, c_{\sigma(2)}, ..., c_{\sigma(n)}).$$

Note that equivalent codes have the same minimum distance and so the same error detection/correction capability. Hence, for studying error detection/correction, we may work with equivalent codes if that helps our study. Any linear code over a finite field is equivalent to a code generated by a matrix in standard form. In this paper, most of the constructions use generator matrices in standard form. Therefore, it is important to find out whether the permutation equivalence of codes preserves the property of being linear with complementary dual.

**Theorem 4.** *Suppose $C_1$ and $C_2$ are two permutation equivalent linear codes. If $C_1$ is LCD, then $C_2$ is also LCD.*

*Proof.* Assume that $C_2 \cap C_2^{\perp} \neq \{0\}$. Then there is a nonzero vector $u$ such that $u \in C_2$ and $u \in C_2^{\perp}$. By Definition 2, since $C_2$ is permutation equivalent to $C_1$, there exists a permutation of coordinates $\sigma$ such that $C_2 = \{\sigma(c) \mid c \in C_1\}$. Hence $u = \sigma(x)$, for some vector $x \in C_1$. Since $u \in C_2^{\perp}$, we have $u \bullet v = 0$ for all $v \in C_2$. This implies that $\sigma(x) \bullet \sigma(y) = 0$ for all $y \in C_1$. Let $x = (x_1, x_2, ..., x_n)$ and $y = (y_1, y_2, ..., y_n)$. Observe

$$\sigma(x_1, x_2, ..., x_n) \bullet \sigma(y_1, y_2, ..., y_n) = 0,$$
$$(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)}) \bullet (y_{\sigma(1)}, y_{\sigma(2)}, ..., y_{\sigma(n)}) = 0,$$
$$\sum_{i=1}^{n} x_{\sigma(i)} y_{\sigma(i)} = 0,$$
$$\sum_{i=1}^{n} x_i y_i = 0.$$

We have shown that $x \bullet y = 0$ for all $y \in C_1$. Thus, $x \in C_1^{\perp}$, and so, $x \in C_1 \cap C_1^{\perp}$. Since $C_1$ is an LCD code, $x = 0$. This contradicts our assumption that $u = \sigma(x)$ is a nonzero vector. Therefore, $C_2$ is an LCD code.

## 4. LCD CODES FROM ORTHOGONAL, ANTIORTHOGONAL, AND SELF-ORTHOGONAL MATRICES

In this section, we construct LCD codes using the characterization given in Theorem 1. This theorem provides a concrete way of constructing LCD codes, i.e., by finding a generator matrix $G$ such that $GG^T$ is nonsingular. We note however that this condition does not imply that $G$ is nonsingular. In fact, $G$ may not even be a square matrix. On the other hand, it is easy to see that the matrix $GG^T$ is nonsingular whenever $G$ is nonsingular.

Thus, by Theorem 1, every nonsingular matrix generates an LCD code. Now, we determine whether or not invertible matrices generate interesting LCD codes.

Let $C$ be a code over $F_q$ generated by an $n \times n$ invertible matrix $G$. Recall that the rows of a generator matrix $G$ form a basis of a linear code $C$. So, rank $G$ = dim $C = n$ since $G$ is nonsingular. Consequently, $C = F_q^n$, and thus, $C$ is the linear code with parameters [$n$, $n$, $1$]. This proves the following proposition.

**Proposition 5.** *If G is a nonsingular matrix, then G generates the trivial* [$n$, $n$, $1$] *LCD code.*

This result shows that a nonsingular generator matrix generates an LCD code with the most number of codewords but lacks the error-correction capability. This type of code is less interesting. Hence, to construct good LCD codes, we should avoid generator matrices $G$, which are invertible.

One way to construct a generator matrix $G$ such that $GG^T$ is invertible is to force $GG^T = I$. Such a matrix is called orthogonal. Massey (1998) defined orthogonal, antiorthogonal, and self-orthogonal matrices over arbitrary fields together with their nonsquare analogs. Hereafter, we use $F$ to denote an arbitrary field.

**Definition 3.** Let $A$ be square matrix $A$ over $F$. Then

*i.* $A$ is said to be *orthogonal* if $AA^T = I$ where $I$ denotes an identity matrix of appropriate order.

*ii.* $A$ is *self-orthogonal* if $AA^T = O$, where $O$ denotes the zero matrix of appropriate dimension.

*iii.* $A$ is *antiorthogonal* if $AA^T = -I$

**Definition 4.** Let $B$ be an $m \times n$ matrix over $F$. Then

*i.* $B$ is said to be *row-orthogonal* if $BB^T = I$.

*ii.* $B$ is *row-self-orthogonal* if $BB^T = O$.

*iii.* $B$ is *row-antiorthogonal* if $BB^T = -I$.

In view of Theorem 1, it is apparent that orthogonal matrices generate LCD codes as indicated in the following corollary.

