On self-dual MRD codes

Wolfgang Willems

DARNEC'15, Istanbul, Nov. 4-6, 2015

set up:

- $\mathcal{C} \leq k^{m\times n}$, linear of dimension ℓ, $k = \mathbb{F}_q$. $(m \geq n)$

- $\mathrm{d}(A, B) = \mathrm{rank}\,(A - B)$ for $A, B \in k^{m\times n}$.

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

- If $\mathcal{C} = \mathcal{C}^\perp$, then $\mathcal{C}$ is called self-dual.

- $\mathcal{C}$ is called MRD if $\mathrm{d}(\mathcal{C}) = d = n - \frac{\ell}{m} + 1$.

- If $\mathcal{C}$ is a self-dual MRD code, then $\ell = \frac{mn}{2}$ and $d = \frac{n}{2} + 1 \geq 2$.

Problem.

What can we say about self-dual MRD codes?

- Do they exist?

- If so, are they of interest?

Joint work with G. Nebe, RWTH Aachen, Germany.

Disappointing: They do not exist in characteristic 2.

Theorem 1.
Assume that $\operatorname{char} k = 2$ and $\mathcal{C} \subseteq \mathcal{C}^{\perp} \leq k^{m \times n}$. Then the all-ones matrix J is in $\mathcal{C}^{\perp}$. In particular, $\mathrm{d}(\mathcal{C}^{\perp}) = 1$.

Proof:

- $A = (a_{ij}) \in \mathcal{C}$.
- $0 = \langle A, A \rangle = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij}^2 = (\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij})^2 = \langle A, J \rangle^2$.
- $\mathrm{d}(\mathcal{C}^{\perp}) \leq \mathrm{d}(J, 0) = \operatorname{rank} J = 1$.

Example.

Let $\mathcal{C} \leq \mathbb{F}_q^{2\times 2}$ be an MRD code of dimension 2. Then $\mathcal{C} = \langle A, B \rangle$ with $A = \begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ c & d \end{pmatrix}$.

Lemma 1. $\mathcal{C}$ is a self-dual MRD code if and only if the following holds true:

(i) $-1 \notin \mathbb{F}_q^2$, i.e. $q \equiv 3 \bmod 4$ and

(ii) $a^2 + b^2 = -1$ and $(c, d) \in \{(-b, a), (b, -a)\}$.

Remark. All codes in Lemma 1 are pairwise equivalent and equivalent to Gabidulin codes of full length.

Theorem 2. (Hua, Wan; $\sim$ '50, '60)

If φ is a linear isometry of $k^{m\times n}$ $(m, n \geq 2)$ w.r.t. d$(\cdot\,,\cdot)$, then there exist $X \in \mathrm{GL}(m, k)$ and $Y \in \mathrm{GL}(n, k)$ s.t.

$$\varphi(A) = \kappa_{X,Y}(A) = XAY \quad \text{for all } A \in k^{m\times n} \qquad \text{(proper isometry)}$$

or, but only in case $m = n$,

$$\varphi(A) = \tau_{X,Y} = XA^tY \quad \text{for all } A \in k^{n\times n}$$

Remark.

If φ also preserves $\langle\cdot\,,\cdot\rangle$, then $XX^t = aI_m$ and $YY^t = a^{-1}I_n$.

Proposition.

$\mathcal{C} \leq k^{m\times n}$ with $\operatorname{char} k \neq 2$ is properly equivalent to a self-dual code if and only if the following holds:

(i) $\quad X = X^t \in \mathsf{GL}(m,k),\ Y = Y^t \in \mathsf{GL}(n,k)$

(ii) $\quad \det X, \det Y \in (k^\times)^2$

(iii) $\quad \mathcal{C}^\perp = X\mathcal{C}Y.$

Proof. Suppose that $X_0\mathcal{C}Y_0 = \mathcal{D} = \mathcal{D}^\perp$.

$0 = \text{trace}\,(X_0C_1Y_0(X_0C_2Y_0)^t) = \text{trace}\,(X_0C_1Y_0Y_0^tC_2^tX_0^t) = \text{trace}\,(X_0^tX_0C_1Y_0Y_0^tC_2^t)$

Put $X := X_0^tX_0$ and $Y := Y_0Y_0^t$. Then X and X are symmetric of square determinant and $\mathcal{C}^\perp = X\mathcal{C}Y$.

Conversely, (i) and (ii) imply $X = X_0^tX_0$ and $Y = Y_0Y_0^t$ (due to the classification of regular quadratic forms).

