Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia *pp. 348–353*

On a construction of optimal codes in term rank metric via $p(x)$-circulants [1]

Vladimir Gritsenko gritsenko.vld@gmail.com
Southern Federal University, Rostov-on-Don, Russia
Alexey Maevskiy tim_org@mail.ru
Southern Federal University, Rostov-on-Don, Russia

Abstract. We consider a term rank metric space $\mathcal{M}_{TR} = (\mathbb{F}_q^{m\times n},\, d_{TR})$ and present new family of codes in $\mathcal{M}_{TR}$ attaining the corresponding Singleton bound. Our approach is based on the generalization of circulant matrices over $\mathbb{F}_q$ which we called $p(x)$-circulants. Some of our codes are optimal in the rank metric space too.

1 Introduction

Fix a finite field $\mathbb{F}_q$ with q elements, q is a prime power, and for $m, n \in \mathbb{N}$, $m \le n$, let $\mathbb{F}_q^{m\times n}$ be a $m \cdot n$-dimensional vector space over $\mathbb{F}_q$, whose elements will be regarded as matrices with m rows and n columns. For every $m \times n$ matrix A define its term rank weight

$$\|A\|_{TR} = \min_{\mathcal{I}(A)} |\mathcal{I}(\mathcal{A})|,$$

where $\mathcal{I}(A)$ is a set of lines (rows and/or columns) in A which cover all nonzero elements of A [1], and a rank weight

$$\|A\|_R = \mathrm{rank}(A).$$

It's easy to check that these weight functions derive two distances between any $m \times n$ matrices A, B as

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

with obvious property

$$d_R(A,B) \le d_{TR}(A,B) \le \min\{m,n\}. \tag{1}$$

In coding theory the corresponding metric spaces $\mathcal{M}_{TR} = (\mathbb{F}_q^{m\times n}, d_{TR})$ and $\mathcal{M}_R = (\mathbb{F}_q^{m\times n}, d_R)$ are called term rank space (or array metric space) [2] and

[1] The second author's research was partially supported by RFBR grant no. 13-07-00978

rank space [3], respectively. They arise in problems related to the transmission of $(m{\cdot}n)$-length block data through memoryless "matrix channel" with independent crisscross errors ([2], [4], [5]). Matrix channel consists of m parallel q-ary subchannels, transmitted blocks of data are modeled by elements of $\mathbb{F}_q^{m\times n}$ and crisscross error per one block A select r different lines (rows and/or columns) of A with probability $P(r)$ and fill these lines by elements of $\mathbb{F}_q$ independently and equiprobable (assume that $P(r)$ decreases with r). Such models of matrix channels can be found in data storage systems (e.g. memory chips), magnetic tapes and some types of wireless communications (cf. [5]). Note that the rank metric space also arises in space-time coding [6], random network coding [7], public-key cryptography [8] and steganography [9].

Recall that a linear $[m\cdot n,\, k]_q$-code $\mathcal{C}$ is simply a k-dimensional vector subspace of $\mathbb{F}_q^{m\times n}$. Since $\mathbb{F}_q^{m\times n}$ is a support of both spaces $\mathcal{M}_{TR}$ and $\mathcal{M}_R$, the code $\mathcal{C}$ may be considered as its subset and thus has two appropriate minimal distances

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

We assume w.l.o.g. that $m \le n$. Note that for any $\mathcal{C}$ from (1) follows

$$D_R(\mathcal{C}) \le D_{TR}(\mathcal{C}) \le m \tag{2}$$

and $D_R(\mathcal{C}) = m$ implies $D_{TR}(\mathcal{C}) = m$. It is a well known (e.g., [4]) that parameters of any linear code $\mathcal{C}$ in both metric spaces must satisfy the inequality which called Singleton bound

$$k \le n(m - D + 1),$$

where $D = D_{TR}(\mathcal{C})$ or $D = D_R(\mathcal{C})$. 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. $k = n(m-D_R(\mathcal{C})+1)$). Optimal codes plays an important role in applications of coding theory and one of the main tasks is to specify explicit constructs for all of them. It is clear that any optimal code in $\mathcal{M}_R$ is also optimal in $\mathcal{M}_{TR}$ and most of the methods for constructing an optimal codes in $\mathcal{M}_{TR}$ are based on this fact (e.g., [4], [5]). In [2] for the case $D_{TR}(\mathcal{C}) = m$ was presented a method for construct optimal codes in $\mathcal{M}_{TR}$ but non-optimal in $\mathcal{M}_R$ ($D_R(\mathcal{C}) = 1$) which based on considering the set of all circulant matrices from $\mathbb{F}_q^{m\times n}$. In this paper in Section 2 we define a wider class of $p(x)$-circulants and present a construction of a large class of codes in $\mathcal{M}_{TR}$ and $\mathcal{M}_R$. In Section 3 we give a necessary and some sufficient conditions on optimality of the resulting codes.

