On the Construction of Some LCD Codes over Finite Fields

Eusebio R. Lina Jr.[1], Ederlina G. Nocon[1]*
[1]Mathematics Department, De La Salle University
*Corresponding Author: ederlina.nocon@dlsu.edu.ph

Abstract: A linear code is called an LCD (linear with complementary dual) code if it intersects with its dual trivially, i.e. a linear code C is LCD provided $C \cap C^{\perp} = \{0\}$. These codes, introduced by Massey in 1992, give an optimum linear coding solution for the two user binary adder channel. In this paper, we aim to construct some families of LCD codes. To this end, we use the characterization of an LCD code proved by Massey. We present construction based on some special types of matrices such as orthogonal, self-orthogonal, and antiorthogonal matrices. In particular, we obtain some classes of binary LCD codes using the permutation matrix and the all one matrix. In addition, we propose explicit construction of generator matrices of LCD codes using the generator matrices of some known codes such as self-dual codes and binary Hamming codes. For $3 \le r \le 7$, the binary LCD codes that we obtained using the Hamming matrix H_r are optimal. We also prove that permutation equivalence of codes preserves the LCD-ness of codes.

Key Words: LCD codes; complementary dual codes; construction of LCD codes; binary LCD codes

1. INTRODUCTION

Error-correcting codes play an important role in digital communication. 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 two-user binary adder channel. They are also used 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 proposed in (Dougherty et al., 2015). Yang and Massey (1994) gave the 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-cylic codes to be LCD codes. Recently, LCD codes over finite chain rings were studied in (Liu & Liu, 2015).

In this paper, we propose some explicit construction of LCD codes by applying the characterization given in (Massey, 1992). We present some families of binary LCD codes using the permutation matrix and the all one matrix. We also obtain some classes of LCD codes from the generator matrices of self-dual codes and binary Hamming 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.

Let $x=(x_1,\ldots,x_2)$ and $y=(y_1,\ldots,y_n)$ 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. $d(x,y)=|\{i \mid x_i \neq y_i\}|$. 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. The *minimum distance* of a code C is defined by $d=d(C)=\min_{x,y\in C, x\neq y}\{d(x,y)\}$. We use $[n,k,d]_q$ code as the notation for a k-dimensional linear code of length n over F_q with minimum distance d. The *inner product* of vectors x and y is defined by $x \bullet y = x_1y_1+\ldots+x_ny_n$. 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. $C^\perp=\{x\in F_q^n \mid x\bullet y=0$ for all $x,y\in C\}$.

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 *parity check matrix* for C is an $(n-k)\times n$ matrix H such that $c\in C$ if and only if $cH^T=0$.

Now, we define formally an LCD code.

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

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 Π_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

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

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.*

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.*

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

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

3. RESULTS

3.1 LCD Codes and Permutation Equivalence

Often we are interested in properties of codes, such as weight distribution, which remain unchanged when passing from one code to another that is essentially the same. We use the term equivalence when comparing two codes which are ``essentially the same''. Here, we define the simplest form of equivalence, called permutation equivalence, and prove that it preserves the LCD-ness of a code.

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 σ of the n symbols *{1, 2, …, n}* such that $c'=(c_1',c_2',\ldots,c_n')\in C'$ iff $c'=\sigma(c)$ for some $c\in C$, where

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

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. We now show that permutation equivalence of codes preserves the LCD-ness of a code.

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 σ 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 $\sigma(x) \bullet \sigma(y) = 0$, so $x \bullet y = 0$ for all $y \in C_1$. Thus, $x \in C_1^{\perp}$ and hence $x \in C_1 \cap C_1^{\perp}$. 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. □

3.2 LCD Codes from Orthogonal, Antiorthogonal and Self-orthogonal Matrices

Theorem 1 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. 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 G generates an LCD code. The following result is easy to see.

Proposition 5. *If G is a nonsingular matrix $n \times n$, 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 $GG^T = I$, where I is the identity matrix of appropriate order. This can be done using the matrices which we define below. 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 $AA^T = I$.
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 $A^{-1} = A^T$. 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 of an LCD code with good parameters.

Proposition 7. (Massey, 1998) *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.*

The next results give generator matrices of LCD codes which make use of antiorthogonal matrices.

Proposition 8. (Massey, 1998) *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. (Massey, 1998) *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.