**Corollary 6.** *Let G be a generator matrix for a code over a finite field* $F_q$. *If G is a row-orthogonal matrix, then G generates an LCD code.*

Notice that a matrix $A$ is nonsingular whenever $A$ is orthogonal since $AA^T = I$ implies $A^{-1} = A^T$. As pointed out in the earlier part of this section, this type of matrix does not generate good LCD codes. On the other hand, a row-orthogonal matrix is not necessarily square and thus a plausible generator matrix of an LCD code with good parameters.

We state the following results by Massey (1998), which give generator matrices of LCD codes using the matrices in Definition 4.

**Proposition 7.** *Let* $G = [I : A]$ *be a generator matrix in standard form of a linear code C. Then C is an LCD code if A is row-self-orthogonal or, equivalently, if G is row-orthogonal.*

**Proposition 8.** *If B is any* $m \times m$ *antiorthogonal matrix and Q is any* $k \times m$ *matrix, then* $G = [I : Q : QB]$ *is a generator matrix of an LCD code of length* $n = k + 2m$ *and dimension k.*

**Proposition 9.** *If Q is any* $k \times k$ *matrix, C is any* $k \times m$ *row-self-orthogonal matrix, and A is any* $m \times m$ *orthogonal matrix, then* $G = [I : QCA]$ *is a generator matrix of an LCD code of length* $n = k + m$ *and dimension k. The same holds true if A is any* $m \times m$ *antiorthogonal matrix.*

The following examples illustrate the constructions given above.

**Example 1.** Let $A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$. It is easy to verify that $A$ is self-orthogonal over $F_2$. So, $G = [I : A]$ is row-orthogonal. The code generated by $G$ is an [8, 4, 2] binary LCD code.

**Example 2.** Let $Q = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix}$;

$$C = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \quad A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

It is easy to check that $C$ is self-orthogonal and $A$ is orthogonal. The matrix $[I : QCA]$ generates a binary LCD code with parameters [8, 4, 2].

Now, we present a method of constructing orthogonal/row-orthogonal matrices from existing ones. A type of matrix multiplication known as the Kronecker product provides a noteworthy construction. Let $M_{m,n}(F)$ denote the space of all $m \times n$ matrices over the field $F$.

**Definition 5.** (Broxson, 2006) The *Kronecker product* of $A = [a_{ij}] \in M_{m,n}(F)$ and $A = [b_{ij}] \in M_{r,s}(F)$, denoted by $A \otimes B$, is defined to be the block matrix

$$A \otimes B = \begin{bmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \dots & a_{mn}B \end{bmatrix} \in M_{mr,ns}(F).$$

**Proposition 10.** *Let* $A \in M_{m,n}(F)$ *and* $B \in M_{r,s}(F)$. *If A and B are row-orthogonal matrices, then* $A \otimes B$ *is also row-orthogonal.*

*Proof.* Since $A$ and $B$ are row-orthogonal, $AA^T = I_m$ and $BB^T = I_r$ Now by Broxson (2006, Theorem 5 and Theorem 7), we have

$$\begin{aligned} (A \otimes B)(A \otimes B)^T &= (A \otimes B)\left(A^T \otimes B^T\right) \\ &= AA^T \otimes BB^T \\ &= I_m \otimes I_r \\ &= I_{mr} \end{aligned}$$

This completes the proof. ■

Since every orthogonal matrix is row-orthogonal, the following corollary follows directly from Proposition 10.

**Corollary 11.** *If A and B are orthogonal matrices, then* $A \otimes B$ *is also an orthogonal matrix.*

Now we construct some classes of binary LCD codes using the permutation matrix and the all-one matrix.

A permutation matrix is known to be orthogonal and hence nonsingular. By Proposition 5, a permutation matrix $P$ of order $n$ generates the trivial [*n, n, 1*] LCD code. We use this information to construct a class of 1-error correcting LCD codes of rate 1/3.

**Theorem 12.** *Let P be the permutation matrix of size n. Then* $G = [P : P : P]$ *generates a binary LCD code of parameters* [3*n*, *n*, 3]

*Proof.* Clearly, $G$ is row-orthogonal since $GG^T = PP^T = I$. Let $C$ be the code generated by $G$. By Corollary 6, $C$ is an LCD code. It is clear from the construction of $G$ that the length of the codewords in $C$ is 3$n$. Since the rows of $P$ are linearly independent, it follows that rank $G$ = dim $C = n$. Each column of $G$ has exactly one

1, and each row of $G$ has exactly three 1s. This implies that every row of $G$ has exactly three 1s, which are located in distinct columns, and thus, every linear combination of two or more rows of $G$ contains at least three 1s. Hence, the minimum distance of $C$ is 3.

■

We generalize this result to a class of binary LCD codes with rate $1/k$ and minimum distance $k$ in the following proposition. The proof follows the same argument as in Theorem 12.

**Theorem 13.** *Let $P$ be a permutation matrix of size $n$ and let $k$ be a positive odd integer. Then $G = \left[\underbrace{P : P : \ldots : P}_{k \text{ times}}\right]$ generates a binary LCD code with parameters [kn,n,k].*

Let $J_n$ denote the all-one $n \times n$ matrix. We use this matrix to construct a class of binary LCD codes of rate 1/2.

