# Some Non-Gabidulin MRD Codes

Kamil Otal and Ferruh Özbudak

Middle East Technical University

Algebraic combinatorics and applications, ALCOMA15
(Conference in memory of Axel Kohnert)
March 15-20, 2015 / Kloster Banz, Germany.

# Outline

## Rank metric codes

- Let $\mathbb{F}_q^{m\times n}$ be the set of $m \times n$ matrices over $\mathbb{F}_q$.
- Assume $m \leq n$ w.l.o.g.
- The **rank distance** on $\mathbb{F}_q^{m\times n}$ is the metric

$$d(A, B) = rank(A - B)$$

  for all $A, B \in \mathbb{F}_q^{m\times n}$.
- A **rank metric code** is a nonempty subset $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ with this distance.
- The **minimum distance** of a code $\mathcal{C}$ is

$$d(\mathcal{C}) = \min\{d(A, B) : A, B \in \mathcal{C} \text{ and } A \neq B\}.$$

## Rank metric codes

- If a rank metric code $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ is linear, then

  $$d(\mathcal{C}) = \min\{rank(A) : A \in \mathcal{C} \text{ and } A \neq 0\}.$$

  In some studies, $rank(A)$ is called the **rank weight** of $A$ and is denoted by $wt(A)$.
- The **equivalence** of two rank metric codes $\mathcal{C}, \mathcal{C}' \subseteq \mathbb{F}_q^{m \times n}$:

  $$\mathcal{C} \approx \mathcal{C}' \Leftrightarrow \mathcal{C}' = X\mathcal{C}Y$$

  for some $X \in GL(\mathbb{F}_q, m)$ and $Y \in GL(\mathbb{F}_q, n)$.

## Rank metric codes

### Remark

Equivalence notion in the literature[a]:

- Case $m \neq n$: $\mathcal{C} \approx \mathcal{C}' \Leftrightarrow \mathcal{C}' = X\mathcal{C}Y$ for some $X \in GL(\mathbb{F}_q, m)$ and $Y \in GL(\mathbb{F}_q, n)$,
- Case $m = n$: $\mathcal{C} \approx \mathcal{C}' \Leftrightarrow \mathcal{C}' = X\mathcal{C}Y$ or $X\mathcal{C}^tY$ for some $X, Y \in GL(\mathbb{F}_q, n)$

due to the related result of Morrison[b], where $\mathcal{C}^t$ denotes the set of transpose elements.

[a] J. Cruz, M. Kiermaier, A. Wassermann and W. Willems, *Algebraic structures of MRD codes*, preprint.

[b] K. Morrison, *Equivalence of rank-metric and matrix codes and automorphism groups of Gabidulin codes*, ArXiv:1304.0501v1, 2013.

## MRD codes

- **Singleton-like bound:**

$$|\mathcal{C}| \leq q^{n(m-d(\mathcal{C})+1)}.$$

  This bound is the $q$-analogue of Singleton bound.
- If this bound is met, then the code is called **maximum rank distance (MRD) code**. MRD codes are the $q$-analogue of MDS codes.
- There is an important class of linear MRD codes, **Gabidulin codes**[1], which is the $q$-analogue of RS codes.

[1] E. M. Gabidulin, *The theory with maximal rank metric distance*, Probl. Inform. Transm., 21, pp. 1-12, 1985.

## Gabidulin codes

### Theorem & Definition of Gabidulin Codes[a]

[a] E. M. Gabidulin, *The theory with maximal rank metric distance*, Probl. Inform. Transm., 21, pp. 1-12, 1985.

Let

- $0 < k \leq m$,
- $\alpha_1, \ldots, \alpha_m \in \mathbb{F}_{q^n}$ be $\mathbb{F}_q$-linearly independent elements,
- $\theta : \mathbb{F}_{q^n} \to \mathbb{F}_q^n$ be the coordinate transformation

$$c_1\beta_1 + c_2\beta_2 + \ldots + c_n\beta_n \mapsto (c_1, c_2, \ldots, c_n)$$

with respect to a fixed $\mathbb{F}_q$-basis $\{\beta_1, \beta_1, \ldots, \beta_n\}$ of $\mathbb{F}_{q^n}$,

