On the q-Analogue of Cauchy Matrices

Alessandro Neri

17-21 June 2019 - VUB

Universität Zürich[UZH]

On the q-Analogue of Cauchy Matrices

Alessandro Neri

I am a friend of Finite Geometry!

17-21 June 2019 - VUB

Universität Zürich[UZH]

q-Analogues Model

Finite set	$\rightsquigarrow$	Finite dim vector space over $\mathbb{F}_q$
Element	$\rightsquigarrow$	1-dim subspace
$\emptyset$	$\rightsquigarrow$	$\{0\}$
Cardinality	$\rightsquigarrow$	Dimension
Intersection	$\rightsquigarrow$	Intersection
Union	$\rightsquigarrow$	Sum

Examples

1. Binomials and q-binomials:

$$\binom{n}{k} = \prod_{i=0}^{k-1} \frac{n-i}{k-i}, \qquad \binom{n}{k}_q = \prod_{i=0}^{k-1} \frac{1-q^{n-i}}{1-q^{k-i}}.$$

2. (Chu)-Vandermonde and q-Vandermonde identity:

$$\binom{m+n}{k} = \sum_{j=0}^{k} \binom{m}{j}\binom{n}{k-j}, \quad \binom{m+n}{k}_q = \sum_{j=0}^{k} \binom{m}{k-j}_q \binom{n}{j}_q q^{j(m-k+j)}.$$

3. Polynomials and q-polynomials:

$$a_0 + a_1 x + \ldots + a_k x^k, \qquad a_0 x + a_1 x^q + \ldots + a_k x^{q^k}.$$

4. Gamma and q-Gamma functions:

$$\Gamma(z+1) = z\Gamma(z), \qquad \Gamma_q(x+1) = \frac{1-q^x}{1-q}\Gamma_q(x).$$

Vandermonde Matrix

Let $k \leq n$.

$$V = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_n^{k-1} \end{pmatrix}$$

Vandermonde Matrix

Let $k \leq n$.

$$V = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_n^{k-1} \end{pmatrix}$$

For $n = k$, $\det(V) \neq 0$ if and only if the α_i's are all distinct.

$$|\{\alpha_1, \dots, \alpha_n\}| = n.$$

In particular, all the $k \times k$ minors of V are non-zero.

Moore Matrix

Let $k \leq n$.

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

Moore Matrix

Let $k \leq n$.

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

For $n = k$, $\det(G) \neq 0$ if and only if the g_i's are all $\mathbb{F}_q$-linearly independent.

$$\dim_{\mathbb{F}_q} \langle g_1, \dots, g_n \rangle_{\mathbb{F}_q} = n.$$

In particular, for every $M \in \mathrm{GL}_n(\mathbb{F}_q)$, all the $k \times k$ minors of GM are non-zero.

Moore Matrix

Let $k \leq n$, $\sigma : x \longmapsto x^q$

$$G = \begin{pmatrix} g_1 & g_2 & \dots & g_n \\ \sigma(g_1) & \sigma(g_2) & \dots & \sigma(g_n) \\ \vdots & \vdots & & \vdots \\ \sigma^{k-1}(g_1) & \sigma^{k-1}(g_2) & \dots & \sigma^{k-1}(g_n) \end{pmatrix},$$

For $n = k$, $\det(G) \neq 0$ if and only if the g_i's are all $\mathbb{F}_q$-linearly independent.

$$\dim_{\mathbb{F}_q} \langle g_1, \dots, g_n \rangle_{\mathbb{F}_q} = n.$$

In particular, for every $M \in \mathrm{GL}_n(\mathbb{F}_q)$, all the $k \times k$ minors of GM are non-zero.

Moore matrix

1. Dickson used the Moore matrix for finding the modular invariants of the general linear group over a finite field.

2. It is widely used in the study of normal bases of finite fields.

3. $$\det(G) = \prod_{1 \leq i \leq n} \prod_{c_1, \ldots, c_{i-1} \in \mathbb{F}_q} \left(c_1 g_1 + \cdots + c_{i-1} g_{i-1} + g_i \right).$$

Generalized Cauchy Matrix

(1) $x_1, \dots, x_r \in \mathbb{F}_q$ pairwise distinct,

(2) $y_1, \dots, y_s \in \mathbb{F}_q$ pairwise distinct,

(3) $y_1, \dots, y_s \in \mathbb{F}_q \setminus \{x_1, \dots, x_r\}$,

(4) $c_1, \dots, c_r, d_1, \dots, d_s \in \mathbb{F}_q^*$.

