On LCD Codes

Wolfgang Willems

joint with J. de la Cruz

Otto-von-Guericke-Universität, Magdeburg
and Universidad del Norte, Barranquilla

ACCT 2016, Albena, June 18-24, 2016

Def. (Massey, '92)

A linear code $C \leq K^n$ (classical) or $\mathcal{C} \leq K^{m\times n}$ (rank metric) is called complementary dual or shortly an LCD code if

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

(On $K^{m\times n}$ the bilinear form is given by $\langle A, B\rangle = trace(AB^t)$)
Delsarte bilinear form

Classical LCD codes are of interest:

- (Massey, '92) They are asymptotically good.

- (Sendrier, '04) They achieve the Gilbert-Varshamov bound.

- (Carlet-Guilley, '15) They may be used as counter-measures for side channel and fault injection attacks.
  (most effective: LCD codes which are MDS)

1. LCD group codes

Theorem. (Yang-Massey, '94)
If $g(x)$ is the generator polynomial of an $[n, k]$ cyclic code C of block length n (the characteristic of K and n not necessarily coprime), then C is an LCD code if and only if $g(x)$ is self-reciprocal and all the monic irreducible factors of $g(x)$ have the same multiplicity in $g(x)$ and in $x^n - 1$.

Remark.
Cyclic codes are ideals in the group algebra
$\mathbb{F}_q G \cong F_q[x]/(x^n - 1)$ where G is a cyclic group of order n.

Problem.

Characterize LCD codes which are ideals in a group algebra KG where G is an arbitrary finite group.

- $\langle \sum_{g\in G} a_g g, \sum_{g\in G} b_g g\rangle = \sum_{g\in G} a_g b_g$.
- $\langle ah, bh\rangle = \langle a, b\rangle,\ a, b \in KG, h \in G$.
- Suppose that $C \oplus C^{\perp} = KG$ (LCD code)
- C is a projective KG-module.
- $C \cong KG/C^{\perp} \cong C^*$, hence C is a self-dual KG-module.
- (Dickson) $|G|_p \mid \dim C$, where $p = \operatorname{char} K$.

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 $e^2 = e = \widehat{e}$ $\qquad$ ($\widehat{\ }$: $g \to g^{-1}$).

For a cyclic group G we immediately get the Yang-Massey Theorem.

Theorem 2.

If $C = eKG$ with $e^2 = e = \hat{e}$ is an LCD code and $\mathrm{char}K = 2$, 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.

(If in addition $P(1) \nmid C$, then $\langle \cdot\,, \cdot \rangle|_C$ is the polarization of a G-invariant quadratic form on C.)

Example.

- $G = A_5$ and $K = \mathbb{F}_2$

- $e =$ sum of all elements of order 3 and 5.

- $C = eKG$ is a $[60, 16, 18]$ LCD code.

- Grassl: $20 \le d \le 22$ for any optimal $[60, 16]$ code.

- $\langle \cdot\, , \cdot \rangle|_C$ is symplectic, by Theorem 2.

Proposition.

There are LCD MDS group codes (i.e. Reed-Solomon codes) over $\mathbb{F}_q$ of dimension k with $0 < k < n$ and length $n = q - 1$ if

a) (Carlet-Guilley) q is even and k arbitrary

b) q is odd and k is even.

(Do not exist if q and k are odd.)

2. Rank metric LCD codes

As in section 1 we may consider rank metric LCD codes in the algebra $K^{n\times n}$ which are ideals.

Theorem 3. If $\mathcal{C} \leq A = K^{n\times n}$ is a right ideal, then the following are equivalent.

a) $\mathcal{C}$ is an LCD code.

b) $\mathcal{C} = eA$ where $e^2 = e = e^t$.

Disappointing: the minimum distance is always 1.

Def.

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

if $tr(a_i a_j) = \delta_{ij}$.

b) A basis of the form $a, a^q, \ldots, a^{q^{n-1}}$ is called normal.

Theorem. (Lempel and Weinberger '88)

$\mathbb{F}_{q^n}$ has a self-dual normal basis over $\mathbb{F}_q$ if and only if n is odd, or $n \equiv 2 \bmod 4$ and q is even.

Theorem 4.

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.
Then the corresponding rank metric code is MRD and LCD.

Warning: The converse does not hold true.
(A counterexample exists already for $n = 4$ and $q = 2$.)

Remarks:

a) In $\mathbb{F}_3^{2\times 2}$ there are two 2-dimensional Gabidulin codes, one is self-dual the other is an LCD code.
(There is no self-dual basis of $\mathbb{F}_9$ over $\mathbb{F}_3$.)

b) Let K be of characteristic 2. If $0 \neq \mathcal{C} \leq K^{m\times n}$ is an MRD and LCD code, then there exists an $A \in \mathcal{C}$ such that $\langle A, A\rangle \neq 0$; i.e., $\mathcal{C}$ is not symplectic.

Questions.

1. Are there always LCD Gabidulin codes, if $4 \mid n$ and the - characteristic of the underlying field is 2?
2. Which semifields of order $|K|^n$ in $K^{n \times n}$ give raise to an LCD code?
3. Do have LCD MRD codes applications in cryptography?