## Gabidulin codes

### Theorem & Definition of Gabidulin Codes (Continued)

- $\mathcal{L}_k$ be the set of linearized polynomials over $\mathbb{F}_{q^n}$ of degree less than $q^k$, i.e.

$$\mathcal{L}_k = \{a_0 T + \ldots + a_{k-1} T^{q^{k-1}} : a_0, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\}.$$

Then the set

$$\mathcal{C} = \{ \begin{bmatrix} \theta(f(\alpha_1)) \\ \vdots \\ \theta(f(\alpha_m)) \end{bmatrix} : f \in \mathcal{L}_k\} \subseteq \mathbb{F}_q^{m \times n}$$

is an $\mathbb{F}_q$-linear rank metric code with $d(\mathcal{C}) = m - k + 1$ and $|\mathcal{C}| = q^{nk}$, i.e. a linear MRD code.

## Gabidulin codes

### Proposition

Let $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ be a Gabidulin code with the notations in the previous theorem.

- Multiplying $\mathcal{C}$ with an invertible matrix from the left corresponds to alter $\mathbb{F}_q$-linearly independent elements $\alpha_1, ..., \alpha_m \in \mathbb{F}_{q^n}$ to $\alpha'_1, ..., \alpha'_m \in \mathbb{F}_{q^n}$ such that both are bases of the same subspace.
- Multiplying $\mathcal{C}$ with an invertible matrix from the right corresponds to alter the $\mathbb{F}_q$-basis $\beta_1, ..., \beta_n$ of $\mathbb{F}_{q^n}$.

## Gabidulin codes

### Corollary

All Gabidulin codes $\subseteq \mathbb{F}_q^{n\times n}$ having the same minimum distance are in one equivalence class, and a code in this class is a Gabidulin code.

## Motivation and the related work

### Question

How can we produce non-Gabidulin MRD codes?

Cruz et al[2] have investigated this question and obtained very nice results especially for the full rank case (i.e. for $n = m = d(\mathcal{C})$):

- They have proved that there is a bijective correspondence between linear MRD codes and finite quasifields.
- They have linear (e.g. corresponds to semifields) and nonlinear (e.g. corresponds to nearfields) examples.

[2] J. Cruz, M. Kiermaier, A. Wassermann and W. Willems, *Algebraic structures of MRD codes*, preprint.

## Motivation and the related work

- They have also some computational results for the case $q = 3, n = m = 3, d(\mathcal{C}) = 2$. They say that there are two class of linear MRD codes, one of them is Gabidulin. For the other one they have a basis

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 2 & 0 & 2 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 2 & 2 \end{pmatrix}.$$

  They have asked for a way to produce such codes. This was our the main motivation.

## Linearized polynomials and rank metric codes

In our approach, one of the main ideas we use:

**Fact**

There is a one to one correspondence between a matrix of dimension $m \times n$ over $\mathbb{F}_q$ and a linearized polynomial map $V \to \mathbb{F}_{q^n}$ (up to a fixed $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$) where $V$ is an $m$-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$ .

## Linearized polynomials and rank metric codes

### Example

The set

$$\mathcal{C} = span_{\mathbb{F}_{q^n}}\{T, T^q, ..., T^{q^{k-1}}\} \subseteq \mathbb{F}_{q^n}[T],$$

or equivalently

$$\begin{aligned}\mathcal{C} \quad = span_{\mathbb{F}_q}\{ \quad & \beta_1 T, \beta_2 T, ..., \beta_n T, \\ & \beta_1 T^q, \beta_2 T^q, ..., \beta_n T^q, \\ & \vdots \\ & \beta_1 T^{q^{k-1}}, \beta_2 T^{q^{k-1}}, ..., \beta_n T^{q^{k-1}}\}\end{aligned}$$

is a Gabidulin code with $d(\mathcal{C}) = m - k + 1$, where $\{\beta_1, ..., \beta_n\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$.

## Linearized polynomials and rank metric codes

This example indicates an important property of Gabidulin codes: Gabidulin codes are not only $\mathbb{F}_q$-linear but also $\mathbb{F}_{q^n}$-linear. Therefore, if we want to construct a non-Gabidulin MRD code, then it makes sense to search for ones which are $\mathbb{F}_q$-linear but not $\mathbb{F}_{q^n}$-linear.

