Characterizations of MRD and Gabidulin codes

Anna-Lena Trautmann

University of Zurich

March 16th, 2015
ALCOMA 15, Kloster Banz

In collaboration with Kyle Marshall.

Introduction

- *Rank-distance codes* are matrix codes $C \subseteq \mathbb{F}_q^{m \times n}$, equipped with the rank distance

$$d_R(A, B) = \operatorname{rank}(A - B).$$

They are useful in network coding, distributed storage ect.

Introduction

- *Rank-distance codes* are matrix codes $C \subseteq \mathbb{F}_q^{m\times n}$, equipped with the rank distance

$$d_R(A, B) = \operatorname{rank}(A - B).$$

  They are useful in network coding, distributed storage ect.
- Singleton bound for linear rank-distance codes $C \subseteq \mathbb{F}_q^{m\times n}$ of dimension k:

$$d_{\min}(C) \leq \min(m, n) - \max(m, n)k + 1.$$

Introduction

- *Rank-distance codes* are matrix codes $C \subseteq \mathbb{F}_q^{m\times n}$, equipped with the rank distance

$$d_R(A, B) = \operatorname{rank}(A - B).$$

  They are useful in network coding, distributed storage ect.
- Singleton bound for linear rank-distance codes $C \subseteq \mathbb{F}_q^{m\times n}$ of dimension k:

$$d_{\min}(C) \leq \min(m, n) - \max(m, n)k + 1.$$

- Codes that attain this bound exist for any set of parameters and are called *maximum rank distance (MRD) codes.*

- Until recently the only known MRD codes were *Gabidulin codes* (Delsarte '73, Gabidulin '85).

- Until recently the only known MRD codes were *Gabidulin codes* (Delsarte '73, Gabidulin '85).
- This year we know about other MRD codes:
  - John Sheekey presented a construction related to semi-fields at BIRS workshop in January (and today).
  - The previous talk by Wolfgang Willems et al.
  - The previous talk by Kamil Otal, Ferruh Özbudak.

- Until recently the only known MRD codes were *Gabidulin codes* (Delsarte '73, Gabidulin '85).
- This year we know about other MRD codes:
  - John Sheekey presented a construction related to semi-fields at BIRS workshop in January (and today).
  - The previous talk by Wolfgang Willems et al.
  - The previous talk by Kamil Otal, Ferruh Özbudak.
- *Our contribution*: We will give some general characterizations of linear MRD and Gabidulin codes. The results give rise to equations one can solve to find all MRD or Gabidulin codes (up to equivalence).

- Since $\mathbb{F}_q^{m\times n} \cong \mathbb{F}_{q^m}^n$, any rank-metric code over the base field can also be considered as a block code over the extension field.

- Since $\mathbb{F}_q^{m\times n} \cong \mathbb{F}_{q^m}^n$, any rank-metric code over the base field can also be considered as a block code over the extension field.
- We will assume $n \leq m$ and study MRD codes $C \subseteq \mathbb{F}_{q^m}^n$ that are $\mathbb{F}_{q^m}$-linear. These codes have a generator matrix $G \in \mathbb{F}_{q^m}^{k\times n}$ and a respective parity check matrix $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$.

Example

Let $\mathbb{F}_2^2 = \mathbb{F}_2[\alpha]$ and

$$G = (1, \alpha).$$

Then the code generated by G is

$$C = \{(0,0), (1,\alpha), (\alpha, \alpha^2), (\alpha^2, 1)\}$$

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

It has dimension 1 (over $\mathbb{F}_{2^2}$) and minimum rank distance 2 (over $\mathbb{F}_2$). A respective parity check matrix is

$$H = (\alpha, 1).$$

Known characterization of the MRD property

Theorem (Gabidulin)

Let $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$ *be a parity check matrix of the code* C*. Then* C *is MRD if and only if*

$$\operatorname{rank}(VH^T) = n - k$$

for all $V \in \mathbb{F}_q^{(n-k)\times n}$ *with* $\operatorname{rank}(V) = n - k$*.*

Known characterization of the MRD property

Theorem (Gabidulin)

Let $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$ *be a parity check matrix of the code* C*. Then* C *is MRD if and only if*

$$\operatorname{rank}(VH^T) = n - k$$

for all $V \in \mathbb{F}_q^{(n-k)\times n}$ *with* $\operatorname{rank}(V) = n - k$*.*

Simplification: Since $\mathrm{GL}_{n-k}(q)$ does not change the rank of VH^T, it suffices to check the rank property for all elements of the left orbit of H^T under $\mathcal{G}_q(n-k, n)$ (i.e. only V in reduced row echelon form).

