Maximum Rank Distance Codes are Generic – Gabidulin Codes are Not

Anna-Lena Horlemann-Trautmann

Algorithmics Laboratory, EPF Lausanne, Switzerland

April 4th, 2016
Network Coding and Designs, Dubrovnik

joint work with Alessandro Neri, Tovohery Randrianarisoa, Joachim Rosenthal

Introduction

- Codes achieving the Singleton bound for rank metric are called *MRD (maximum rank distance) codes* .
- Known since 1978 (Delsarte)/1985 (Gabidulin): General construction for MRD codes for any set of parameters.
  $\Longrightarrow$ *Gabidulin codes*

Introduction

- Codes achieving the Singleton bound for rank metric are called *MRD (maximum rank distance) codes* .
- Known since 1978 (Delsarte)/1985 (Gabidulin): General construction for MRD codes for any set of parameters.
  $\Longrightarrow$ *Gabidulin codes*
- Until 2 years ago no really different general construction was known. Now few new results.
- In the smallest non-trivial case, all MRD codes are Gabidulin.
- Question: How many (linear) MRD codes are there and how many of those are Gabidulin codes?

Rank metric:

$$d_R(A,B) := \operatorname{rank}(A-B), \quad A,B \in \mathbb{F}_q^{m\times n}$$

$$d_R(a,b) := \operatorname{rank}(\varphi(a)-\varphi(b)), \quad a,b \in \mathbb{F}_{q^m}^n$$

with $\varphi : \mathbb{F}_{q^m}^n \to \mathbb{F}_q^{m\times n}$ isomorphism.

Definition

A linear code $C \subseteq \mathbb{F}_{q^m}^n$ of dimension k is called an *MRD (maximum rank distance) code*, if the minimum rank distance of C is equal to $n-k+1$.

Lemma

Any MRD code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension k has a generator matrix $G \in \mathbb{F}_{q^m}^{k \times n}$ in systematic form, i.e.

$$G = \left[\begin{array}{c|c} I_k & X \end{array}\right]$$

Moreover, all entries in X are from $\mathbb{F}_{q^m} \backslash \mathbb{F}_q$.

Lemma

Any MRD code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension k has a generator matrix $G \in \mathbb{F}_{q^m}^{k \times n}$ in systematic form, i.e.

$$G = \left[\begin{array}{c|c} I_k & X \end{array}\right]$$

Moreover, all entries in X are from $\mathbb{F}_{q^m} \backslash \mathbb{F}_q$.

Question: Which $X \in \mathbb{F}_{q^m}^{k(n-k)}$ generate what type of code?

MRD Criteria

Theorem (Gabidulin)

Let $G \in \mathbb{F}_{q^m}^{k \times n}$ be a generator matrix of a rank-metric code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$. Then $\mathcal{C}$ is an MRD code if and only if for any $A \in \mathbb{F}_q^{n \times k}$ of rank k, $\det(GA) \neq 0$.

MRD Criteria

Let $UT_n^*(q)$ be the subgroup of $GL_n(q)$ of upper triangular matrices with all 1 on the diagonal, i.e

$$UT_n^*(q) = \left\{ \begin{bmatrix} 1 & a_{12} & \cdots & a_{1n} \\ 0 & 1 & & a_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 \end{bmatrix} \;\middle|\; a_{ij} \in \mathbb{F}_q \right\}$$

Theorem (HT-Marshall)

Let $G \in \mathbb{F}_{q^m}^{k \times n}$ be a generator matrix of a rank-metric code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$. Then $\mathcal{C}$ is an MRD code if and only if for any $A \in UT_n^*(q)$ every maximal minor of GA is non-zero.

Definition

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

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

is called a *generalized Gabidulin code*. For $s = 1$ it is a classical Gabidulin code.

For $s = 1$ it was shown by Delsarte (1978) and Gabidulin (1985) that these codes are MRD. For $s > 1$ this fact was shown by Kshevetskiy and Gabidulin (2005).

Theorem (HT-Marshall)

An MRD code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension k is a generalized Gabidulin code if and only if

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

Theorem (HT-Marshall)

An MRD code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension k is a generalized Gabidulin code if and only if

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

If $G = [I_k \mid X]$ is generator matrix, then $\dim(\mathcal{C} \cap \mathcal{C}^{(q^s)}) = k - 1$ is equivalent to

$$\begin{aligned} & \operatorname{rank} \begin{bmatrix} I_k & X \\ I_k & X^{(q^s)} \end{bmatrix} = k + 1 \\ \iff & \operatorname{rank} \begin{bmatrix} I_k & X \\ 0 & X^{(q^s)} - X \end{bmatrix} = k + 1 \\ \iff & \operatorname{rank}(X^{(q^s)} - X) = 1. \end{aligned}$$

A *generic* property is one that holds *almost everywhere*.