Generalized Cauchy Matrix

(1) $x_1, \dots, x_r \in \mathbb{F}_q$ pairwise distinct,

(2) $y_1, \dots, y_s \in \mathbb{F}_q$ pairwise distinct,

(3) $y_1, \dots, y_s \in \mathbb{F}_q \setminus \{x_1, \dots, x_r\}$,

(4) $c_1, \dots, c_r, d_1, \dots, d_s \in \mathbb{F}_q^*$.

The matrix $X \in \mathbb{F}_q^{r \times s}$ defined by

$$X_{i,j} = \frac{c_i d_j}{x_i - y_j}$$

is called Generalized Cauchy (GC) Matrix.

For $j \leq \min\{r, s\}$, all the $j \times j$ minors are non-zero.

Question

How to define a q-analogue of Cauchy matrices?

Generalized Reed-Solomon Codes

[Reed, Solomon '60]

- $\mathbb{F}_q[x]_{<k} := \{f(x) \in \mathbb{F}_q[x] \mid \deg f < k\}$.

Generalized Reed-Solomon Codes

[Reed, Solomon '60]

- $\mathbb{F}_q[x]_{<k} := \{f(x) \in \mathbb{F}_q[x] \mid \deg f < k\}$.

- $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ distinct elements
- $b_1, \ldots, b_n \in \mathbb{F}_q^*$
- $\mathcal{C} = \{(b_1 f(\alpha_1), b_2 f(\alpha_2), \ldots, b_n f(\alpha_n)) \mid f \in \mathbb{F}_q[x]_{<k}\}$

Generalized Reed-Solomon Codes

[Reed, Solomon '60]

- $\mathbb{F}_q[x]_{<k} := \{f(x) \in \mathbb{F}_q[x] \mid \deg f < k\}$.

- $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ distinct elements
- $b_1, \ldots, b_n \in \mathbb{F}_q^*$
- $\mathcal{C} = \{(b_1 f(\alpha_1), b_2 f(\alpha_2), \ldots, b_n f(\alpha_n)) \mid f \in \mathbb{F}_q[x]_{<k}\}$

THEN

$\mathcal{C}$ is the Generalized Reed-Solomon code $\mathrm{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{b})$

Generalized Reed-Solomon Codes

[Reed, Solomon '60]

- $\mathbb{F}_q[x]_{<k} := \{f(x) \in \mathbb{F}_q[x] \mid \deg f < k\}$.

- $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ s.t. $|\{\alpha_1, \ldots, \alpha_n\}| = n$
- $b_1, \ldots, b_n \in \mathbb{F}_q^*$
- $\mathcal{C} = \{(b_1 f(\alpha_1), b_2 f(\alpha_2), \ldots, b_n f(\alpha_n)) \mid f \in \mathbb{F}_q[x]_{<k}\}$

THEN

$\mathcal{C}$ is the Generalized Reed-Solomon code $\mathrm{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{b})$

Canonical Generator Matrix for GRS codes

Consider the canonical monomial basis $\{1, x, \ldots, x^{k-1}\}$ and evaluate it. We get the following generator matrix

Weighted Vandermonde (WV) matrix

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \ldots & \alpha_n^{k-1} \end{pmatrix} \mathrm{diag}(\mathbf{b})$$

GRS Codes and Cauchy Matrices

1. Every $[n, k]_q$ code has many generator matrices $G \in \mathbb{F}_q^{k \times n}$.

2. Every $[n, k]_q$ code has a unique generator matrix in Reduced Row Echelon Form (RREF).

GRS Codes and Cauchy Matrices

1. Every $[n, k]_q$ code has many generator matrices $G \in \mathbb{F}_q^{k \times n}$.

2. Every $[n, k]_q$ code has a unique generator matrix in Reduced Row Echelon Form (RREF).

3. If $\mathcal{C}$ is MDS the generator matrix in RREF is of the form $(I_k \mid X)$.

4. GRS codes are MDS.

GRS Codes and Cauchy Matrices

1. Every $[n, k]_q$ code has many generator matrices $G \in \mathbb{F}_q^{k\times n}$.
2. Every $[n, k]_q$ code has a unique generator matrix in Reduced Row Echelon Form (RREF).
3. If $\mathcal{C}$ is MDS the generator matrix in RREF is of the form $(I_k \mid X)$.
4. GRS codes are MDS.