Towards a new characterization of the MRD property

It is known that $\mathrm{GL}_n(q)$ acts (on the right) as an isometry on rank-metric codes in $\mathbb{F}_{q^m}^n$. $\Longrightarrow$

Lemma

The orbit under $\mathrm{GL}_n(q)$ of an MRD code in $\mathbb{F}_{q^m}^n$ consists of just MRD codes.

Towards a new characterization of the MRD property

It is known that $\mathrm{GL}_n(q)$ acts (on the right) as an isometry on rank-metric codes in $\mathbb{F}_{q^m}^n$. $\Longrightarrow$

Lemma

The orbit under $\mathrm{GL}_n(q)$ of an MRD code in $\mathbb{F}_{q^m}^n$ consists of just MRD codes.

Lemma

The generator matrix G of an MRD code $C \subseteq \mathbb{F}_{q^m}^n$ of dimension k in reduced row echelon form is of the form

$$G = \left(\begin{array}{c|c} I_k & A \end{array} \right),$$

where $A \in (\mathbb{F}_{q^m} \setminus \mathbb{F}_q)^{k \times (n-k)}$.

Theorem

A generator matrix $G \in \mathbb{F}_{q^m}^{k \times n}$ gives rise to an MRD code if and only if any element of the orbit of G under $\mathrm{GL}_n(q)$ has only non-zero maximal minors.

Theorem

A generator matrix $G \in \mathbb{F}_{q^m}^{k \times n}$ gives rise to an MRD code if and only if any element of the orbit of G under $\mathrm{GL}_n(q)$ has only non-zero maximal minors.

Simplification: Instead of all of $\mathrm{GL}_n(q)$ it suffices to study the orbit of the subgroup of

- the upper triangular matrices (since swapping columns does not change the minors, up to sign)
- with an all-1 diagonal (since multiplying columns of the generator matrix with $\mathbb{F}_q^*$-scalars does not change the non-zero property of the minors).

Definition

Let $g_1, \ldots, g_n \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$. The code with generator matrix

$$G = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^q & g_2^q & \cdots & g_n^q \\ g_1^{q^2} & g_2^{q^2} & \cdots & g_n^{q^2} \\ \vdots & \vdots & & \vdots \\ g_1^{q^{k-1}} & g_2^{q^{k-1}} & \cdots & g_n^{q^{k-1}} \end{pmatrix}$$

is called a *Gabidulin code* of length n and dimension k.

Definition

Let $g_1, \ldots, g_n \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$. The code with generator matrix

$$G = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^q & g_2^q & \cdots & g_n^q \\ g_1^{q^2} & g_2^{q^2} & \cdots & g_n^{q^2} \\ \vdots & \vdots & & \vdots \\ g_1^{q^{k-1}} & g_2^{q^{k-1}} & \cdots & g_n^{q^{k-1}} \end{pmatrix}$$

is called a *Gabidulin code* of length n and dimension k.

Theorem

Gabidulin codes are MRD codes.

Definition

Let $g_1, \ldots, g_n \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$ and $s \in \mathbb{N}$ with $\gcd(s, m) = 1$. The code with generator matrix

$$G = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{q^s} & g_2^{q^s} & \cdots & g_n^{q^s} \\ g_1^{q^{2s}} & g_2^{q^{2s}} & \cdots & g_n^{q^{2s}} \\ \vdots & \vdots & & \vdots \\ g_1^{q^{(k-1)s}} & g_2^{q^{(k-1)s}} & \cdots & g_n^{q^{(k-1)s}} \end{pmatrix}$$

is a *generalized Gabidulin code* of length n and dimension k.

