On a Construction of Optimal Codes in Term Rank Metric via $p(x)$-circulants

V. V. Gritsenko[1] A. E. Maevskiy[2]

[1]Department of Mathematic, Mechanic and Computer Science
Southern Federal University, Rostov-on-Don, Russia

[2]Institute for Information Transmission Problems
Russian Academy of Sciences, Moscow, Russia

Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT 2014)
Svetlogorsk (Kaliningrad region), Russia, 7–13 September 2014

Outline

Outline

Matrix channel

Fix

- $\mathbb{F}_q$ – finite field, $q = p^a$, $a \in \mathbb{N}$
- m, $n \in \mathbb{N}$, $m \leq n$.

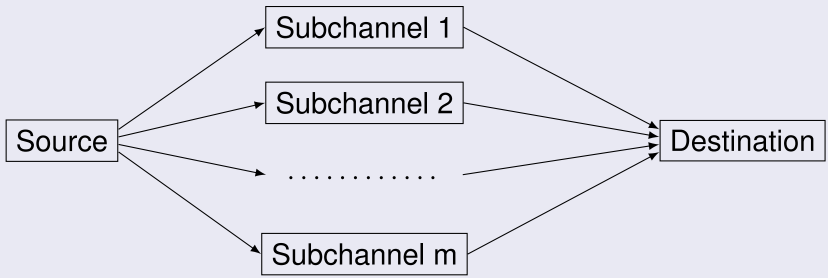
Matrix channel $\mathcal{W}$

Matrix channel

Fix

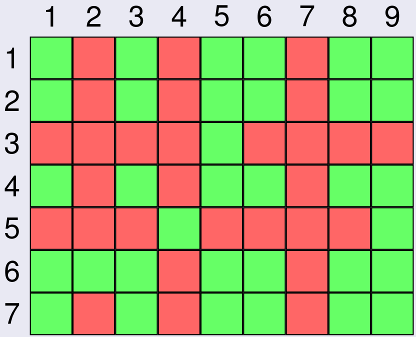
- $\mathbb{F}_q$ – finite field, $q = p^a$, $a \in \mathbb{N}$
- m, $n \in \mathbb{N}$, $m \leq n$.

Matrix channel $\mathcal{W}$



Crisscross errors

Crisscross error pattern ($m = 7$, $n = 9$)



Matrix channel applications

- Data storage systems (e.g. memory chips)
- Magnetic tapes
- Wireless communications
- Space-time coding
- Random network coding
- Public-key cryptography
- Steganography

Outline

1. Preliminaries
   - Matrix channel with crisscross errors
   - Term rank metric and rank metric spaces
   - Linear codes in $\mathcal{M}_{TR}$ and $\mathcal{M}_R$
2. Algebra of $p(x)$-circulants and a code construction
   - $p(x)$-circulants
   - Code construction
3. Some optimal codes
   - Optimal codes in $\mathcal{M}_R$
   - Optimal codes in $\mathcal{M}_{TR}$
   - Open questions

Term rank metric

Definition

Let $\mathbb{F}_q^{m\times n}$ be a set of all matrices over $\mathbb{F}_q$ with m rows and n columns.

Term rank weight

$$\forall A \in \mathbb{F}_q^{m\times n} : \ \|A\|_{TR} = \min_{\mathcal{I}(A)} |\mathcal{I}(\mathcal{A})|,$$

$\mathcal{I}(A)$ is a set of lines (rows and/or columns) in A which cover all nonzero elements of A

Term rank metric

Example

$$\left\| \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \right\|_{TR} = 1, \quad \left\| \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \right\|_{TR} = 2$$

Example

$$\left\| \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\|_{TR} = 4, \quad \left\| \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \right\|_{TR} = 4$$

Term rank metric

Example

$$\left\| \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \right\|_{TR} = 1, \quad \left\| \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \right\|_{TR} = 2$$

Example

$$\left\| \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\|_{TR} = 4, \quad \left\| \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \right\|_{TR} = 4$$

Term rank metric

Term rank distance function

$$d_{TR}(A, B) = \|A - B\|_{TR}$$

Term rank metric space

$$\mathcal{M}_{TR} = (\mathbb{F}_q^{m \times n}, d_{TR})$$

Term rank metric

Definition

A diagonal Δ_τ in a matrix $A \in \mathbb{F}_q^{m\times n}$ is a set of positions

$$\Delta_\tau = \{(0, \tau(0)), (1, \tau(1)), \ldots, (m-1, \tau(m-1))\},$$

where τ is an injection from $[0,\ m-1]$ to $[0,\ n-1]$.

