Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 18-24, 2016, Albena, Bulgaria *pp. 108–110*

On LCD Codes

Javier de la Cruz delacruz@uninorte.edu.co
Universidad del Norte, Barranquilla, Colombia

Wolfgang Willems willems@ovgu.de
Otto-von-Guericke Universität, Magdeburg, Germany, and
Universidad del Norte, Barranquilla, Colombia

Abstract. We characterize group codes with complementary duals; i.e. ideals C in a group algebra KG for which $KG = C \oplus C^{\perp}$. Furthermore, in the rank metric case we give necessary conditions that a Gabidulin code in $K^{n\times n}$ has a complementary dual.

1 Introduction

Let K be a finite field and $n, m \in \mathbb{N}$. According to a definition of Jim Massey [3] a linear code $C \leq K^n$ (the classical case) or $\mathcal{C} \leq K^{m\times n}$ (the rank metric case) is called *a Linear Code with Complementary Dual* or shortly an LCD code if

$$K^n = C \oplus C^{\perp}, \quad \text{respectively} \quad K^{m\times n} = \mathcal{C} \oplus \mathcal{C}^{\perp}.$$

On K^n we use here the standard Euclidian form and on $K^{m\times n}$ the Delsarte bilinear form which is given by

$$\langle A, B\rangle = \operatorname{trace}(AB^t)$$

for $A, B \in K^{m\times n}$, where B^t denotes the transpose of the matrix B.

Classical LCD codes are of particular interest since they are asymptotically good [3], they achieve the Gilbert-Varshamov bound [4] and they play a crucial role in information protection against side channel and fault injection attacks [1]. In the latter case LCD MDS codes are the most powerful. Note that LCD codes are somehow opposite of self-dual codes.

2 Group Codes

A (right) ideal C in a group algebra KG, where G is a finite group, is called a *group code*. On KG we define a non-degenerate G-invariant K-bilinear form by $\langle g, h\rangle = \delta_{g,h}$ where $g, h \in G$. Observe that with C the dual code $C^{\perp}$ is an ideal as well since $\langle\cdot\,,\cdot\rangle$ is G-invariant. In [5] it has been proved that self-dual group codes only exist if the characteristic of K is 2 and $2 \mid |G|$. For instance, the extended binary $[24, 12, 8]$ Golay code is a self-dual group code in $\mathbb{F}_2 S_4$, where S_4 denotes the symmetric group on 4 letters, whereas the extended ternary $[12, 6, 6]$ Golay code is self-dual, but not a group code. To state the main results for LCD group codes we associate to each $a = \sum_{g \in G} a_g g \in KG$ (where $a_g \in K$) the adjoint $\hat{a} = \sum_{g \in G} a_g g^{-1}$. We call a *self-adjoint* if $a = \hat{a}$.

Theorem 1. If $C \leq KG$ is a (right) ideal in KG, then the following are equivalent.

a) C is an LCD code.

b) $C = eKG$ where $e^2 = e = \hat{e}$.
In other words, C is generated as an ideal by a self-adjoint idempotent.

With a bit knowledge from representation theory Theorem 1 directly proves the main result of [6] in which the group G is cyclic, i.e. C is a cyclic code.

Theorem 2. If $C = eKG$ with $e^2 = e = \hat{e}$ is an LCD code and $\operatorname{char} K = 2$, then the following are equivalent.

a) $\langle c, c \rangle = 0$ for all $c \in C$; i.e. C is symplectic.

b) $\langle 1, e \rangle = 0$; i.e. the coefficient of e at 1 is zero.

Thus, if $K = \mathbb{F}_2$ is the binary field, then a) means that C is an even code.

Example. Let $G = A_5$ be the alternating group on 5 letters and let $K = \mathbb{F}_2$ be the binary field. Furthermore, let e denote the sum of all elements of order 3 and 5 in G. Then the LCD code $C = eKG$ is even and has parameters $[60, 16, 18]$. The best known binary code of length 60 and dimension 16 has minimum distance 20 according to [2].

Remark. Cyclic Reed-Solomon codes of length n and dimension $0 < k < n$ over $\mathbb{F}_q$ are LCD codes if $n = q - 1$ and $q = 2^m$ (see [1], Lemma 1). The same proof also works if q is odd and k is even. In case q and k odd cyclic Reed-Solomon codes are not LCD codes.

3 Rank Metric Codes

Ideals $\mathcal{C}$ in the K-algebra $K^{n \times n}$ which are LCD codes are not of particular interest since one can easily see that the minimum distance of $\mathcal{C}$ is 1. However there exist MRD codes which are LCD.

Recall that a basis $a_1, \ldots, a_n$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is called self-dual if

$$\mathrm{tr}(a_i a_j) = \sum_{k=0}^{n-1} (a_i a_j)^{q^k} = \delta_{i,j}$$

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

Theorem 3. Let $v = (a, a^q, \ldots, a^{q^{n-1}})$ be the first row of a generator matrix defining a k-dimensional Gabidulin code in $\mathbb{F}_{q^n}^n$, where $a, a^q, \ldots, a^{q^{n-1}}$ is a self-dual (normal) basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then the corresponding rank metric code is MRD and LCD.

In the theory of finite fields it is well-known that a self-dual normal basis only exists if n is odd, or $n \equiv 2 \bmod 4$ and q is even. In case $4 \mid n$ and q even we do not know whether the class of Gabidulin codes in $\mathbb{F}_q^{n \times n}$ always contains LCD codes.

Question. Do have LCD MRD codes applications in cryptography like LCD MDS codes?

References

[1] C. Carlet and S. Guilley, Complementary Dual Codes for Counter-measures to Side-Channel Attacks. Online accessible `https://eprint.iacr.org/2015/603.pdf`

[2] M. Grassl, Bounds on the minimum distance of linear codes. Online accessible `http://www.codetables.de`

[3] J.L. Massey, Linear codes with complementary duals. A collection of contributions in honour of Jack van Lint. *Discrete Math.* 106/107 (1992), 337-342.

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

[5] W. Willems, A note on self-dual group codes. *IEEE Trans. Inf. Theory* 48 (2002), 3107-3109.

[6] X. Yang and J.L. Massey, The necessary and sufficient condition for a cyclic code to have a complementary dual. *Discrete Math.* 126 (1994), 391-393.