For the rest of this subsection, we restrict our construction of matrices to the binary field F_2 in order to obtain generator matrices of binary LCD codes. We now construct some families of binary LCD codes using the permutation matrix and the all one matrix using the preceding results.

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.

Proposition 10. *Let P be the permutation matrix of size n. Then $G = [P : P : P]$ generates an LCD code of parameters* $[3n, n, 3]$.

Proof. It is easy to see that G is row-orthogonal. By Corollary 6, G generates an LCD code. The parameters of the code generated by G are clear from its construction. □

We generalize this result to a class of LCD codes with rate *1/k* and minimum distance k in the following proposition. The proof follows the same argument as in Proposition 10.

Proposition 11. *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 an 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. The next lemma is easy to see.

Lemma 12. *If n is even, then J_n is self-orthogonal.*

Proposition 13. *Let J_n be the all one matrix, where n is even. Then $G = [I_n : J]$ generates a binary LCD code with parameters* [*2n, n, 2*].

Proof. By Proposition 7 and Lemma 12, 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 1. $G = [I_6 : J_6]$ generates a [12, 6, 2] binary LCD code.

The following corollary to Theorem 1, which also uses the all one matrix, gives us an alternative generator matrix of an LCD code.

Corollary 14. (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.*

3.3 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.

3.3.1 Self-dual Codes

A self-dual code cannot be an 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 $G' = [I : G]$. Then, $G' G'^T = I$.

Theorem 15. *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 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. The minimum distance and the dimension of C are clear from the construction of G'. □

Example 2. 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 $AA^T = I_{12}$. It is easy to see that the matrix $G = [I : I : A]$ is row-orthogonal and generates a binary LCD code with parameters [36, 12, 9].

Let $G = [I : A]$ be a systematic generator matrix (i.e., generator matrix in standard form) of a binary self-dual code. Then $GG^T = O$. 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 16. *Let $G = [I : A]$ be a systematic generator matrix of a binary self-dual code. Then*

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

This result indicates that we can randomly choose rows from 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 systematic generator matrix 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 3. Using the rows of matrix A in Example 2, we obtain binary LCD codes with parameters [12, 6, 3], [12, 8, 2] and [12, 4, 5].

3.3.2 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. 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 a parity check matrix H_r is by forming a matrix whose ith column is the binary representation of the number i (when necessary, we put leading 0s to have an r-tuple). The following lemma gives a recursive construction of a parity check matrix H_r.

Lemma 17. *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*

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

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

The next lemma, which counts the number of 1s in the rows of the matrix H_r, can be proved using Lemma 17 by induction on r.

Lemma 18. *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}.*

Lemma 19. *For $r \geq 3$, the parity check matrix H_r of a binary Hamming code is row-orthogonal over F_2.*

Similarly, we can prove Lemma 19 by induction on r using Lemma 17 and 18. We now state the main result in this subsection which describes a family of binary LCD codes.

ISSN 2449-3309

Theorem 20. *Let* H_r *be a parity check matrix of a binary Hamming code of length* $n = 2^r - 1$. *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 19 and Proposition 7. The length and the dimension of the code generated by *G* are clear from the construction of *G*. □

For $3 \le r \le 7$, 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 all of the LCD codes in Table 1 are optimal based on the database of codes compiled in (Grassl, n.d.).

Table 1. Optimal binary LCD codes obtained using Hamming matrix

r	The code C generated by $G = [I_r : H_r]$	$C^{\perp}$
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]

4. CONCLUSIONS

This paper is devoted to construction of LCD codes. Constructions based on orthogonal/row-orthogonal matrices and generator matrices of self-dual codes and binary Hamming codes were presented. Optimal binary LCD codes were obtained from the construction based on the Hamming matrix. We also proved that permutation equivalence of codes preserves the LCD-ness of a code.

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.

5. ACKNOWLEDGMENTS

The first author would like to thank DOST-SEI for the support through the ASTHRDP-NSC scholarship program.

6. REFERENCES

Carlet, C., & Guilley, S. (2015). Complementary dual codes for counter-measures to side-channel attacks. *Cryptology ePrint Archive, Report 2015/603*.

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

Esmaeili, M., & Yari, S. (2009). On complementary-dual quasi-cyclic codes. *Finite Fields and Their Applications, 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. *Communications and coding , 2* (3).

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

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