**Theorem 14.** *Let $J_n$ be the all-one matrix, where $n$ is even. Then $G = [I_n : J_n]$ generates a binary LCD code with parameters [2n, n, 2].*

*Proof.* Let $A_{ij}$ denote the $ij$-entry of the matrix $A$. Then

$$\begin{aligned}(J_n {J_n}^T)_{ij} &= \sum_{k=1}^{n} (J_n)_{ik} \, ({J_n}^T)_{kj} \\ &= \sum_{k=1}^{n} 1 \\ &= n \\ &= 0 (\mathrm{mod}\, 2)\end{aligned}$$

Thus, $J_n$ is row-orthogonal. By Proposition 7, $G$ generates an LCD code. From the construction of $G$, it is easy to see that the code $C$ generated by $G$ has length $2n$, dimension $n$ and minimum distance 2.

■

**Example 3.** $G = [I_6 : J_6]$ generates a [12, 6, 2] binary LCD code. The weight distribution of this code is given by $1 + 15x^2 + 15x^4 + x^6 + 6x^7 + 20x^9 + 6x^{11}$.

Let $A = J_n - I_n$. Note that $J_n$ and $I_n$ are symmetric matrices. Suppose $n$ is even. Then $AA^T = I_n$ and thus orthogonal. Since $A$ is a square matrix, the orthogonality of this matrix also implies that it is nonsingular. The following corollary to Theorem 1, which follows from the fact the $A$ is nonsingular, gives an alternative generator matrix of an LCD code.

**Corollary 15.** (Dougherty et al., 2015) *Let $G$ be a generator matrix for a code over a finite field. If $GG^T = J_n - I_n$, $n$ even, then $G$ generates an LCD code.*

## 5. LCD CODES FROM GENERATOR MATRICES OF OTHER LINEAR CODES

Massey (1992) showed that the asymptotic goodness of LCD codes follows trivially from that of general linear codes. He showed that for every linear code $C$, there always exists a corresponding LCD code by modifying an arbitrary $[n, k]$ linear code to produce an LCD code whose minimum Hamming distance is at least as good. In this section, we construct LCD codes using the generator matrices of other known codes, namely self-dual codes and binary Hamming codes.

### 5.1 Arbitrary Linear [*n, k, d*] Code

As a motivation, we revisit the construction given by Massey. The first proposition is a construction of LCD codes over a field of characteristic 2 while the latter gives a more general result.

**Proposition 16.** (Massey, 1992) *Let $G = [I_k : A]$ be the generator matrix of a linear $[n, k, d]$*

*code C over the field F of characteristic 2. Then* $G = [I_k : A : A]$ *is a generator matrix of a* $[2n-k, k, d']$ *linear code over F with* $d' \geq d$.

**Proposition 17.** (Massey, 1992) *For any linear* $[n, k, d]$ *code C over the field F of prime characteristic p, there exists a corresponding* $[5n-4k, k, d']$ *LCD code C' with* $d' \geq d$.

### 5.2 Self-Dual Codes

A self-dual code cannot be LCD; however, we can take advantage of its properties to construct LCD codes. Recall that a linear code $C$ is self-dual if $C = C^{\perp}$. This implies that a generator matrix $G$ of a self-dual code $C$ is also a generator matrix of its dual code $C^{\perp}$. Thus, $GG^T = O$ and so $G$ is row-self-orthogonal. Let $G' = [I : G]$. We have,

$$G'G'^T = [I \quad G][I \quad G]^T = I.$$

Hence, $G'G'^T = I$.

**Theorem 18**. *Let G be a* $k \times n$ *generator matrix of a self-dual* $[n,k,d]$ *code over* $F_q$. *Then* $G' = [I : G]$ *is a generator matrix of an LCD code over* $F_q$ *of length n + k, dimension k and minimum distance d + 1.*

*Proof.* Let $C$ be the code generated by $G'$. From the preceding discussion, $G'$ is a row-orthogonal matrix. Then $C$ is an LCD code by Proposition 7. It is clear from the construction of $G'$ that dim $C = k$ and the length of the codes in $C$ is $n + k$. Moreover, since the minimum distance of the self-dual code generated by $G$ is $d$ and the rows of $I$ are distinct, any linear combination of the rows of $G'$ gives a vector with weight of at least $d + 1$.

■

**Example 4.** Consider the binary Golay code of length 24. It is a self-dual code with generator matrix $[I : A]$, where

$$A = \begin{bmatrix} 0&1&1&1&1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&0&0&0&1&0 \\ 1&1&0&0&1&1&0&0&0&1&0&1 \\ 1&0&1&1&1&0&0&0&1&0&1&1 \\ 1&1&1&1&0&0&0&1&0&1&1&0 \\ 1&1&1&1&0&0&1&0&1&1&0&1 \\ 1&1&0&0&0&1&0&1&1&0&1&1 \\ 1&0&0&0&1&0&1&1&0&1&1&1 \\ 1&0&0&0&0&1&1&0&1&1&1&0 \\ 1&0&1&1&1&1&0&1&1&1&0&0 \\ 1&1&0&0&1&0&1&1&1&0&0&0 \\ 1&0&1&1&0&1&1&1&0&0&0&1 \end{bmatrix}$$

The matrix $A$ is orthogonal since $AA^T = I_{12}$. Now, let $G = [I : I : A]$. It is easy to see that $G$ is a row-orthogonal matrix and $G$ generates a binary LCD code with parameters [36, 12, 9].