Theorem

$$\forall A \in \mathbb{F}_q^{m\times n}:\ \|A\|_{TR} = \max_\tau |\Delta_\tau(A)|,$$

where τ runs overall injections from $[0,\ m-1]$ to $[0,\ n-1]$ and $|\Delta_\tau(A)|$ – a number of nonzero entries of A on the Δ_τ.

Rank metric

Rank weight

$$\forall A \in \mathbb{F}_q^{m\times n} : \ \|A\|_R = \mathrm{rank}(A)$$

Rank distance function

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

Rank metric space

$$\mathcal{M}_R = (\mathbb{F}_q^{m\times n}, d_R)$$

Metric spaces

Connection between term rank metric and rank metric

$$\forall A,\ B \in \mathbb{F}_q^{m\times n}:\ d_R(A,B) \le d_{TR}(A,B) \le \min\{m,n\}$$

Outline

1. Preliminaries
   - Matrix channel with crisscross errors
   - Term rank metric and rank metric spaces
   - Linear codes in $\mathcal{M}_{TR}$ and $\mathcal{M}_R$
2. Algebra of $p(x)$-circulants and a code construction
   - $p(x)$-circulants
   - Code construction
3. Some optimal codes
   - Optimal codes in $\mathcal{M}_R$
   - Optimal codes in $\mathcal{M}_{TR}$
   - Open questions

Linear codes

Definition

A linear $[m \cdot n, k]_q$-code $\mathcal{C}$ is a k-dimensional subspace of $\mathbb{F}_q^{m \times n}$.

Minimal distances of $\mathcal{C}$

$$D_{TR}(\mathcal{C}) \triangleq \min_{A \in \mathcal{C} \setminus \{0\}} \|A\|_{TR}, \quad D_R(\mathcal{C}) \triangleq \min_{A \in \mathcal{C} \setminus \{0\}} \|A\|_R.$$

Connection between minimal distances

$$D_R(\mathcal{C}) \leq D_{TR}(\mathcal{C}) \leq \min\{m, n\}$$

Optimal linear codes

Singleton-type bound

For any $[m \cdot n, k]_q$-code $\mathcal{C}$ we have

$$k \leq n(m - D_{TR}(\mathcal{C}) + 1), \quad k \leq n(m - D_{TR}(\mathcal{C}) + 1).$$

Definition

A linear code $\mathcal{C}$ is called *optimal* in $\mathcal{M}_{TR}$ (in $\mathcal{M}_R$) if $k = n(m - D_{TR}(\mathcal{C}) + 1)$ (resp. $k = n(m - D_R(\mathcal{C}) + 1)$).

Constructions of optimal codes in $\mathcal{M}_{TR}$

- By construct an optimal codes in $\mathcal{M}_R$ (e.g. Gabidulin codes)
- By considering a set of all circulant $m \times n$ matrices over $\mathbb{F}_q$ (only for the case $D_{TR} = m$)
- By considering a set of Toeplic-like matrices (only for the case $D_{TR} = 2$)
- ???

Constructions of optimal codes in $\mathcal{M}_{TR}$

- By construct an optimal codes in $\mathcal{M}_R$ (e.g. Gabidulin codes)
- By considering a set of all circulant $m \times n$ matrices over $\mathbb{F}_q$ (only for the case $D_{TR} = m$)
- By considering a set of Toeplic-like matrices (only for the case $D_{TR} = 2$)
- ???

Constructions of optimal codes in $\mathcal{M}_{TR}$

- By construct an optimal codes in $\mathcal{M}_R$ (e.g. Gabidulin codes)
- By considering a set of all circulant $m \times n$ matrices over $\mathbb{F}_q$ (only for the case $D_{TR} = m$)
- By considering a set of Toeplic-like matrices (only for the case $D_{TR} = 2$)
- ???