Definition

A property of an irreducible algebraic variety is said to be *true generically*, if it holds on a non-empty Zariski-open subset.

A *generic* property is one that holds *almost everywhere*.

Definition

A property of an irreducible algebraic variety is said to be *true generically*, if it holds on a non-empty Zariski-open subset.

Denote by $\bar{\mathbb{F}}_q$ the algebraic closure of $\mathbb{F}_q$.

Definition (Zariski topology)

The Zariski topology on $\bar{\mathbb{F}}_q^r$ can be defined by specifying its closed sets, namely as the algebraic sets:

$$V(S) = \{\boldsymbol{x} \in \mathbb{F}_q^r \mid f(\boldsymbol{x}) = 0, \forall f \in S\},$$

where S is any set of polynomials in $\mathbb{F}_q[x_1, \ldots, x_r]$.

The *open sets* in the Zariski topology on $\bar{\mathbb{F}}_q^r$ are the complements of a closed set. All sets of the form

$$O = \{\boldsymbol{x} \in \bar{\mathbb{F}}_q^r \mid f(\boldsymbol{x}) \neq 0, \forall f \in S\}$$

are open since their complement is given by

$$O^C = \{\boldsymbol{x} \in \bar{\mathbb{F}}_q^r \mid \prod_{f \in S} f(\boldsymbol{x}) = 0\},$$

which is a Zariski-closed set.

Recall that $\mathcal{C} = \text{rowspan}[I_k \mid X] \subseteq \mathbb{F}_{q^m}^n$ is an MRD code if and only if for any $A \in \mathbb{F}_q^{n \times k}$ of rank k, $\det([I_k \mid X]A) \neq 0$.
The entries of $X \in \mathbb{F}_{q^m}^{k(n-k)}$ are the variables $x_1, \dots, x_{k(n-k)}$.
Since $\det([I_k \mid X]A) \in \mathbb{F}_{q^m}[x_1, \dots, x_{k(n-k)}]$ we get in the algebraic closure:

Lemma

The set of non-MRD codes $\mathcal{C} \subseteq \bar{\mathbb{F}}_{q^m}^n$ is a Zariski-closed set.

Corollary

The set of MRD codes $\mathcal{C} \subseteq \bar{\mathbb{F}}_{q^m}^n$ is a Zariski-open set and therefore a generic set.

$\Longrightarrow$ For very large field size a random linear code is most likely an MRD code!

$\Longrightarrow$ For very large field size a random linear code is most likely an MRD code!

MRD is generic!

Recall that an MRD code $\mathcal{C} = \text{rowspan}[I_k \mid X] \subseteq \mathbb{F}_{q^m}^n$ is a generalized Gabidulin code if and only if $\text{rank}(X - X^{(q^s)}) = 1$. This condition is equivalent to (if all $x_i \notin \mathbb{F}_q$)

$$\forall 2 \times 2 - \text{submatrices M of } (X - X^{(q^s)}) : \det(M) = 0.$$

Since $\det(M) \in \mathbb{F}_{q^m}[x_1, \dots, x_{k(n-k)}]$ we get in the algebraic closure:

Recall that an MRD code $\mathcal{C} = \mathrm{rowspan}[I_k \mid X] \subseteq \mathbb{F}_{q^m}^n$ is a generalized Gabidulin code if and only if $\mathrm{rank}(X - X^{(q^s)}) = 1$. This condition is equivalent to (if all $x_i \notin \mathbb{F}_q$)

$$\forall 2 \times 2 - \text{submatrices M of } (X - X^{(q^s)}) : \det(M) = 0.$$

Since $\det(M) \in \mathbb{F}_{q^m}[x_1, \ldots, x_{k(n-k)}]$ we get in the algebraic closure:

Theorem

The set of Gabidulin codes $\mathcal{C} \subseteq \bar{\mathbb{F}}_{q^m}^n$ is a Zariski-closed subset of the set of MRD codes.

$\Longrightarrow$ For very large field size a random linear MRD code is most likely not a generalized Gabidulin code!