Definition

Let $g_1, \ldots, g_n \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$ and $s \in \mathbb{N}$ with $\gcd(s, m) = 1$. The code with generator matrix

$$G = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{q^s} & g_2^{q^s} & \cdots & g_n^{q^s} \\ g_1^{q^{2s}} & g_2^{q^{2s}} & \cdots & g_n^{q^{2s}} \\ \vdots & \vdots & & \vdots \\ g_1^{q^{(k-1)s}} & g_2^{q^{(k-1)s}} & \cdots & g_n^{q^{(k-1)s}} \end{pmatrix}$$

is a *generalized Gabidulin code* of length n and dimension k.

Theorem

Generalized Gabidulin codes are MRD codes.

New Gabidulin criterion

Theorem

An MRD code is a Gabidulin code if and only if

$$\dim(C \cap C^q) = k - 1.$$

New Gabidulin criterion

Theorem

An MRD code is a Gabidulin code if and only if

$$\dim(C \cap C^q) = k - 1.$$

Theorem (generalized)

An MRD code is a generalized Gabidulin code with parameter s if and only if

$$\dim(C \cap C^{q^s}) = k - 1.$$

Lemma (Gabidulin)

The dual of an MRD code is an MRD code. Moreover, the dual of a Gabidulin code is a Gabidulin code.

Lemma (Gabidulin)

The dual of an MRD code is an MRD code. Moreover, the dual of a Gabidulin code is a Gabidulin code.

Easy to see:

Theorem

All MRD codes of dimension $k = 1$ are Gabidulin codes.

Lemma (Gabidulin)

The dual of an MRD code is an MRD code. Moreover, the dual of a Gabidulin code is a Gabidulin code.

Easy to see:

Theorem

All MRD codes of dimension $k = 1$ are Gabidulin codes.

Corollary

All MRD codes of dimension $k = n - 1$ are Gabidulin codes.

Lemma (Gabidulin)

The dual of an MRD code is an MRD code. Moreover, the dual of a Gabidulin code is a Gabidulin code.

Easy to see:

Theorem

All MRD codes of dimension $k = 1$ are Gabidulin codes.

Corollary

All MRD codes of dimension $k = n - 1$ are Gabidulin codes.

Corollary

All MRD codes of length $n = 1, 2, 3$ are Gabidulin codes.

First non-trivial case $n = m = 4, k = 2$

We want to find a description of all MRD codes with generator matrix in RREF

$$G = \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \end{pmatrix}, \quad a, b, c, d \in \mathbb{F}_{q^4} \backslash \mathbb{F}_q.$$

First non-trivial case $n = m = 4, k = 2$

We want to find a description of all MRD codes with generator matrix in RREF

$$G = \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \end{pmatrix}, \quad a, b, c, d \in \mathbb{F}_{q^4} \backslash \mathbb{F}_q.$$

We require that the orbit of upper-triangular matrices gives matrices with only non-zero maximal minors:

$$G \begin{pmatrix} 1 & u_1 & u_2 & u_3 \\ 0 & 1 & u_4 & u_5 \\ 0 & 0 & 1 & u_6 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & u_1 & u_2 + a & u_3 + au_6 + b \\ 0 & 1 & u_4 + c & u_5 + cu_6 + d \end{pmatrix}$$

for any $u_1, \ldots, u_6 \in \mathbb{F}_q$.