Constructions of optimal codes in $\mathcal{M}_{TR}$

- By construct an optimal codes in $\mathcal{M}_R$ (e.g. Gabidulin codes)
- By considering a set of all circulant $m \times n$ matrices over $\mathbb{F}_q$ (only for the case $D_{TR} = m$)
- By considering a set of Toeplic-like matrices (only for the case $D_{TR} = 2$)
- ???

Outline

$p(x)$-circulants

Fix

A monic polynomial $p(x) \in \mathbb{F}_q[x]$ of degree n

$$p(x) = x^n - p_{n-1}x^{n-1} - \ldots - p_1 x - p_0,$$

$p_0 \neq 0$, with its companion matrix

$$B_{p(x)} = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ p_0 & p_1 & p_2 & \ldots & p_{n-1} \end{pmatrix} \in \mathbb{F}_q^{n\times n}.$$

$p(x)$-circulants

Define $\mathbb{F}_q$-algebras homomorphism

$$\varphi : \mathbb{F}_q[x] \to \mathbb{F}_q^{n\times n}, \quad x^i \mapsto (B_{p(x)})^i$$

Properties of φ

- $\ker \varphi = (p(x))$
- $\mathcal{C}_{p(x)} \triangleq \mathrm{Im}\,\varphi \simeq \mathbb{F}_q[x]/(p(x))$
- $\dim \mathcal{C}_{p(x)} = n$

Definition

Elements of $\mathcal{C}_{p(x)}$ we called $p(x)$-circulants

$p(x)$-circulants

Define $\mathbb{F}_q$-algebras homomorphism

$$\varphi : \mathbb{F}_q[x] \to \mathbb{F}_q^{n\times n}, \quad x^i \mapsto (B_{p(x)})^i$$

Properties of φ

- $\ker \varphi = (p(x))$
- $\mathcal{C}_{p(x)} \triangleq \mathrm{Im}\, \varphi \simeq \mathbb{F}_q[x]/(p(x))$
- $\dim \mathcal{C}_{p(x)} = n$

Definition

Elements of $\mathcal{C}_{p(x)}$ we called $p(x)$-circulants

$p(x)$-circulants

Define $\mathbb{F}_q$-algebras homomorphism

$$\varphi : \mathbb{F}_q[x] \to \mathbb{F}_q^{n\times n}, \quad x^i \mapsto (B_{p(x)})^i$$

Properties of φ

- $\ker \varphi = (p(x))$
- $\mathcal{C}_{p(x)} \triangleq \mathrm{Im}\,\varphi \simeq \mathbb{F}_q[x]/(p(x))$
- $\dim \mathcal{C}_{p(x)} = n$

Definition

Elements of $\mathcal{C}_{p(x)}$ we called $p(x)$-circulants

$p(x)$-circulants

Example ($p(x) = x^n - 1$)

C_{x^n-1} is the algebra of all circulant $(n \times n)$-matrices over $\mathbb{F}_q$

Example ($p(x) = x^5 + 1$)

C_{x^5+1} is the algebra of all skew-circulant (negacirculant)

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 \\ -a_4 & a_0 & a_1 & a_2 & a_3 \\ -a_3 & -a_4 & a_0 & a_1 & a_2 \\ -a_2 & -a_3 & -a_4 & a_0 & a_1 \\ -a_1 & -a_2 & -a_3 & -a_4 & a_0 \end{pmatrix}$$

$p(x)$-circulants

Example ($p(x) = x^n - 1$)

C_{x^n-1} is the algebra of all circulant $(n \times n)$-matrices over $\mathbb{F}_q$

Example ($p(x) = x^5 + 1$)

C_{x^5+1} is the algebra of all skew-circulant (negacirculant)

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 \\ -a_4 & a_0 & a_1 & a_2 & a_3 \\ -a_3 & -a_4 & a_0 & a_1 & a_2 \\ -a_2 & -a_3 & -a_4 & a_0 & a_1 \\ -a_1 & -a_2 & -a_3 & -a_4 & a_0 \end{pmatrix}$$

$p(x)$-circulants

Example ($p(x) = x^5 - r$)

C_{x^5-r} is the algebra of all r-circulant matrices

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 \\ ra_4 & a_0 & a_1 & a_2 & a_3 \\ ra_3 & ra_4 & a_0 & a_1 & a_2 \\ ra_2 & ra_3 & ra_4 & a_0 & a_1 \\ ra_1 & ra_2 & ra_3 & ra_4 & a_0 \end{pmatrix}$$

