JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A SURVEY ON LCD CODES

[1]Nitin Darkunde,[2]Sachin Basude,[3]Mahesh Wavare

[1]Assistant Professor,[2]Assistant Professor,[3]Associate Professor
[1]School of Mathematical Sciences, SRTM University, Nanded, India.
[2]SSGS Institute of Engineering and Technology, Nanded, India.
[3]Rajarshi Shahu College, Latur, India.

Abstract: LCD codes is a topic of immense importance since their introduction by Massey ([1]) in 1992. After that, in last decade several developments in the field of LCD codes has been carried out by several authors ([2] to [22] etc.). Authors studied these codes over some small finite fields, further study of LCD codes has been carried out on some large fields. Their generalizations over commutative rings is also carried out. The present paper by us, is a honest attempt to throw a light on these gradual developments via the survey. This will certainly become an important document for budding researchers in this field.

Keywords: LCD code, generator matrix, symplectic LCD codes, bounds on LCD codes.

I. INTRODUCTION

LCD (Linear complementary dual) codes play an important role in the coding theory. These codes can be employed for studying side-channel attacks, and study some cryptosystems ([16]). Encoding of messages is important in order to protect our information while their propagation through noisy channel. Moreover, fast decoding of messages is also an important aspect for recovery of message. Such thing forms a central object in coding theory.

In this paper, we are going to throw light on developments from rudimentary level to recent in the field of LCD codes. These are the codes whose intersection with their dual code comes out to be trivial. These codes have been studied via different inner products([1]-[22]). LCD codes with respect to symplectic inner product has been studied recently in ([21]). Most of the LCD codes were studied with respect to usual inner product and Hamming distance.

Let us see some basic results and definitions which are available in ([23]).

Definition 1.1([7],[23]): Let F_2^n be the n-dimensional vector space over the binary field F_2. A binary linear $[n,k]$ code is a k-dimensional subspace of the vector space F_2^n.

So linear codes are nothing but vector spaces over finite fields. Note that, n,k in above definition refers to length and dimension of linear code respectively. For practical purposes, we should have n to be as large as possible. There is one more aspect of code , which is defined in all textbooks of coding theory in the following way.

Definition 1.2([23]): $d(C) = min\{d(x,y): x,y \in C \text{ and } x \neq y\}$, where $d(x,y)$ means the number of positions at which x and y differes from each other.

Example 1.3: Let $= \{000,100,010,110\}$, then as per above definitions, this code C is [3,2,1] code over the binary field.

Definition1.4([21]): Let $u = (u_1, u_2, \dots, u_n), v = (v_1, v_2, \dots, v_n) \in \mathbb{F}_q^n$, the Euclidean inner product $<,>_E$ is given by $< u, v\rangle_E = \sum_{i=1}^n u_i . v_i$. For an $\mathbb{F}_q$-linear code C in $\mathbb{F}_q^n$, define the Euclidean dual $C^{\perp_E} = \{x \in \mathbb{F}_q^n : \langle x, c >_E = 0 \forall c \in C\}$.

Definition 1.5([21]): For $u, v \in \mathbb{F}_{q^2}$, the Hermitian inner product $<,>_H$ is defined by $< u, v\rangle_H = \sum_{i=1}^n \bar{u}_i . v_i$. For an $\mathbb{F}_{q^2}$-linear code C in $\mathbb{F}_{q^2}^n$, define the Hermitian dual $C^{\perp_H} = \{x \in \mathbb{F}_{q^2}^n : \langle x, c >_H = 0 \forall c \in C\}$

II. RECENT DEVELOPMENTS PERTAINING TO LCD CODES.

Definition 2.1([1]-[22]): A linear code with a complementary dual (or an LCD code) is defined to be a linear code C whose dual code $\mathrm{C}^{\perp}$ satisfies $\mathrm{C} \cap \mathrm{C}^{\perp} = \{0\}$.

Example 2.2: $C = \{00,01\} \subseteq F_2^2$

Non Example 2.3: If C is self dual, then it can not be LCD Code, for if, assume that, C is self dual, then $\mathrm{C} = \mathrm{C}^{\perp}$, therefore $\mathrm{C} \cap \mathrm{C}^{\perp} \neq \{0\}$. Therefore any non-trivial self dual code can not be LCD code.

Remark 2.4([1]): If C is LCD, then so is $\mathrm{C}^{\perp}$. This is because of the fact that, $(\mathrm{C}^{\perp})^{\perp} = \mathrm{C}$.

Theorem 2.5([1]-[22]): If G is a generator matrix for the [n, k] linear code C, then C is an LCD code if and only if the k × k matrix GG^{T} is an invertible matrix.
This is one of the most important characterizations of LCD codes, which is widely used in each of the references from [1] to [22].