Now we want to find a description of all non-Gabidulin MRD codes. For this we need that $\dim(C \cap C^q) \neq k-1$ (and $a, b, c, d \in \mathbb{F}_{q^4} \setminus \mathbb{F}_q$):

$$\operatorname{rank} \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \\ 1 & 0 & a^q & b^q \\ 0 & 1 & c^q & d^q \end{pmatrix} \neq 3$$

$$\iff \operatorname{rank} \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \\ 0 & 0 & a^q - a & b^q - b \\ 0 & 0 & c^q - c & d^q - d \end{pmatrix} = 4$$

$$\iff (a^q - a)(d^q - d) - (b^q - b)(c^q - c) \neq 0.$$

Now we want to find a description of all non-Gabidulin MRD codes. For this we need that $\dim(C \cap C^q) \neq k-1$ (and $a, b, c, d \in \mathbb{F}_{q^4} \setminus \mathbb{F}_q$):

$$\operatorname{rank} \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \\ 1 & 0 & a^q & b^q \\ 0 & 1 & c^q & d^q \end{pmatrix} \neq 3$$

$$\iff \operatorname{rank} \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \\ 0 & 0 & a^q - a & b^q - b \\ 0 & 0 & c^q - c & d^q - d \end{pmatrix} = 4$$

$$\iff (a^q - a)(d^q - d) - (b^q - b)(c^q - c) \neq 0.$$

For non-generalized Gabidulin codes with $s = 3$ we get

$$(a^{q^3} - a)(d^{q^3} - d) - (b^{q^3} - b)(c^{q^3} - c) \neq 0.$$

We can now solve this system of equations to get non-Gabidulin MRD codes.

We can now solve this system of equations to get non-Gabidulin MRD codes.
For $q = 2$ we could not find a solution.

Theorem

All 2^4-linear MRD codes in $\mathbb{F}_{2^4}^4$ are Gabidulin codes.

We can now solve this system of equations to get non-Gabidulin MRD codes.
For $q = 2$ we could not find a solution.

Theorem

All 2^4-linear MRD codes in $\mathbb{F}_{2^4}^4$ are Gabidulin codes.

For $q = 3$ we found many solutions, e.g. (with $\alpha^4 = \alpha^3 + 1$)

$$G = \begin{pmatrix} 1 & 0 & \alpha & \alpha^2 \\ 0 & 1 & \alpha^2 & 2\alpha \end{pmatrix}.$$

Theorem

There are many non-Gabidulin 3^4-linear MRD codes in $\mathbb{F}_{3^4}^4$.

Summary and Conclusion

- We give new characterizations of MRD and Gabidulin codes.

Summary and Conclusion

- We give new characterizations of MRD and Gabidulin codes.
- With these criteria we show that all q^m-liner MRD codes in $\mathbb{F}_{q^m}^n$ are (generalized) Gabidulin codes if
  - $n \in \{1, 2, 3\}$
  - $k \in \{1, n-1\}$
  - $q = 2, n = m = 4, k = 2$.

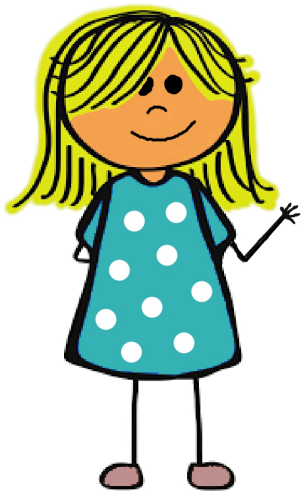
Summary and Conclusion

- We give new characterizations of MRD and Gabidulin codes.
- With these criteria we show that all q^m-liner MRD codes in $\mathbb{F}_{q^m}^n$ are (generalized) Gabidulin codes if
  - $n \in \{1, 2, 3\}$
  - $k \in \{1, n-1\}$
  - $q = 2, n = m = 4, k = 2$.
- Moreover, we give an example of a non-Gabidulin q^m-linear MRD code for $q = 3, n = m = 4, k = 2$.

Summary and Conclusion

- We give new characterizations of MRD and Gabidulin codes.
- With these criteria we show that all q^m-liner MRD codes in $\mathbb{F}_{q^m}^n$ are (generalized) Gabidulin codes if
  - $n \in \{1, 2, 3\}$
  - $k \in \{1, n-1\}$
  - $q = 2, n = m = 4, k = 2$.
- Moreover, we give an example of a non-Gabidulin q^m-linear MRD code for $q = 3, n = m = 4, k = 2$.
- This method can also be used for slightly larger parameters.

Thank you for your attention!



Questions? Comments?