Let $G = [I : A]$ be a generator matrix in standard form of a binary self-dual code. By self-duality, we have

$$\begin{aligned} GG^T &= [I : A][I : A]^T \\ &= [I + AA^T] \\ &= O. \end{aligned}$$

This implies that $AA^T = I$, and so, $A$ is either orthogonal or row-orthogonal. By Corollary 6, $A$ generates an LCD code. Moreover, since $AA^T = I$, each row of $A$ is orthogonal to every other row of $A$ but has a scalar product of 1 with itself. This means that any collection of rows of $A$ forms a matrix which generates a binary LCD code. This proves the following result.

**Theorem 19.** *Let* $G = [I : A]$ *be a generator matrix in standard form of a binary self-dual code. Then*

*i. A generates a binary LCD code.*
*ii. Any matrix whose rows are a collection of rows of A generates a binary LCD code.*

This result indicates that we can randomly choose rows of $A$ to form a generator matrix of a binary LCD code with high rate and good error-correction capability. In general, if $G = [I : A]$ is a generator matrix in standard form of a self-dual code over $F_q$, then $A$ is an antiorthogonal or a row-antiorthogonal matrix. Hence, by Propositions 8 and 9, we can use $A$ to generate an LCD code over $F_q$.

**Example 5.** LCD codes with parameters [12, 6, 3], [12, 8, 2], and [12, 4, 5] can be constructed using the rows of the matrix $A$ in Example 4.

### 5.3 Binary Hamming Codes

Binary Hamming codes are a class of binary linear codes. Let $n = 2^r - 1$, with $r \geq 2$. Then the $r \times (2^r - 1)$ matrix $H_r$, whose columns, in order, are the numbers $1, 2, \ldots, 2^r - 1$ written as binary numerals, is the parity check matrix of an $[n = 2^r - 1, k = n - r]$ binary code. Any rearrangement of columns of $H_r$ gives an equivalent code, and hence, any one of these equivalent codes will be called the *binary Hamming code* of length $n = 2^r - 1$. Moreover, any binary code with parameters $[2^r - 1, 2^r - r - 1, 3]$ is equivalent to the binary Hamming code (Huffman & Pless, 2003, p. 29). As mentioned earlier, a convenient way of constructing the parity check matrix $H_r$ is by forming a matrix whose $i$th column is the binary representation of the number $i$ (when necessary, we put leading 0s to have an $r$-tuple). Consider the following examples.

**Example 6.**

1. If $r = 2$, then $H_2$ is a $2 \times 3$ matrix given by $H_2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$. This is a parity check matrix of the [3, 1, 3] binary Hamming code.

2. If $r = 3$, then $H_3$ is a $3 \times 7$ matrix given by $H_3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$. The matrix $H_3$ is a parity check matrix of the [7, 4, 3] binary Hamming code.

The following lemma gives a recursive construction of the parity check matrix $H_r$.

**Lemma 20.** *Let $H_r$ be a parity check matrix of a binary Hamming code of length $n = 2^r - 1$ with $r \geq 2$. Suppose that the ith column of $H_r$ represents the binary representation of the number i. Then*

$$H_{r+1} = \begin{bmatrix} O_{1\times 2^r - 1} & 1 & J_{1\times 2^r - 1} \\ H_r & O_{r\times 1} & H_r \end{bmatrix}, \qquad (5.1)$$

where $O_{m\times n}$ denotes an $m \times n$ zero matrix and $J_{m\times n}$ an $m \times n$ all-one matrix.

*Proof.* The matrix $H_{r+1}$ has $2^{r+1} - 1$ columns. It suffices to show that the columns of $H_{r+1}$ correspond to the binary representations of the numbers, in order, 1, 2,..., $2^{r+1} - 1$. We decompose the matrix in (5.1) into three submatrices: $\begin{bmatrix} O_{1\times 2^r - 1} \\ H_r \end{bmatrix}$; $\begin{bmatrix} 1 \\ O_{r+1} \end{bmatrix}$; and $\begin{bmatrix} J_{1\times 2^r - 1} \\ H_r \end{bmatrix}$

Since the columns of $H_r$ correspond to the numbers $1, 2, \ldots, 2^r - 1$, in that order, it follows that the columns of $\begin{bmatrix} O_{1\times 2^r - 1} \\ H_r \end{bmatrix}$ represent the same set of numbers.