## Linearized combination

This example says something more: Consider the Gabidulin codes in the previous example as

$$\{x_0 T + x_1 T^q + \ldots + x_{k-1} T^{q^{k-1}} + 0 T^{q^k} + \ldots + 0 T^{q^{n-1}} : x_0, \ldots, x_{k-1} \in \mathbb{F}_{q^n}\}.$$

Here the coefficients can be considered as independent variables. In that way, take the set

$$\left\{ \sum_{i=0}^{n-1} L_i(x_0, \ldots, x_{k-1}) T^{q^i} : x_0, \ldots, x_{k-1} \in \mathbb{F}_{q^n} \right\}$$

where each $L_i$ is a multivariable linearized polynomial for all $0 \leq i \leq n-1$. We will call this procedure as $\mathbb{F}_{q^n}$-linearized combination of $T^{q^i}$s.

## Multivariable linearized polynomials

Remark that multivariable linearized polynomials have no mixed terms [3]. That is, they are of the form

$$L(x_1, ..., x_k) = L_1(x_1) + ... + L_k(x_k)$$

where $L_i$ is a linearized polynomial in one variable for all $i = 1, ..., k$.

### Example

All linear maps $(\mathbb{F}_{q^2})^2 \to \mathbb{F}_{q^2}$ are of the form

$$L(x, y) = a_0 x + a_1 x^q + b_0 y + b_1 y^q \in \mathbb{F}_{q^2}[x, y]$$

where $a_0, a_1, b_0, b_1 \in \mathbb{F}_{q^2}$.

[3] J. Berson, *Linearized polynomial maps over finite fields*, Journal of Algebra 399, pp. 389 – 406, 2014.

## Construction of MRD codes via linearized combinations

### Proposition

Consider the linearized polynomial

$$C_{x_1,\dots,x_k}(T) = \sum_{i=0}^{n-1} L_i(x_1,\dots,x_k) T^{q^i} \in \mathbb{F}_{q^n}[T]$$

where $L_i$ is a multivariable linearized polynomial in $\mathbb{F}_{q^n}[x_1,\dots,x_k]$ which maps $(\mathbb{F}_{q^n})^k \to \mathbb{F}_{q^n}$ for all $i = 0, 1, \dots, n-1$. Let

- $\phi : (\mathbb{F}_{q^n})^k \to \mathbb{F}_{q^n}[T]$ given by $(x_1,\dots,x_k) \mapsto C_{x_1,\dots,x_k}(T)$ be one to one, and
- $dim_{\mathbb{F}_q}(kernel(C_{x_1,\dots,x_k}(T))) \leq k-1$ for all $x_1,\dots,x_k \in \mathbb{F}_{q^n}$ which are not all zero.

## Construction of MRD codes via linearized combinations

**Proposition (Continued)**

Then the set

$$\{C_{x_1,\dots,x_k}(T) : x_1,\dots,x_k \in \mathbb{F}_{q^n}\} \subseteq \mathbb{F}_{q^n}[T]$$

corresponds to a linear MRD code $\mathcal{C} \subseteq \mathbb{F}_q^{n\times n}$ with $|\mathcal{C}| = q^{nk}$ and $d(\mathcal{C}) = n - k + 1$.

## Construction of MRD codes via linearized combinations

### Proposition

Consider two codes with the linearized combinations $C^{(1)}_{x_1,\ldots,x_k}(T)$ and $C^{(2)}_{x_1,\ldots,x_k}(T)$ as in the previous theorem. These codes are equivalent if and only if there exist linearized permutation polynomial maps $A(T), B(T) : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ such that

$$A(T) \circ C^{(1)}_{x_1,\ldots,x_k}(T) \circ B(T) = C^{(2)}_{u_1,\ldots,u_k}(T)$$

with some one to one mapping

$$(x_1, \ldots, x_k) \mapsto (u_1, \ldots, u_k)$$

where $\circ$ denotes the composition of functions.