In order to study some combinatorial aspects of LCD codes, one object was defined in ([7]), which we are going to state below. This object is useful to study bounds on LCD codes in binary set up.

Definition 2.6([7]): $LD(n,k) := \max\{d \mid \text{there exists a binary } [n,k,d]\ LCD \text{ code}\}$. It means for fixed n and k, write all LCD codes and then collect their distance in one set. The maximum distance among those distances will be denoted as $LD(n,k)$.

Some well known bounds on $LD(n,k)$ in binary set up are given in subsequent theorems. These bounds are similar to that of $A_q(n,d)$ and $B_q(n,d)$. For more details of these two notations, one may refer [23].

Theorem 2.7([7]): $LD(n,2) \leq \left\lfloor \frac{2n}{3} \right\rfloor$ for $n \geq 2$.
For some values of n the inequality in above theorem becomes equality which is shown explicitly by authors in their article [7].

Theorem 2.8([7]): Let $n \geq 2$. Then $LD(n,2) = \left\lfloor \frac{2n}{3} \right\rfloor$ for $n \equiv 1, \pm 2$, or $3(\bmod 6$.

The upper bound on $LD(n,2)$ for value of $k \geq 3$ is given in [7], via the use of well known Griesmer bound. For exposition of Griesmer bound, one may refer [23].

Theorem 2.9([7]): $LD(n,k) \leq \left\lfloor \frac{n \cdot 2^{k-1}}{2^k - 1} \right\rfloor$ for $3 \leq k \leq n$.

The characterization of LCD codes can be stated for Hermitian as well as Euclidean case in following theorem, which is stated in [21].

Theorem 2.13([21]): Let G be a generator matrix for the $[n,k]$-linear code C, then C is an Hermitian (respectively. a Euclidean) LCD code if and only if (iff) the $k \times k$ matrix $G\mathrm{G}^{\mathrm{T}}$ has non-zero determinant.

In case of Symplectic LCD codes, the characterization of LCD codes is little bit modified and it is given in [21].
Theorem 2.14([21]): Suppose G is a generator matrix for the F_q-linear code C in F_q^{2n} with parameters $[2n,k]$, then C is a symplectic LCD code iff the $k \times k$ matrix $G\Omega G^{\mathrm{T}}$ is invertible, where $\Omega = \begin{bmatrix} O & I_n \\ -I_n & 0 \end{bmatrix}$ and O means zero matrix of compatible size.

In [21], new constructions of Symplectic LCD codes out of old ones is derived. Such constructions used to produce new codes with new parameters, which are most of the times superior to their ancestral codes.

Theorem 2.15([21]): LetC_i be a q-ary $[2n_i, 2k_i, d_i]$ symplectic LCD code with a generator matrix $G^{(i)} = \left[G_1^{(i)} \mid G_2^{(i)}\right]$, where $i = 1,2$. Then

$$G = \begin{bmatrix} G_1^{(1)} & 0 & G_2^{(1)} & 0 \\ 0 & G_1^{(2)} & 0 & G_2^{(2)} \end{bmatrix}$$

generates a q-ary $[2n_1 + 2n_2, 2k_1 + 2k_2, \min\{d_1, d_2\}]$ symplectic LCD code C.
Above construction have been generalized in [21] by authors for n number of codes. This is stated below.

Theorem 2.16([21]): LetC_i be a q-ary $[2n_i, 2k_i, d_i]$ symplectic LCD code for $i = 1,2,,n$ and

$$G^{(i)} = \left[G_1^{(i)} \mid G_2^{(i)}\right]$$

be a generator matrix of C_i. Then,

$$G = \begin{bmatrix} G_1^{(1)} & 0 & \cdots & 0 & G_2^{(1)} & 0 & \cdots & 0 \\ 0 & G_1^{(2)} & \cdots & 0 & 0 & G_2^{(2)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & G_1^{(n)} & 0 & 0 & \cdots & G_2^{(n)} \end{bmatrix}$$

generates a q-ary$[\sum_{i=1}^{n} n_i, \sum_{i=1}^{n} k_i, \min\{d_i\}]$ symplectic LCD code C.

In [21], authors put forth one more condition on generator matrices of C_1 and C_2 and come up with one more construction of symplectic LCD codes.

Theorem 2.17([21]): Let$C$ be a q-ary linear code with a generator matrix

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

where G_i is a generator matrix of a q-ary $[n, k, d_i]$ linear code $C_i, i = 1,2$. If C_1, C_2 are Euclidean LCD and $G_1^{\top} G_2$ is symmetric, then C is a $[2_n, 2_k, d_S]$ symplectic LCD code, where $d_S = \min\{d_1, d_2\}$.