Clearly, the column matrix $\begin{bmatrix} 1 \\ O_{r+1} \end{bmatrix}$ represents the number $2^r$. Now, let us consider $\begin{bmatrix} J_{1\times 2^r - 1} \\ H_r \end{bmatrix}$

Each of the 1s in the row matrix $J_{1\times 2^r - 1}$ has value $2^r$. Once again, since the columns of $H_r$ correspond to the numbers 1, 2,..., $2^r - 1$ in that order, the columns of $\begin{bmatrix} J_{1\times 2^r - 1} \\ H_r \end{bmatrix}$ represent the numbers $2^r + 1, 2^r + 2, \ldots, 2^r + 2^r - 1 = 2^{r+1} - 1$. Therefore, $H_{r+1}$ is a

parity-check matrix of the binary Hamming code of length $2^{r+1}-1$.

■

The next lemma counts the number of 1s in the rows of the matrix $H_r$.

**Lemma 21.** *Let $H_r$ be a parity check matrix of a binary Hamming code of length $n = 2^r - 1$, with $r \geq 2$. Then, the number of 1s in each row of $H_r$ is even. In particular, the number of 1s in each row of $H_r$ is $2^{r-1}$.*

*Proof.* We proceed by induction on $r$. The assertion is true for $r = 2$ since each row of $H_2$ has $2^{2-1} = 2$ 1s. Assume that each row of $H_r$ has $2^{r-1}$ 1s. We show that each row of $H_{r+1}$ has $2^r$ 1s. By Lemma 20,

$$H_{r+1} = \begin{bmatrix} O_{1\times 2^r-1} & 1 & J_{1\times 2^r-1} \\ H_r & O_{r\times 1} & H_r \end{bmatrix}.$$

Clearly, the first row of $H_{r+1}$ has $2^r$ 1s. From our assumption, each row of $H_r$ has $2^{r-1}$ 1s. Hence, each of the remaining rows of $H_{r+1}$ has $2 \cdot 2^{r-1} = 2^r$ 1s.
Therefore, the number of 1s in each row of the parity-check matrix $H_r$ of a binary Hamming code is $2^{r-1}$, which is even.

■

**Lemma 22.** *For $r \geq 3$, the parity check matrix $H_r$ of a binary Hamming code is row-orthogonal over $F_2$.*

*Proof.* We proceed by induction on $r$. If $r = 3$, we have $H_3 H_3{}^T = O_3$.
Assume that $H_r H_r{}^T = O_r$. We show that $H_{r+1} H_{r+1}{}^T = O_{r+1}$. By Lemma 20,

$$H_{r+1} = \begin{bmatrix} O_{1\times 2^r-1} & 1 & J_{1\times 2^r-1} \\ H_r & O_{r\times 1} & H_r \end{bmatrix}.$$ Now,

$$\begin{aligned} H_{r+1}H_{r+1}{}^T &= \begin{bmatrix} O_{1\times 2^r-1} & 1 & J_{1\times 2^r-1} \\ H_r & O_{r\times 1} & H_r \end{bmatrix} \begin{bmatrix} O_{1\times 2^r-1} & H_r \\ 1 & O_{r\times 1} \\ J_{1\times 2^r-1} & H_r \end{bmatrix} \\ &= \begin{bmatrix} 0+1+1 & O_{1\times r} + O_{1\times r} + X \\ O_{r\times 1} + O_{r\times 1} + Y & H_r H_r{}^T + O_{r\times r} + H_r H_r{}^T \end{bmatrix} \\ &= \begin{bmatrix} 0 & X \\ Y & O_r \end{bmatrix}, \end{aligned} \tag{5.2}$$

where $X = J_{1\times(2^r-1)} H_r{}^T$ and $Y = H_r J_{(2^r-1)\times 1}$.

Now, observe that $X$ is a $1 \times r$ matrix whose $i$th entry corresponds to the sum of the entries in $i$th row of $H_r$. Similarly, $Y$ is an $r \times 1$ matrix whose $j$th entry corresponds to the sum of the entries in the $j$th row of $H_r$. By Lemma 21, $X_{1j} = 2^{r-1} = 0 (\mathrm{mod}\, 2)$ for $1 \leq j \leq r$ and $Y_{i1} = 2^{r-1} = 0 (\mathrm{mod}\, 2)$ for $1 \leq i \leq r$. From (5.2), $H_{r+1} H_{r+1}{}^T = O_{r+1}$. This completes the proof.

■

We now state the main result in this subsection, which gives another family of binary LCD codes.

**Theorem 23.** *Let $H_r$ be a parity check matrix of a binary Hamming code of length $n = 2^r - 1$ where $r \geq 3$. Then, $G = [I_r : H_r]$ generates a binary LCD code of length $2^r + r - 1$ and dimension r.*

*Proof.* The statement that $G = [I_r : H_r]$ generates an LCD code follows from Lemma 22 and Proposition 7. The length and the dimension of the code generated by $G$ is clear from the construction of $G$.

■

For $3 \leq r \leq 7$, we list the parameters of the binary LCD codes generated by $G = [I_r : H_r]$ in Table 1. We note that the dual codes of these codes are also LCD. It is interesting to

note that the LCD codes in Table 1 are optimal based on the database of codes compiled in Grassl (n.d.)