## A family of MRD codes for $k = 2$

### Theorem

Let $\alpha, \beta \in \mathbb{F}_{q^3}$ such that $Norm_{q^3/q}(\alpha) \neq 1$ and $Norm_{q^3/q}(\beta) \neq 1$. The set

$$C^\alpha = \{C^\alpha_{x,y}(T) = xT + yT^q + \alpha y^{q^2} T^{q^2} : x, y \in \mathbb{F}_{q^3}\} \subseteq \mathbb{F}_{q^3}[T].$$

corresponds to a linear MRD code $\mathcal{C} \subseteq \mathbb{F}_q^{3\times 3}$ with $|\mathcal{C}| = q^6$ and $d(\mathcal{C}) = 2$. Moreover,

- If $\alpha = 0$ then it is Gabidulin.
- If $Norm_{q^3/q}(\alpha) \neq Norm_{q^3/q}(\beta)$ then $C^\alpha$ and $C^\beta$ corresponds to non-equivalent codes.
- If $Norm_{q^3/q}(\alpha) = Norm_{q^3/q}(\beta)$ then $C^\alpha$ and $C^\beta$ corresponds to equivalent codes.

## A family of MRD codes for $k = 2$

### Sketch of the Proof

Obviously the set

$$C^\alpha = \{C^\alpha_{x,y}(T) = xT + yT^q + \alpha y^{q^2} T^{q^2} : x, y \in \mathbb{F}_{q^3}\}$$

is $\mathbb{F}_q$-linear, and it is Gabidulin when $\alpha = 0$. Moreover,

$$\begin{array}{rccc} \phi : & \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} & \to & \mathbb{F}_{q^3}[T] \\ & (x, y) & \mapsto & C^\alpha_{x,y}(T) \end{array}$$

is one to one, i.e. that implies $C^\alpha$ has $q^6$ elements.

# A family of MRD codes for $k = 2$

## Sketch of the Proof (Continued)

Additionally,

$$rank_{\mathbb{F}_q}(xT + yT^q + \alpha y^{q^2} T^{q^2}) \geq 2$$

when $x$ and $y$ are not both zero. To see it, observe that the Dickson matrix

$$\begin{bmatrix} x & y & \alpha y^{q^2} \\ \alpha^q y & x^q & y^q \\ y^{q^2} & \alpha^{q^2} y^q & x^{q^2} \end{bmatrix}$$

of it can not have rank 1 since $Norm_{q^3/q}(\alpha) \neq 1$. Therefore, it is $\mathbb{F}_q$-linear MRD.

## A family of MRD codes for $k = 2$

### Sketch of the Proof (Continued)

When $Norm_{q^3/q}(\alpha) = Norm_{q^3/q}(\beta)$, let $\alpha = \gamma^r$ and $\beta = \gamma^s$ for some integers $r$ and $s$ and a primitive element $\gamma \in \mathbb{F}_{q^3}$.
$Norm_{q^3/q}(\alpha) = Norm_{q^3/q}(\beta)$ implies

$$\gamma^{(r-s)(q^2+q+1)} = 1$$

and thus $q - 1 | r - s$, i.e. $r = s + (q-1)t$ for some integer $t$.
Therefore,

$$A(T) = \gamma^{s-t} T^{q^2} \text{ and } B(T) = T^q$$

can be used to show the equivalence in case $Norm_{q^3/q}(\alpha) = Norm_{q^3/q}(\beta)$. Here, $(u, v) = (\gamma^{s-t} x^{q^2}, \gamma^{s-t} y^{q^2})$.

# A family of MRD codes for $k = 2$

## Sketch of the Proof (Continued)

When $Norm_{q^3/q}(\alpha) \neq Norm_{q^3/q}(\beta)$, assume there exist linearized permutation polynomials $A(T) = a_0 T + a_1 T^q + a_2 T^{q^2},\ B(T) = b_0 T + b_1 T^q + b_2 T^{q^2} \in \mathbb{F}_{q^3}[T]$ such that

$$A(T) \circ (xT + yT^q + \alpha y^{q^2} T^{q^2}) \circ B(T) = (uT + vT^q + \beta v^{q^2} T^{q^2})$$

for some one to one correspondence $(x, y) \leftrightarrow (u, v)$. Then, use the property

$$\beta(\text{the coefficient of } T^q)^{q^2} = (\text{the coefficient of } T^{q^2})$$