CONCLUSION:

Study of LCD codes is quite important from the prospective of coding theory. Study of bound on LCD codes is quite important for studying important parameters of codes from which error detection and error correction capabilities of such codes can be studied. The present article will serve a better , concise reference material for future work on LCD codes.

REFERENCES

[1] Massey, J.L., 1992. Linear codes with complementary duals. Discrete Mathematics, 106, pp.337-342.

[2] Carlet, C., Mesnager, S., Tang, C., Qi, Y. and Pellikaan, R., 2018. Linear Codes Over F_q Are Equivalent to LCD Codes for q> 3. IEEE Transactions on Information Theory, *64*(4), pp.3010-3017.

[3] Dougherty, S.T., Kim, J.L., Ozkaya, B., Sok, L. and Solé, P., 2017. The combinatorics of LCD codes: Linear Programming bound and orthogonal matrices. International Journal of Information and Coding Theory, 4(2-3), pp.116-128.

[4] Zhou, Z., Li, X., Tang, C. and Ding, C., 2018. Binary LCD codes and self-orthogonal codes from a generic construction. IEEE Transactions on Information Theory, 65(1), pp.16-27.

[5] Galindo, C., Geil, O., Hernando, F. and Ruano, D., 2018. New binary and ternary LCD codes. IEEE Transactions on Information Theory, 65(2), pp.1008-1016.

[6] Li, C., Ding, C. and Li, S., 2017. LCD cyclic codes over finite fields. IEEE Transactions on Information Theory, 63(7), pp.4344-4356.

[7] Galvez, L., Kim, J.L., Lee, N., Roe, Y.G. and Won, B.S., 2018. Some bounds on binary LCD codes. Cryptography and Communications, 10(4), pp.719-728.

[8] Sok, L., Shi, M. and Solé, P., 2018. Constructions of optimal LCD codes over large finite fields. Finite Fields and Their Applications, 50, pp.138-153.

[9] Araya, M., Harada, M. and Saito, K., 2021. Characterization and classification of optimal LCD codes. Designs, Codes and Cryptography, 89(4), pp.617-640.

[10] Chen, B. and Liu, H., 2017. New constructions of MDS codes with complementary duals. IEEE Transactions on Information Theory, 64(8), pp.5776-5782.

[11] Huang, X., Yue, Q., Wu, Y., Shi, X. and Michel, J., 2020. Binary primitive LCD BCH codes. Designs, Codes and Cryptography, 88(12), pp.2453-2473.

[12] Fu, Q., Li, R., Fu, F. and Rao, Y., 2019. On the construction of binary optimal LCD codes with short length. International Journal of Foundations of Computer Science, 30(08), pp.1237-1245.

[13] Carlet, C., Güneri, C., Özbudak, F. and Solé, P., 2018. A new concatenated type construction for LCD codes and isometry codes. Discrete Mathematics, 341(3), pp.830-835.

[14] Benbelkacem, N., Borges, J., Dougherty, S.T. and Fernández-Córdoba, C., 2020. On Z2Z4-additive complementary dual codes and related LCD codes. Finite Fields and Their Applications, *62*, p.101622.

[15] Rao, Y., Li, R., Lv, L., Chen, G. and Zuo, F., 2017. On binary LCD cyclic codes. Procedia Computer Science, 107, pp.778-783.

[16] Carlet, C. and Guilley, S., 2016. Complementary dual codes for counter-measures to side-channel attacks. Advances in Mathematics of Communications, 10(1), p.131.

[17] Pang, B., Zhu, S. and Kai, X., 2020. Some new bounds on LCD codes over finite fields. Cryptography and Communications, pp.1-13.

[18] Araya, M., Harada, M. and Saito, K., 2019. On the minimum weights of binary LCD codes and ternary LCD codes. arXiv preprint arXiv:1908.08661.

[19] Crnković, D., Egan, R., Rodrigues, B.G. and Švob, A., 2021. LCD codes from weighing matrices. Applicable Algebra in Engineering, Communication and Computing, 32(2), pp.175-189.

[20] Darkunde N.S., Patil A.R., 2020, On ternary LCD codes, J. Math. Comput. Sci., 10 (2020), 2008-2014.

[21] Xu, H.Q. and Du, W., 2021. Constructions of Symplectic LCD MDS Codes. Bulletin of the Malaysian Mathematical Sciences Society, pp.1-14.

[22] Xu, H. and Du, W., 2020. On some binary symplectic self-orthogonal codes. Applicable Algebra in Engineering, Communication and Computing, pp.1-17.

[23] Ling, S. and Xing, C., 2004. Coding theory: a first course. Cambridge University Press.