GRS Codes and Cauchy Matrices

1. Every $[n,k]_q$ code has many generator matrices $G \in \mathbb{F}_q^{k\times n}$.
2. Every $[n,k]_q$ code has a unique generator matrix in Reduced Row Echelon Form (RREF).
3. If $\mathcal{C}$ is MDS the generator matrix in RREF is of the form $(I_k \mid X)$.
4. GRS codes are MDS.

Theorem [Roth, Seroussi '85]

There is a 1-1 correspondence between GC matrices and GRS codes codes given by

$$X \longleftrightarrow \mathrm{rowsp}(\ I_k \mid X\ ).$$

General Setting

- $\mathbb{F}_{q^m}$ extension field of degree m of a finite field $\mathbb{F}_q$.
- $\mathbb{F}_{q^m} \cong \mathbb{F}_q^m$ as vector spaces over $\mathbb{F}_q$.
- $\mathbb{F}_{q^m}^n \cong \mathbb{F}_q^{m \times n}$ as vector spaces over $\mathbb{F}_q$.

General Setting

- $\mathbb{F}_{q^m}$ extension field of degree m of a finite field $\mathbb{F}_q$.
- $\mathbb{F}_{q^m} \cong \mathbb{F}_q^m$ as vector spaces over $\mathbb{F}_q$.
- $\mathbb{F}_{q^m}^n \cong \mathbb{F}_q^{m\times n}$ as vector spaces over $\mathbb{F}_q$.

Rank Distance

The rank distance d_R on $\mathbb{F}_q^{m\times n}$ is defined by

$$d_R(X,Y) := \mathrm{rk}(X-Y), \quad X,Y \in \mathbb{F}_q^{m\times n}.$$

The rank distance d_R on $\mathbb{F}_{q^m}^n$ is defined by

$$d_R(u,v) := \dim\langle u_1 - v_1, u_2 - v_2, \ldots, u_n - v_n\rangle_{\mathbb{F}_q}.$$

A rank metric code $\mathcal{C}$ is a subset of $\mathbb{F}_{q^m}^n$ equipped with the rank distance.

Linearized Polynomials and Gabidulin Codes

[Delsarte '78], [Gabidulin '85], [Roth '91], [Kshevetskiy, Gabidulin '05]

- $\sum_{i=0}^{m-1} f_i x^{q^i}$ a linearized polynomial over $\mathbb{F}_{q^m}$,
- $\mathcal{G}_k := \left\{ f_0 x + f_1 x^q + \ldots + f_{k-1} x^{q^{k-1}} \mid f_i \in \mathbb{F}_{q^m} \right\}$.

Linearized Polynomials and Gabidulin Codes

[Delsarte '78], [Gabidulin '85], [Roth '91], [Kshevetskiy, Gabidulin '05]

- $\sum_{i=0}^{m-1} f_i x^{q^i}$ a linearized polynomial over $\mathbb{F}_{q^m}$,
- $\mathcal{G}_k := \left\{ f_0 x + f_1 x^q + \ldots + f_{k-1} x^{q^{k-1}} \mid f_i \in \mathbb{F}_{q^m} \right\}$.

- $g_1, \ldots, g_n \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$
- $\mathcal{C} = \{(f(g_1), f(g_2), \ldots, f(g_n)) \mid f \in \mathcal{G}_k\}$

Linearized Polynomials and Gabidulin Codes

[Delsarte '78], [Gabidulin '85], [Roth '91], [Kshevetskiy, Gabidulin '05]

- $\sum_{i=0}^{m-1} f_i x^{q^i}$ a linearized polynomial over $\mathbb{F}_{q^m}$,
- $\mathcal{G}_k := \left\{ f_0 x + f_1 x^q + \ldots + f_{k-1} x^{q^{k-1}} \mid f_i \in \mathbb{F}_{q^m} \right\}$.

- $g_1, \ldots, g_n \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$
- $\mathcal{C} = \{(f(g_1), f(g_2), \ldots, f(g_n)) \mid f \in \mathcal{G}_k\}$

THEN

$\mathcal{C}$ is the Gabidulin code $\mathcal{G}_k(g_1, \ldots, g_n)$

Linearized Polynomials and Gabidulin Codes

[Delsarte '78], [Gabidulin '85], [Roth '91], [Kshevetskiy, Gabidulin '05]

- $\sum_{i=0}^{m-1} f_i x^{q^i}$ a linearized polynomial over $\mathbb{F}_{q^m}$,
- $\mathcal{G}_k := \left\{ f_0 x + f_1 x^q + \ldots + f_{k-1} x^{q^{k-1}} \mid f_i \in \mathbb{F}_{q^m} \right\}$.