## A family of MRD codes for $k = 2$

### Sketch of the Proof (Continued)

and thus obtain the equation system

**(1)** $\beta^q a_0 b_0^q + \beta^q \alpha^q a_1 b_1 = \alpha^q a_0^q b_0 + a_2^q b_2^q,$

**(2)** $\beta^q a_1 b_2^{q^2} + \beta^q \alpha^{q^2} a_2 b_0^q = \alpha^{q^2} a_1^q b_2^q + a_0^q b_1^{q^2},$

**(3)** $\beta^q a_2 b_1 + \beta^q \alpha a_0 b_2^{q^2} = \alpha a_2^q b_1^{q^2} + a_1^q b_0,$

**(4)** $\beta^q a_0 b_1 = a_2^q b_0,$

**(5)** $\beta^q a_1 b_0^q = a_0^q b_2^q,$

**(6)** $\beta^q a_2 b_2^{q^2} = a_1^q b_1^{q^2}.$

## A family of MRD codes for $k = 2$

### Sketch of the Proof (Continued)

When we examine this system in each one of the cases

- Case 1: $a_0 = 0$ and $a_1 = 0$,
- Case 2: $a_0 \neq 0$ and $a_1 = 0$,
- Case 3: $a_0 = 0$ and $a_1 \neq 0$,
- Case 4: $a_0 \neq 0$ and $a_1 \neq 0$

## A family of MRD codes for $k = 2$

### Sketch of the Proof (Continued)

we will obtain that

- $A(T) = 0$ (i.e. it is not permutation)
- or $B(T) = 0$ (i.e. it is not permutation)
- or $Norm_{q^3/q}(\alpha) = 1$
- or $Norm_{q^3/q}(\beta) = 1$
- or $Norm_{q^3/q}(\alpha) = Norm_{q^3/q}(\beta)$

i.e. some contradiction at the end of each case.

## A family of MRD codes for $k = 2$

### Sketch of the Proof (Continued)

For example, in Case 4 (i.e. for $a_0 \neq 0$ and $a_1 \neq 0$) we have

- If $b_1 = 0$: By (4) we have $a_2 = 0$ or $b_0 = 0$.
  - If $b_0 = 0$ then $b_2 = 0$ by (5), that is $B(T) = 0$.
  - If $b_0 \neq 0$ then $a_2 = 0$ by (4) and then $b_2 \neq 0$ by (5). It implies $Norm_{q^3/q}(\alpha) = Norm_{q^3/q}(\beta)$ by (1).
- If $b_1 \neq 0$: (4) implies $a_2 \neq 0$ and $b_0 \neq 0$. Also, (6) implies $b_2 \neq 0$. Then, using (4,5,6) and some arithmetic manipulations we obtain $Norm_{q^3/q}(\beta) = 1$.

Therefore, they are not equivalent when

$$Norm_{q^3/q}(\alpha) \neq Norm_{q^3/q}(\beta).$$

## A family of MRD codes for $k = 2$

### Corollary

When $n = m = 3$, there exist at least $q - 1$ distinct (i.e. mutually nonequivalent) linear MRD codes with the minimum distance 2 for all prime power $q$.

### Example

- If $q = 2$ then we can produce only Gabidulin ones. Actually there is no non-Gabidulin linear MRD ones (easily provable computationally).

## A family of MRD codes for $k = 2$

### Example (Continued)

- If $q = 3$ there is at least one non-Gabidulin MRD code $\mathcal{C} \subseteq \mathbb{F}_3^{3\times 3}$ with $d(\mathcal{C}) = 2$. And a sample of it corresponds to

$$\{xT + yT^q + 2y^{q^2}T^{q^2} : x, y \in \mathbb{F}_{q^3}\} \subseteq \mathbb{F}_{q^3}[T]$$

  where $q = 3$. In that way, we have also given a solution to our motivative problem[a]. Remark that they computationally proved there is not another non-Gabidulin linear MRD class.

[a] J. Cruz, M. Kiermaier, A. Wassermann and W. Willems, *Algebraic structures of MRD codes*, preprint.

## Finally...

Thank you very much.

Any questions?