## 6. NEW LCD CODES FROM OLD

Many interesting and important codes will arise by modifying or combining existing codes. In this section, we examine if such modification

**Table 1.** Optimal binary LCD codes obtained using Hamming matrix

| $r$ | The parameters of the code C generated by $G = [I_r : H_r]$ | The parameters of the dual code $C^{\perp}$ |
|---|---|---|
| 3 | [10, 3, 5] | [10, 7, 2] |
| 4 | [19, 4, 9] | [19, 15, 2] |
| 5 | [36, 5, 17] | [36, 31, 2] |
| 6 | [69, 6,33] | [69, 63, 2] |
| 7 | [134, 7, 65] | [134, 127, 2] |

or combination of LCD codes will result to linear codes with complementary duals. To this end, we recall some classic methods of constructing new codes using known codes.

### 6.1 Direct Product

Consider a block code of length $n = n_1 n_2$. Instead of writing the codewords as row vectors of length $n$, we can represent the codewords by $n_1 \times n_2$ matrices. One way of doing this is by representing the codeword $a = (a_0, a_1, \ldots, a_{n-1})$ by the matrix $A = [a_{ij}]$ $i = 0, 1, 2, \ldots, n_1 - 1$, $j = 0, 1, 2, \ldots, n_2 - 1$, where $a_{ij} = a_{in_2+j}$. This is called the *canonical ordering*.

**Definition 6.** Let $C_1$ and $C_2$ be linear codes of parameters $[n_1, k_1]$ and $[n_2, k_2]$, respectively.

Let $C$ be a code of length $n_1 n_2$ represented by $n_1 \times n_2$ matrices with the canonical ordering. We say that $C$ is the *direct product* of $C_1$ and $C_2$, denoted by $C_1 \otimes C_2$, if and only if $C$ consists of all codewords for which the matrix representation has the following properties:

i. each column of a matrix is the transpose of a codeword of $C_1$,

ii. each row of the matrix is a codeword of $C_2$.

*Remark.* The product code of $C_1$ and $C_2$ can also be defined by

$$C_1 \otimes C_2 = \left\{ (c_{ij})_{1 \le i \le n_1, 1 \le j \le n_2} \middle| \begin{matrix} (c_{ij})_{1 \le i \le n_1, \text{ for all } j} \\ (c_{ij})_{1 \le j \le n_2, \text{ for all } i} \end{matrix} \right\}.$$

In the literature, the direct product is also called the *Kronecker product* or *tensor product*.

*Remark.* It is easy to see that the direct product of two linear codes is again a linear code.

We also note that $C_1 \otimes C_2$ is equivalent to $C_2 \otimes C_1$. The following result gives the parameters of the direct product of two linear codes.

**Proposition 24.** (van Lint, 1973) *Let $C_1$ and $C_2$ be linear codes with parameters $[n_1, k_1, d_1]$ and $[n_2, k_2, d_2]$, respectively. Then, $C_1 \otimes C_2$ has parameters $[n_1 n_2, k_1 k_2, d_1 d_2]$.*

In this subsection, we aim to show that the product code of two LCD codes is again an

LCD code. To this end, we need to describe the generator matrix of the direct product of two linear codes.

**Lemma 25.** (van Lint, 1973, p. 38) *Let* $G_1$ *and* $G_2$ *be generator matrices of* $C_1$ *and* $C_2$ *respectively. Then,* $G_1 \otimes G_2$ *is a generator matrix of* $C_1 \otimes C_2$.

Now, we are ready to prove the desired result in this subsection.

**Theorem 26.** *If* $C_1$ *and* $C_2$ *are LCD codes, then* $C_1 \otimes C_2$ *is also LCD.*

*Proof.* Let $G_1$ and $G_2$, respectively, be generator matrices of $C_1$ and $C_2$. Then, $G = G_1 \otimes G_2$ generates $C_1 \otimes C_2$ by Lemma 25. We show that $GG^T$ is invertible. By Broxson (2006, Theorem 5 and Theorem 7), we have

$$\begin{aligned} GG^T &= (G_1 \otimes G_2)(G_1 \otimes G_2)^T \\ &= (G_1 \otimes G_2)(G_1{}^T \otimes G_2{}^T) \\ &= G_1G_1{}^T \otimes G_2G_2{}^T. \end{aligned}$$

Since $C_1$ and $C_2$ are LCD codes, $G_1G_1{}^T$ and $G_2G_2{}^T$ are both nonsingular by Theorem 1. By Broxson (2006, Corollary 10), $GG^T$ is nonsingular. Thus, $C_1 \otimes C_2$ is an LCD code by Theorem 1.

■

To illustrate this construction, we look at the following example.

**Example 7.** Let $C_1$ be the binary linear code generated by $G_1 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$ and let $C_2$ be the binary linear code generated by $G_2 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$. By observing that $G_1G_1{}^T = G_2G_2{}^T = I_2$, then $C_1$ and $C_2$ are binary LCD codes with parameters [4, 2, 2] and [6, 2, 3], respectively. The matrix $G = G_1 \otimes G_2$ generates the direct product $C_1 \otimes C_2$, which is a binary LCD code with parameters [24, 4, 6].