- $g_1, \ldots, g_n \in \mathbb{F}_{q^m}$ s.t. $\dim\langle g_1, \ldots, g_n \rangle_{\mathbb{F}_q} = n$.
- $\mathcal{C} = \{(f(g_1), f(g_2), \ldots, f(g_n)) \mid f \in \mathcal{G}_k\}$

THEN

$\mathcal{C}$ is the Gabidulin code $\mathcal{G}_k(g_1, \ldots, g_n)$

Canonical Generator Matrix for $\mathcal{G}_k(g_1, \ldots, g_n)$

Let

$$\begin{array}{rcl} \sigma : \mathbb{F}_{q^m} & \longrightarrow & \mathbb{F}_{q^m} \\ z & \longmapsto & z^q \end{array}$$

be the q-Frobenius automorphism.

Canonical Generator Matrix for $\mathcal{G}_k(g_1, \dots, g_n)$

Let

$$\begin{array}{rcl} \sigma : \mathbb{F}_{q^m} & \longrightarrow & \mathbb{F}_{q^m} \\ z & \longmapsto & z^q \end{array}$$

be the q-Frobenius automorphism.

Consider the canonical monomial basis $\{x, x^q, \dots, x^{q^{k-1}}\}$ and evaluate it. We get the following generator matrix

s-Moore Matrix

$$\begin{pmatrix} g_1 & g_2 & \dots & g_n \\ \sigma(g_1) & \sigma(g_2) & \dots & \sigma(g_n) \\ \vdots & \vdots & & \vdots \\ \sigma^{k-1}(g_1) & \sigma^{k-1}(g_2) & \dots & \sigma^{k-1}(g_n) \end{pmatrix},$$

Hamming vs Rank Distance: Recap

d_H

d_R

Hamming vs Rank Distance: Recap

d_H	GRS codes
d_R	

Hamming vs Rank Distance: Recap

d_H	GRS codes
	$\updownarrow$
d_R	Gabidulin codes

Hamming vs Rank Distance: Recap

d_H	GRS codes	$\longleftrightarrow$	WV matrices
	$\updownarrow$		
d_R	Gabidulin codes		

Hamming vs Rank Distance: Recap

d_H	GRS codes	$\longleftrightarrow$	WV matrices
	$\updownarrow$		$\updownarrow$
d_R	Gabidulin codes	$\longleftrightarrow$	Moore matrices

Hamming vs Rank Distance: Recap

$$
\begin{array}{c|ccccc}
\color{red}{d_H} & \text{GRS codes} & \longleftrightarrow & \text{WV matrices} & \longleftrightarrow & \text{GC matrices} \\
 & \updownarrow & & \updownarrow & & \\
\color{red}{d_R} & \text{Gabidulin codes} & \longleftrightarrow & \text{Moore matrices} & &
\end{array}
$$

Hamming vs Rank Distance: Recap

d_H	GRS codes	$\longleftrightarrow$	WV matrices	$\longleftrightarrow$	GC matrices
	$\updownarrow$		$\updownarrow$		$\updownarrow$
d_R	Gabidulin codes	$\longleftrightarrow$	Moore matrices	$\longleftrightarrow$	???

Hamming vs Rank Distance: Recap

d_H	GRS codes	$\longleftrightarrow$	WV matrices	$\longleftrightarrow$	GC matrices
	$\updownarrow$		$\updownarrow$		$\updownarrow$
d_R	Gabidulin codes	$\longleftrightarrow$	Moore matrices	$\longleftrightarrow$	???

(Possible) definition of a q-analogue of Cauchy matrices!