$\Longrightarrow$ For very large field size a random linear MRD code is most likely not a generalized Gabidulin code!

Non-Gabidulin is generic for linear MRD codes!

Lemma (Schwartz-Zippel)

Let $f \in \mathbb{F}[x_1, x_2, \ldots, x_r]$ *be a non-zero polynomial of total degree* $d \geq 0$*. Let* $S \subseteq \mathbb{F}$ *and let* $v_1, v_2, \ldots, v_r$ *be selected at random independently and uniformly from* S*. Then*

$$\Pr[f(v_1, v_2, \ldots, v_r) = 0] \leq \frac{d}{|S|}.$$

MRD Codes (with Gabidulin criterion)

Consider $G = [I_k \mid X]$ and $A \in \mathbb{F}_q^{n \times k}$ of rank k. There are $\prod_{i=0}^{k-1}(q^n - q^i) \leq q^{kn}$ many different A's. Moreover, $\det(GA)$ has degree at most k. Hence the product of all these determinants has degree at most kq^{kn}.

Theorem

The probability that a randomly chosen $X \in \mathbb{F}_{q^m}^{k(n-k)}$ generates a non-MRD code in $\mathbb{F}_{q^m}^n$ is

$$\Pr[P_{\det}(x_1, x_2, \ldots, x_{k(n-k)}) = 0] \leq \frac{kq^{kn}}{q^m} = kq^{kn-m}.$$

For $m \to \infty$ the probability goes to zero!

MRD Codes (with HT-Marshall criterion)

Consider $G = [I_k \mid X]$. The product of all maximal minors of G has degree

$$\sum_{i=0}^{k} \binom{k}{i} \binom{n-k}{k-i} i = (n-k) \binom{n-1}{k-1}.$$

On the other hand we have $|UT_n^*(q)| = q^{\frac{n(n-1)}{2}}$.

Theorem

The probability that a randomly chosen $X \in \mathbb{F}_{q^m}^{k(n-k)}$ generates a non-MRD code in $\mathbb{F}_{q^m}^n$ is

$$\Pr[P_{minor}(x_1, x_2, \ldots, x_{k(n-k)}) = 0] \leq \frac{q^{\frac{n(n-1)}{2}} (n-k)\binom{n-1}{k-1}}{q^m}.$$

For $m \to \infty$ the probability goes to zero!

Gabidulin Codes $(s = 1)$

Recall that $\mathrm{rank}(X - X^q) = 0$ cannot generate an MRD code. We have

$$\{X \mid X \text{ gen. Gabidulin}\} =$$

$$\{X \mid X \text{ gen. MRD}\} \cap \{X \mid \mathrm{rank}(X - X^q) = 1\}|.$$

Gabidulin Codes $(s = 1)$

Recall that $\mathrm{rank}(X - X^q) = 0$ cannot generate an MRD code.
We have

$$\{X \mid X \text{ gen. Gabidulin}\} =$$

$$\{X \mid X \text{ gen. MRD}\} \cap \{X \mid \mathrm{rank}(X - X^q) = 1\}|.$$

Hence

$$|\{X \mid X \text{ generates Gabidulin code}\}| \leq |\{X \mid \mathrm{rank}(X - X^q) \leq 1\}|,$$

i.e.,

$$\Pr[X \text{ generates Gabidulin code}] \leq \Pr[\underbrace{\mathrm{rank}(X - X^q) \leq 1}_{\text{if all } 2\times 2 \text{ minors are zero}}].$$

Gabidulin Codes ($s = 1$)

We will check all non-intersecting 2×2-minors M_{ij} of $(X - X^{(q)})$, of which we have $\lfloor \frac{k}{2} \rfloor \lfloor \frac{n-k}{2} \rfloor$ many. Each determinant has degree $2q$, hence

$$\Pr(M_{ij} = 0) \leq 2q^{1-m}.$$

Since these determinants are independent we get:

Theorem

The probability that a randomly chosen $X \in \mathbb{F}_{q^m}^{k(n-k)}$ generates a Gabidulin code is

$$\prod_{i,j} \Pr[M_{ij} = 0] \leq (2q^{1-m})^{\lfloor \frac{k}{2} \rfloor \lfloor \frac{n-k}{2} \rfloor}.$$

For $m \to \infty$ the probability goes to zero!