Main Theorem.

Let $\mathcal{C} = \mathcal{G}_{\frac{n}{2},\Gamma} \leq k^{n\times n}$ be a Gabidulin code of dimension $\frac{n^2}{2}$. Then $\mathcal{C}$ is equivalent to a self-dual Gabidulin code if and only if

$$n \equiv 2 \bmod 4 \quad \text{and} \quad q \equiv 3 \bmod 4.$$

(compare the result with Lemma 1)

To prove the main theorem we mainly need

Theorem 3. For $0 < \ell < n$ and $k = \mathbb{F}_q$ we have.

a) The group of proper automorphisms of $\mathcal{G}_{\ell,\Gamma} \leq k^{n\times n}$ is

$$\mathrm{Aut}^{(p)}(\mathcal{G}_{\ell,\Gamma}) = \{\kappa_{X,Y} \mid (X,Y) \in (A^j\mathcal{G}_{1,\Gamma}^{\times} \times A^{-j}\mathcal{G}_{1,\Gamma}^{\times}), \\ 0 \leq j \leq n-1\}$$

b) $\mathrm{Aut}(\mathcal{G}_{\ell,\Gamma}) = \langle \mathrm{Aut}^{(p)}(\mathcal{G}_{\ell,\Gamma}), \tau_{T^{-1},TA^{\ell-1}} \rangle$

c) $|\mathrm{Aut}(\mathcal{G}_{\ell,\Gamma})| = 2n(q^n-1)\frac{q^n-1}{q-1}$.

(Note: $\mathcal{G}_{1,\Gamma}^{\times} = \langle S \rangle$, Singer cycle, $\det S \notin (k^{\times})^2$)

Lemma 4.

$$\mathcal{G}^{\perp}_{\frac{n}{2},\Gamma} = TA^{n/2}\mathcal{G}_{\frac{n}{2},\Gamma}T^{-1}$$

, where

- $\Gamma = (\gamma, \gamma^q, \ldots, \gamma^{q^{n-1}})$
- $T = (t_{ij})$ where $t_{ij} = \text{trace}_{\,\mathbb{F}_{q^n}/\mathbb{F}_q}(\gamma^{q^{i+j}})$
- $A = \begin{pmatrix} 0 & \ldots & 0 & 1 \\ 1 & 0 & \ldots & 0 \\ 0 & \ddots & \ddots & \vdots \\ 0 & \ldots & 1 & 0 \end{pmatrix}.$

(Essentially in Berger '02 and Ravagnani '15)

Proof of the main theorem.

- Suppose that $\mathcal{C} = \mathcal{G}_{\frac{n}{2},\Gamma}$ is equiv. to a self-dual one.

(1) $\mathcal{C}$ is properly equiv. to a self-dual code:

- $C \mapsto XC^tY \in \mathcal{D} = \mathcal{D}^\perp$.

- $Y^tCX^t \in \mathcal{D}^t = (\mathcal{D}^t)^\perp$.

(2) $\mathcal{C}^\perp = TA^{n/2}\mathcal{C}T^{-1}$ (by Lemma 4)

(3) $\mathcal{C}^\perp = X\mathcal{C}Y$ with X, Y sym. and $\det X, \det Y \in (k^\times)^2$ (by Proposition).

(4) $(A^{-n/2}T^{-1}X, YT) = (A^jS^i, A^{-j}S^h) \in \mathrm{Aut}(\mathcal{C})$

(by Theorem 3)

(5) What are the conditions that there exist triples (i, j, h)

such that

$X_{i,j} = TA^{n/2+j}S^i$ and $Y_{h,j} = A^{-j}S^hT^{-1}$

are symmetric and have a square determinant.

... is equivalent to $n \equiv 2 \bmod 4$ and $q \equiv 3 \bmod 4$.

Final remarks.

- If $q \equiv 1 \bmod 4$ or $4 \mid n$ we do not know any example of a self-dual MRD code in $\mathbb{F}_q^{n\times n}$.

- Is there a self-dual MRD code in $\mathbb{F}_3^{4\times 4}$?

- (Morrison) In $\mathbb{F}_5^{4\times 2}$ there are 5 equivalence classes of self-dual MRD codes.

- Are there interesting automorphism groups in the class of self-dual MRD codes?

  $\mathrm{Aut}(\mathcal{G}_{\ell,\Gamma}) = ((C_{q^n-1} \curlyvee_{q-1} C_{q^n-1}) \rtimes C_n) \rtimes \langle t \rangle, \quad (t \neq 1 = t^2)$