GRC Matrix

Let $\gamma \in \mathbb{F}_{q^m}$ such that $\mathrm{Tr}(\gamma) \neq 0$ and s be an integer coprime to m. We define the map

$$\begin{array}{rcl} \pi : \mathbb{F}_{q^m} & \longrightarrow & \mathbb{F}_{q^m} \\ \alpha & \longmapsto & -\frac{1}{\mathrm{Tr}(\gamma)} \sum_{i=0}^{m-2} \left(\sigma^{i+1}(\gamma) \sum_{j=0}^{i} (\sigma^j(\alpha)) \right) \end{array}$$

GRC Matrix

Let $\gamma \in \mathbb{F}_{q^m}$ such that $\mathrm{Tr}(\gamma) \neq 0$ and s be an integer coprime to m. We define the map

$$\begin{array}{rcl} \pi : \mathbb{F}_{q^m} & \longrightarrow & \mathbb{F}_{q^m} \\ \alpha & \longmapsto & -\frac{1}{\mathrm{Tr}(\gamma)} \sum_{i=0}^{m-2} \left(\sigma^{i+1}(\gamma) \sum_{j=0}^{i} (\sigma^j(\alpha)) \right) \end{array}$$

(1) $\alpha_1, \ldots, \alpha_k \in \mathbb{F}_{q^m}$, $\mathbb{F}_q$-linearly independent,

(2) $\beta_1, \ldots, \beta_{n-k} \in \mathbb{F}_{q^m}$, $\mathbb{F}_q$-linearly independent,

(3) $\beta_1, \ldots, \beta_{n-k} \in \langle \alpha_1, \ldots, \alpha_k \rangle_{\mathbb{F}_q}^{\times}$,

(4) $C \in \mathbb{F}_q^{k \times (n-k)}$.

GRC Matrix

Let $\gamma \in \mathbb{F}_{q^m}$ such that $\mathrm{Tr}(\gamma) \neq 0$ and s be an integer coprime to m. We define the map

$$\begin{array}{rcl} \pi : \mathbb{F}_{q^m} & \longrightarrow & \mathbb{F}_{q^m} \\ \alpha & \longmapsto & -\frac{1}{\mathrm{Tr}(\gamma)} \sum_{i=0}^{m-2} \left(\sigma^{i+1}(\gamma) \sum_{j=0}^{i} (\sigma^j(\alpha)) \right) \end{array}$$

(1) $\alpha_1, \dots, \alpha_k \in \mathbb{F}_{q^m}$, $\mathbb{F}_q$-linearly independent,
(2) $\beta_1, \dots, \beta_{n-k} \in \mathbb{F}_{q^m}$, $\mathbb{F}_q$-linearly independent,
(3) $\beta_1, \dots, \beta_{n-k} \in \langle \alpha_1, \dots, \alpha_k \rangle_{\mathbb{F}_q}^{\times}$,
(4) $C \in \mathbb{F}_q^{k \times (n-k)}$.

The matrix $X \in \mathbb{F}_{q^m}^{k \times (n-k)}$ defined by

$$X_{i,j} = \pi(\alpha_i \beta_j) + c_{i,j}$$

is a Generalized Rank-Cauchy (GRC) Matrix.

GRC Matrix

Let $\gamma \in \mathbb{F}_{q^m}$ such that $\mathrm{Tr}(\gamma) \neq 0$ and s be an integer coprime to m. We define the map

$$\begin{array}{rcl} \pi : \mathbb{F}_{q^m} & \longrightarrow & \mathbb{F}_{q^m} \\ \alpha & \longmapsto & -\frac{1}{\mathrm{Tr}(\gamma)} \sum_{i=0}^{m-2} \left(\sigma^{i+1}(\gamma) \sum_{j=0}^{i} (\sigma^j(\alpha)) \right) \end{array}$$

(1) $\alpha_1, \ldots, \alpha_k \in \mathbb{F}_{q^m}$, $\mathbb{F}_q$-linearly independent,
(2) $\beta_1, \ldots, \beta_{n-k} \in \mathbb{F}_{q^m}$, $\mathbb{F}_q$-linearly independent,
(3) $\beta_1, \ldots, \beta_{n-k} \in \langle \alpha_1, \ldots, \alpha_k \rangle_{\mathbb{F}_q}^{\times}$,
(4) $C \in \mathbb{F}_q^{k \times (n-k)}$.

The matrix $X \in \mathbb{F}_{q^m}^{k \times (n-k)}$ defined by

$$X_{i,j} = \pi(\alpha_i \beta_j) + c_{i,j}$$

is a Generalized Rank-Cauchy (GRC) Matrix.