$p(x)$-circulants

Example ($p(x) = x^5 - x - 1$)

C_{x^5-x-1} is the algebra of all *FLS*-circulant matrices

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 \\ a_4 & a_0 + a_4 & a_1 & a_2 & a_3 \\ a_3 & a_4 + a_3 & a_0 + a_4 & a_1 & a_2 \\ a_2 & a_3 + a_2 & a_4 + a_3 & a_0 + a_4 & a_1 \\ a_1 & a_2 + a_1 & a_3 + a_2 & a_4 + a_3 & a_0 + a_4 \end{pmatrix}$$

Facts on $p(x)$-circulants

$p(x)$-circulant is defined by its first row

$$\mu_{p(x)} : \mathbb{F}_q^n \to \mathcal{C}_{p(x)}, \quad (a_0, \dots, a_{n-1}) \mapsto \varphi\left(a_0 + \dots + a_{n-1}x^{n-1}\right)$$

Some useful facts

- $A = \mu_{p(x)}((a_0, \dots, a_{n-1})) \in \mathcal{C}_{p(x)}$ is invertible iff

$$\gcd(a_0 + a_1 x + \dots + a_{n-1}x^{n-1}, p(x)) = 1$$

- $\mathcal{C}_{p(x)}$ is a field iff $p(x)$ is irreducible

Outline

Codes via $p(x)$-circulants

Definition

$\mathcal{C}_{p(x)}$ is a linear $[n \cdot n,\ n]_q$-code in $\mathcal{M}_{TR}$ and $\mathcal{M}_R$

Code shortening

To construct a linear $[m \cdot n,\ n]_q$-code for each $m \in [1, n]$ and any $\mathcal{J} \subseteq [0, n-1]$, $|\mathcal{J}| = n - m$, define the $\mathbb{F}_q$-linear "shortening" map

$$\sigma_{\mathcal{J}}^{(n-m)} : \mathbb{F}_q^{n \times n} \to \mathbb{F}_q^{m \times n}$$

by cut all rows with indexes from $\mathcal{J}$.

Codes via $p(x)$-circulants

Definition

$\sigma_{\mathcal{J}}^{(n-m)}(\mathcal{C}_{p(x)})$ is a linear $[m \cdot n,\ n]_q$-code in $\mathcal{M}_{TR}$ and $\mathcal{M}_R$

Properties of code shortening

$$\forall A \in \mathbb{F}_q^{n\times n}: \quad \begin{aligned} \|A\|_{TR} - s \le \|\sigma_{\mathcal{J}}^{(s)}(A)\|_{TR} \le \|A\|_{TR}, \\ \|A\|_{R} - s \le \|\sigma_{\mathcal{J}}^{(s)}(A)\|_{R} \le \|A\|_{R}, \end{aligned}$$

Codes via $p(x)$-circulants

Lemma

Let $\mathcal{C} = \sigma_{\mathcal{J}}^{(s)}(\mathcal{C}_{p(x)})$. Then

- $D_{TR}(\mathcal{C}) \geq D_{TR}(\mathcal{C}_{p(x)}) - s$
- $D_R(\mathcal{C}) \geq D_R(\mathcal{C}_{p(x)}) - s.$

Moreover, if $\mathcal{C}_{p(x)}$ is optimal in $\mathcal{M}_{TR}$ ($\mathcal{M}_R$) then $\mathcal{C}$ still be optimal in $\mathcal{M}_{TR}$ (resp. $\mathcal{M}_R$).

Outline

1. Preliminaries
   - Matrix channel with crisscross errors
   - Term rank metric and rank metric spaces
   - Linear codes in $\mathcal{M}_{TR}$ and $\mathcal{M}_R$
2. Algebra of $p(x)$-circulants and a code construction
   - $p(x)$-circulants
   - Code construction
3. Some optimal codes
   - Optimal codes in $\mathcal{M}_R$
   - Optimal codes in $\mathcal{M}_{TR}$
   - Open questions

Optimal codes in $\mathcal{M}_R$

Proposition

The code $\mathcal{C}_{p(x)}$ is optimal in $\mathcal{M}_R$ (i.e. $D_R(\mathcal{C}_{p(x)}) = n$) iff $p(x)$ is irreducible in $\mathbb{F}_q[x]$.