### 6.2 Direct Sum

In the preceding subsection, we have seen that given an $[n_1, k_1, d_1]$ LCD code $C_1$ and an $[n_2, k_2, d_2]$ LCD code $C_2$, by direct product construction, we get an LCD code with parameters $[n_1n_2, k_1k_2, d_1d_2]$. The product code has rate $(k_1k_2)/(n_1n_2)$, which is equal to the product of the code rates of $C_1$ and $C_2$ In this subsection, we recall another known method of construction that is simpler than the direct product. This construction gives new code with greater rate from two given codes.

**Definition 7.** Given an $[n_1, k_1]$ code $C_1$ and an $[n_2, k_2]$ code $C_2$. Their *direct sum* $C_1 \oplus C_2$ is defined by

$$C_1 \oplus C_2 = \{(c_1, c_2) \mid c_1 \in C_1 \text{ and } c_2 \in C_2\}.$$

*Remark.* If $C_1$ and $C_2$ is linear so is $C_1 \oplus C_2$.

**Lemma 27.** (Huffman & Pless, 2003) *Let* $G_1$ *and* $G_2$ *be generator matrices of the linear codes* $C_1$ *and* $C_2$*, respectively. Then, the generator matrix of* $C_1 \oplus C_2$ *is given by*

$$G_1 \oplus G_2 = \begin{bmatrix} G_1 & O \\ O & G_2 \end{bmatrix}.$$

The following corollary is clear from the structure of the generator matrix of the direct sum of two linear codes given in Lemma 27.

**Corollary 28.** *Given linear codes* $C_1$ *and* $C_2$ *with parameters* $[n_1, k_1, d_1]$ *and* $[n_2, k_2, d_2]$ *respectively. Then,* $C_1 \oplus C_2$ *is a linear* $[n_1 + n_2, k_1 + k_2, d]$ *code where* $d = \min\{d_1, d_2\}$

**Theorem 29.** *If $C_1$ and $C_2$ are LCD codes, then the direct sum $C_1 \oplus C_2$ is also an LCD code.*

*Proof.* By Lemma 27, the generator matrix of $C_1 \oplus C_2$ is given by

$$G = G_1 \oplus G_2 = \begin{bmatrix} G_1 & O \\ O & G_2 \end{bmatrix}.$$

It suffices to show that $GG^T$ is invertible. Now,

$$GG^T = \begin{bmatrix} G_1 & O \\ O & G_2 \end{bmatrix} \begin{bmatrix} {G_1}^T & O \\ O & {G_2}^T \end{bmatrix} = \begin{bmatrix} G_1{G_1}^T & O \\ O & G_2{G_2}^T \end{bmatrix}.$$

Note that $G_1{G_1}^T$ and $G_2{G_2}^T$ are invertible matrices since $G_1$ and $G_2$ are generator matrices of LCD codes. Thus, $G$ is invertible since the inverse of a block diagonal matrix is another block diagonal matrix, composed of the inverses of each block. The desired result follows from Theorem 1.

■

The rate of the direct sum is $(k_1 + k_2)/(n_1 + n_2)$, which is greater than $(k_1k_2)/(n_1n_2)$ the rate of the product code. However, the minimum distance of the direct sum of two codes does not exceed the minimum distance of either of the given codes.

We note that Theorem 26 and Theorem 29 were also proved in Carlet and Guilley (2015). However, in this paper, we obtain these results using different proofs (i.e., using Massey's (1992) characterization of LCD codes).

### 6.3 The Plotkin Sum or $(u \mid u+v)$ Construction

Two codes of the same length can be combined to form a third code of twice the length in a way similar to the direct sum construction. Here, we recall the $(u \mid u + v)$ construction also known as the Plotkin sum. We give a counterexample to show that the Plotkin sum of two LCD codes is not always an LCD code. We also mention a result by Carlet and Guilley (2015), which gives sufficient conditions for the Plotkin sum of two linear codes to be LCD.

**Definition 8.** Let $C_1$ and $C_2$ be linear codes over $F_q$ with parameters $[n_1, k_1, d_1]$ and $[n_2, k_2, d_2]$, respectively. The *Plotkin sum* of $C_1$ and $C_2$ or the $(u \mid u + v)$ construction produces the code $C = \{(u, u+v \mid u \in C_1, v \in C_2\}$.

**Proposition 30.** (Pellikaan et al., 2015, Theorem 2.1.45) *Let $C_i$ be an $[n, k_i, d_i]$ code with generator matrix $G_i$ for $i = 1, 2$. Then, the Plotkin sum of $C_1$ and $C_2$ is a $[2n, k_1 + k_2, \min\{2d_1, d_2\}]$ code with generator matrix* $\begin{bmatrix} G_1 & G_1 \\ O & G_2 \end{bmatrix}$.

In the preceding subsections, we have just shown that the direct product and the direct sum of two LCD codes are again LCD codes. On the contrary, the Plotkin sum of two LCD codes does not in every case give rise to a new LCD code. Consider the following example.