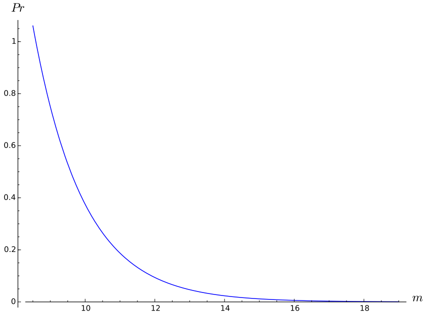
For all other $s \neq 1$ we get the same number, hence for the probability of getting any generalized Gabidulin code we need to multiply with Euler-$\phi(m)$ (since s, m are coprime).

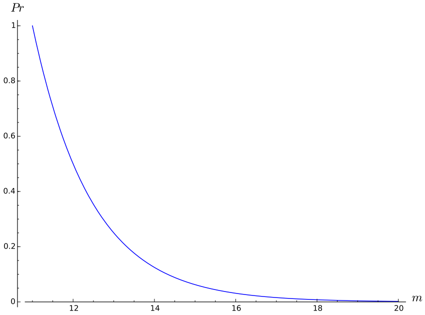
Theorem

The probability that a randomly chosen $X \in \mathbb{F}_{q^m}^{k(n-k)}$ generates a generalized Gabidulin code is upper bounded by

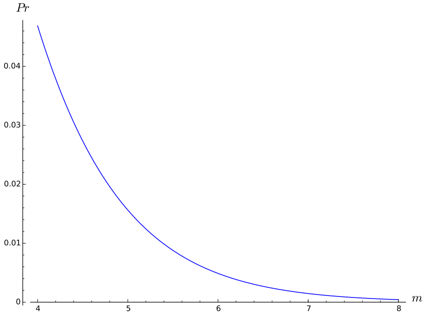
$$\phi(m)(2q^{1-m})^{\lfloor \frac{k}{2} \rfloor \lfloor \frac{n-k}{2} \rfloor} \leq (m-1)(2q^{1-m})^{\lfloor \frac{k}{2} \rfloor \lfloor \frac{n-k}{2} \rfloor}.$$

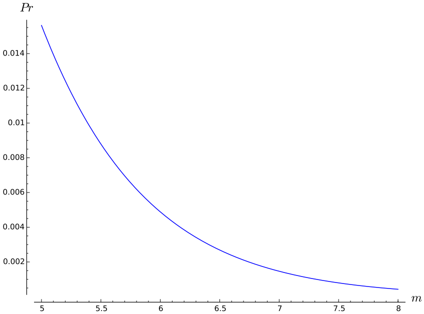
Upper bound on probabilities of non-MRD $n = 4, 5$, $k = 2, q = 2$:



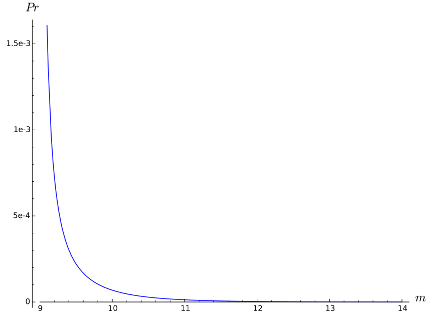


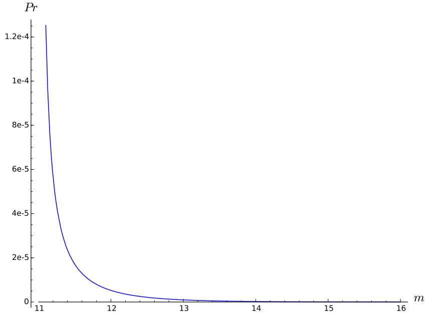
Upper bound on probabilities of generalized Gabidulin $n = 4, 5$, $k = 2, q = 2$:





Upper bound on probabilities that MRD is generalized Gabidulin $n = 4, 5,\ k = 2, q = 2$:





$$\Pr[Gab \mid MRD] = \frac{\Pr[MRD \mid Gab]\Pr[Gab]}{\Pr[MRD]} = \frac{\Pr[Gab]}{\Pr[MRD]}$$

Conclusions

- A random linear code is very likely MRD for large field size.
- A random linear code is very likely non-Gabidulin for large field size.
- Even a random linear MRD code is very likely non-Gabidulin for large field size.

Conclusions

- A random linear code is very likely MRD for large field size.
- A random linear code is very likely non-Gabidulin for large field size.
- Even a random linear MRD code is very likely non-Gabidulin for large field size.

Open question: What are all the other MRD codes out there?

Thanks for your attention!
Questions? – Comments?