Corollary

The shortened code $\sigma_{\mathcal{J}}^{(n-m)}(\mathcal{C}_{p(x)})$ is optimal in $\mathcal{M}_R$ (i.e. $D_R(\mathcal{C}_{p(x)}) = m$) if $p(x)$ is irreducible in $\mathbb{F}_q[x]$.

Outline

Optimal codes in $\mathcal{M}_{TR}$

Theorem

The code $\mathcal{C}_{p(x)}$ is optimal in $\mathcal{M}_{TR}$ (i.e. $D_{TR}(\mathcal{C}_{p(x)}) = n$) when

(i) $p(x)$ *is an irreducible in* $\mathbb{F}_q[x]$;

(ii) $p(x) = x^n - p_0,\ p_0 \in \mathbb{F}_q^*$;

(iii) $p(x) = x^n - p_t x^t - p_0,\ t \in [1, n-1],\ p_0, p_t \in \mathbb{F}_q^*$.

Proof of the Theorem

Theorem (recall)

$$\forall A \in \mathbb{F}_q^{m\times n}: \ \|A\|_{TR} = \max_{\tau} |\Delta_\tau(A)|,$$

where τ *runs overall injections from* $[0,\ m-1]$ *to* $[0,\ n-1]$ *and* $|\Delta_\tau(A)|$ *– a number of nonzero entries of* A *on the* Δ_τ.

Lemma

A linear $[m\cdot n,\ n]_q$*-code* $\mathcal{C}$ *is an optimal in* $\mathcal{M}_{TR}$ *iff for any* $A \in \mathcal{C}\setminus\{0\}$ *there exists a diagonal* Δ_τ *such that* $|\Delta_\tau(A)| = m$.

Proof of the Theorem

Proof of (ii)

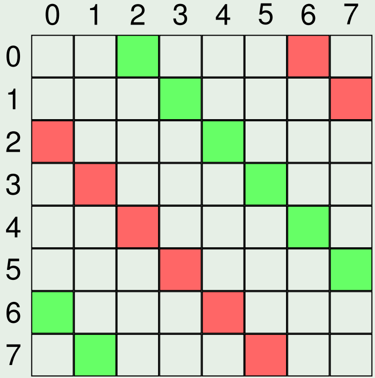
Let $A = \mu_{p(x)}(v)$, where $v = (a_0, \dots, a_{n-1})$ is the first row of A, be a nonzero $p(x)$-circulant. To simplify the notation for each $i \in [0, n-1]$ put

$$\Delta_i = \{(j, (i+j) \mod m) \mid j \in [0, m-1]\}.$$

In the case (ii) for some $i \in [0, n-1]$ we have $a_i \neq 0$ and the entries of A on the Δ_i are equal to a_i or $p_0 a_i$. So $|\Delta_i(A)| = n$ and (ii) is proved.

Proof of the Theorem

Example ($n = 8$, Δ_2 – green, Δ_6 – red)



Proof of the Theorem

Toward to the proof of (iii)

$\forall A \in \mathcal{C}_{p(x)}$, $p(x) = x^n - p_t x^t - p_0$, $t \in [1, n-1]$, $p_0, p_t \in \mathbb{F}_q^*$, there exists a bijection $\tau \in S_n$ such that

- $|\Delta_\tau(A)| = n$;
- $\exists j_1, j_2 \in [0,\ n-1] :\ \Delta_\tau \subseteq \Delta_{j_1} \cup \Delta_{j_2}$.

Optimal codes in $\mathcal{M}_{TR}$

Counterexample for $p(x) = x^n - p_t x^t - p_s x^s - p_0$, $0 < s < t < n$

Let $q = 2$, $p(x) = x^3 + x^2 + x + 1 = (x+1)^3$. Then

$$A = \mu_{p(x)}((1, 0, 1)) = \varphi(1 + x^2) = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

has term rank 2.

Outline

Open questions

- More sufficient and necessary conditions on optimality of $\mathcal{C}_{p(x)}$ in $\mathcal{M}_{TR}$
- Decoding methods for $\mathcal{C}_{p(x)}$ in $\mathcal{M}_{TR}$
- Constructions for optimal codes with $2 < D_{TR} < m$