**Example 8.** Let $C_1$ be the binary linear code generated by $G_1 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$ and let $C_2 = {C_1}^{\perp}$. It was shown in Example 7 that $C_1$ is a [6, 2, 3] binary LCD code. Then $C_2$ is also a binary LCD code with parameters [6, 4, 2] that is generated by $G_2 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$

Let $C$ be the code obtained by taking the Plotkin sum of $C_1$ and $C_2$. Then by Proposition 30, the matrix

$$G = \begin{bmatrix} G_1 & G_1 \\ O & G_2 \end{bmatrix} = \begin{bmatrix} 1&1&1&0&0&0&1&1&1&0&0&0 \\ 0&0&0&1&1&1&0&0&0&1&1&1 \\ 0&0&0&0&0&0&0&0&0&1&0&1 \\ 0&0&0&0&0&0&0&0&0&1&1&0 \\ 0&0&0&0&0&0&1&0&1&0&0&0 \\ 0&0&0&0&0&0&1&1&0&0&0&0 \end{bmatrix}$$

is a generator matrix of $C$. However, $\det(GG^T) = 0$ over $F_2$. This implies that the binary linear code $C$ is not an LCD code by Corollary 3 though both $C_1$ and $C_2$ are LCD codes.

Example 8 serves as a counterexample to show that the Plotkin sum of two LCD codes is not necessarily an LCD code. Despite this result, we can still employ the $(u \mid u + v)$ construction to construct LCD codes. Carlet and Guilley (2015) gave an interesting construction of LCD codes using the Plotkin sum. Given linear codes $C_1$ and $C_2$, they gave a sufficient double condition for the Plotkin sum of $C_1$ and $C_2$ to be LCD. We state this result as follows.

**Proposition 31.** (Carlet & Guilley, 2015) *If $C_1$ and $C_2$ are linear codes with parameters $[n,k_1,d_1]$ and $[n,k_2,d_2]$, respectively, and if $C_2 \cap C_1^{\perp}$ is LCD (i.e., $C_1 + C_2^{\perp}$ is LCD) and $C_1 \cap C_2^{\perp} = \{0\}$, then the Plotkin sum of $C_1$ and $C_2$ is an LCD code.*

In some cases, the construction specified in Proposition 31 gives rise to an LCD code with better rate (Carlet & Guilley, 2015).

## 7. SUMMARY AND RECOMMENDATION

This paper is devoted to construction of LCD codes. Constructions based on orthogonal/row-orthogonal matrices and generator matrices of self-dual codes binary Hamming codes were presented. Optimal binary LCD codes were obtained from the construction based on the Hamming matrix. We also proved that the permutation equivalence of codes preserves the property of being LCD and that the direct sum and direct product of two LCD codes are also LCD codes.

It is worthwhile to consider other known linear codes to construct LCD codes with good parameters. It would be interesting to present a systematic construction of row-orthogonal matrices that will yield an LCD code with high rate and large minimum distance. It is also noteworthy to see codes from designs and codes from graphs in the construction of LCD codes.

## ACKNOWLEDGMENTS

The first author would like to thank the Department of Science and Technology–Science Education Institute for the support through the ASTHRDP-NSC scholarship program. The authors would also like to thank the referee for the comments, corrections, and suggestions, which helped to improve this paper.

## REFERENCES

Broxson, B. J. (2006). The Kronecker Product. *Theses and Dissertations (Paper 25)*. Retrieved May 2015 from http://digitalcommons.unf.edu/etd/25.

Carlet, C., & Guilley, S. (2015). Complementary dual codes for counter-measures to side-channel attacks. *Cryptology ePrint Archive, Report 2015/603*. Retrieved October 2015 from http://eprint.iacr.org.

Dougherty, S. T., Kim, J.-L., Sok, L., & Solé, P. (2015). *The combinatorics of LCD codes: Linear Programming bound and orthogonal matrices*.

Esmaeili, M., & Yari, S. (2009). On complementary-dual quasi-cyclic codes. *15*, 375–386.

Grassl, M. (n.d.). *Bounds on the minimum distance of linear codes and quantum codes*. Retrieved October 17, 2015, from http://www.codetables.de.

Huffman, W., & Pless, V. S. (2003). *Fundamentals of error correcting codes*. Cambridge: Cambridge University Press.

Liu, X., & Liu, H. (2015). LCD codes over finite chain rings. *Finite Fields and Their Applications 34*, 1–19.

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

Massey, J. L. (1998). *Orthogonal, antiorthogonal and self-orthogonal matrices and their codes*.

Pellikaan, R., Wu, X.-W., Bulygin, S., & Jurrius, R. (2015). *Error-correcting codes*. Cambridge: Cambridge University Press.

Pless, V. S. (1998). *Introduction to the theory of error-correcting codes* (3rd ed.). USA: John Wiley and Sons, Inc.

Sendrier, N. (2004). Linear codes with complementary duals meet the Gibert-Varshamov bound. *Discrete Mathematics 285*, 345–347.

van Lint, J. H. (1973). *Coding theory, lecture notes in mathematics* (2nd ed., Vol. 201). Springer Science & Business Media.

Yang, X., & Massey, J. L. (1994). The condition for a cyclic code to have a complementary dual. *Discrete Mathematics 126*, 391–393.