Generalized Cauchy matrix

(1) $x_1, \dots, x_k \in \mathbb{F}_q$ pairwise distinct,

(2) $y_1, \dots, y_{n-k} \in \mathbb{F}_q$ pairwise distinct,

(3) $y_1, \dots, y_{n-k} \in \mathbb{F}_q \setminus \{x_1, \dots, x_k\}$,

(4) $c_1, \dots, c_k, d_1, \dots, d_{n-k} \in \mathbb{F}_q^*$.

The matrix $X \in \mathbb{F}_q^{k\times(n-k)}$ defined by $X_{i,j} = \frac{c_i d_j}{x_i - y_j}$ is called Generalized Cauchy (GC) Matrix.

Generalized Cauchy Matrix

(1) $x_1, \dots, x_k \in \mathbb{F}_q$ s.t. $|\{x_1, \dots, x_k\}| = k$.

(2) $y_1, \dots, y_{n-k} \in \mathbb{F}_q$ s.t. $|\{y_1, \dots, y_{n-k}\}| = n - k$.

(3) $\{y_1, \dots, y_{n-k}\} \subseteq \mathbb{F}_q \setminus \{x_1, \dots, x_k\}$,

(4) $c_1, \dots, c_k, d_1, \dots, d_{n-k} \in \mathbb{F}_q^*$.

The matrix $X \in \mathbb{F}_q^{k\times(n-k)}$ defined by $X_{i,j} = \frac{c_i d_j}{x_i - y_j}$ is called Generalized Cauchy (GC) Matrix.

GRC Matrix

Let $\gamma \in \mathbb{F}_{q^m}$ such that $\mathrm{Tr}(\gamma) \neq 0$ and s be an integer coprime to m. We define the map

$$\begin{array}{rcl} \pi : \mathbb{F}_{q^m} & \longrightarrow & \mathbb{F}_{q^m} \\ \alpha & \longmapsto & -\frac{1}{\mathrm{Tr}(\gamma)} \sum_{i=0}^{m-2} \left(\sigma^{i+1}(\gamma) \sum_{j=0}^{i} (\sigma^j(\alpha)) \right) \end{array}$$

(1) $\alpha_1, \ldots, \alpha_k \in \mathbb{F}_{q^m}$, s.t. $\dim\langle \alpha_1, \ldots, \alpha_k \rangle_{\mathbb{F}_q} = k$,

(2) $\beta_1, \ldots, \beta_{n-k} \in \mathbb{F}_{q^m}$, s.t. $\dim\langle \beta_1, \ldots, \beta_{n-k} \rangle_{\mathbb{F}_q} = n-k$.

(3) $\langle \beta_1, \ldots, \beta_{n-k} \rangle_{\mathbb{F}_q} \subseteq \langle \alpha_1, \ldots, \alpha_k \rangle_{\mathbb{F}_q}^{\times}$,

(4) $C \in \mathbb{F}_q^{k \times (n-k)}$.

The matrix $X \in \mathbb{F}_{q^m}^{k \times (n-k)}$ defined by

$$X_{i,j} = \pi(\alpha_i \beta_j) + c_{i,j}$$

is a Generalized Rank-Cauchy (GRC) Matrix.

Standard Form of Gabidulin Codes

Theorem 1 [N. '18]

There is a 1-1 correspondence between GRC matrices and Gabidulin codes given by

$$X \longleftrightarrow \mathrm{rowsp}(\ I_k \mid X\ ).$$

Standard Form of Gabidulin Codes

Theorem 1 [N. '18]

There is a 1-1 correspondence between GRC matrices and Gabidulin codes given by

$$X \longleftrightarrow \mathrm{rowsp}(\ I_k \mid X\ ).$$

For every $A \in \mathrm{GL}_k(\mathbb{F}_q)$, $B \in \mathrm{GL}_{n-k}(\mathbb{F}_q)$,
every minor of the matrix AXB is non-zero! $(\star)$

Standard form of Gabidulin codes

Standard form of Gabidulin codes

d_H	GRS codes	$\longleftrightarrow$	WV matrices	$\longleftrightarrow$	GC matrices
	$\updownarrow$		$\updownarrow$		$\updownarrow$
d_R	Gabidulin codes	$\longleftrightarrow$	Moore matrices	$\longleftrightarrow$	???

Standard form of Gabidulin codes

d_H	GRS codes	$\longleftrightarrow$	WV matrices	$\longleftrightarrow$	GC matrices
	$\updownarrow$		$\updownarrow$		$\updownarrow$
d_R	Gabidulin codes	$\longleftrightarrow$	Moore matrices	$\longleftrightarrow$	GRC matrices