2 Algebra of $p(x)$-circulants and code construction

Consider a monic polynomial $p(x)$ of degree n over finite field $\mathbb{F}_q$

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

with its companion matrix

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

Define the $\mathbb{F}_q$-algebras homomorphism $\varphi : \mathbb{F}_q[x] \to \mathbb{F}_q^{n\times n}$ by map x^i to $(B_{p(x)})^i$ for all $i \geq 0$ and extend it to $\mathbb{F}_q[x]$ by linearity. Obviously, $\ker\varphi = (p(x))$ and hence

$$\mathcal{C}_{p(x)} \overset{\Delta}{=} \operatorname{Im}\varphi \simeq \mathbb{F}_q[x]/(p(x)). \tag{3}$$

Clearly, $\mathcal{C}_{p(x)}$ is an commutative algebra with identity and its dimension as a vector space over $\mathbb{F}_q$ is n. The elements of $\mathcal{C}_{p(x)}$ are called $p(x)$-circulants [10] and are unique determined by its first row. So we have the isomorphism of vector spaces

$$\mu_{p(x)} : \mathbb{F}_q^n \to \mathcal{C}_{p(x)}, \quad (a_0, \dots, a_{n-1}) \mapsto \varphi\left(a_0 + a_1x + \ldots + a_{n-1}x^{n-1}\right).$$

Note that $\mathcal{C}_{x^n-1}$ is the same as algebra of ordinary $n \times n$ circulants over $\mathbb{F}_q$ and the elements of $\mathcal{C}_{x^n+1}$ are known as skew-circulants (or negacirculants). More detailed description of $\mathcal{C}_{p(x)}$ and some related algebraic and algorithmic facts are given in [10].

Consider the algebra $\mathcal{C}_{p(x)}$ as n-dimensional vector subspace of $\mathbb{F}_q^{n\times n}$ and, therefore, as linear $[n \cdot n, n]$-code $\mathcal{C}$ in $\mathbb{F}_q^{n\times n}$. To construct the linear $[m \cdot n, n]$-code in $\mathbb{F}_q^{m\times n}$, $m \leq n$, we use the code shortening method from [4]. Let the rows and the columns of any $A \in \mathbb{F}_q^{n\times n}$ are indexed by elements from $[0,\, n-1]$. For each $s \in [0, n-1]$ and any $\mathcal{J} \subseteq [0, n-1]$, $|\mathcal{J}| = s$, define the $\mathbb{F}_q$-linear "shortening" map

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

by cut all rows with indexes from $\mathcal{J}$. Then to construct a code $\mathcal{C}$ in $\mathbb{F}_q^{m\times n}$ fix any $\mathcal{J} \subset [0, n-1]$, $|\mathcal{J}| = n - m$, and put $\mathcal{C} = \sigma_{\mathcal{J}}^{(n-m)}(\mathcal{C}_{p(x)})$. By the obvious property of any $\sigma_{\mathcal{J}}^{(s)}$:

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

we get the following lemma.

Lemma 1. *Let $\mathcal{C} = \sigma_{\mathcal{J}}^{(s)}(\mathcal{C}_{p(x)})$. Then $D_{TR}(\mathcal{C}) \geq D_{TR}(\mathcal{C}_{p(x)}) - s$ and $D_R(\mathcal{C}) \geq D_R(\mathcal{C}_{p(x)}) - s$. 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. $\mathcal{M}_R$).*

3 Some optimal codes

In this section we give a necessary and some sufficient conditions on optimality of $\mathcal{C}_{p(x)}$. Note that by lemma 1 the optimality of $\mathcal{C}_{p(x)}$ implies optimality of any its shortening. Assume that $\mathbb{F}_q$, m, n and $p(x)$ are chosen as in the previous section.

Proposition 1. *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 $\mathbb{F}_q[x]$.*

Proof. It follows from (3) and well-known criterion on invertibility of elements from $\mathbb{F}_q[x]/(p(x))$. □

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

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

where τ is an injection from $[0,\ m-1]$ to $[0,\ n-1]$. By $|\Delta_\tau(A)|$ denote a number of nonzero entries of A on the Δ_τ. In [1] was proved that

$$\|A\|_{TR} = \max_\tau |\Delta_\tau(A)|,$$

when τ runs overall injections from $[0,\ m-1]$ to $[0,\ n-1]$. Therefore, we get

Lemma 2. *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 $|\Delta_\tau(A)| = m$.*

It is rather obvious that a code $\mathcal{C}_{p(x)}$ cannot be optimal in $\mathcal{M}_{TR}$ if $n > 1$ and $p(0) = 0$. The following result is the main result of the paper.

Theorem 1. *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. The first statement is a corollary from proposition 1 and (2).

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.

The proof of the case (iii) is more complicated and technical, so we give here its sketch. Let $p(x)$ be as in (iii) and $s = \gcd(n, t)$, $r = n/s$. Put

$$\forall i \in [0, s-1] : \; U_i = \{i + (j+1)t \pmod{n} \mid j \in [0, r-1]\}.$$

Obviously, $\{U_i\}_{i=0}^{s-1}$ is a partition of $[0, n-1]$ and $|U_i| = r$. For every $i \in [0, s-1]$ define a vector $v_i = (v_0^{(i)}, \ldots, v_{n-1}^{(i)}) \in \mathbb{F}_q^n$ by

$$v_j^{(i)} = \begin{cases} a_j, & \text{if } j \in U_i, \\ 0, & \text{otherwise,} \end{cases}$$

and put $A_i = \mu_{p(x)}(v_i)$. Its easy to check that A_{i_1} and A_{i_2}, $i_1 \neq i_2$, has no nonzero entries on the same positions and $A = A_0 + \ldots + A_{s-1}$. It can be proved by direct analysis of $|\Delta_j(A_i)|$, $i \in [0, s-1]$, $j \in U_i$, that for each nonzero A_i there exists a bijection τ_i such that

(a) $|\Delta_{\tau_i}(A_i)| = n$;

(b) $\exists j_1, j_2 \in U_i : \; \Delta_{\tau_i} \subseteq \Delta_{j_1} \cup \Delta_{j_2}$.

From (a) follows $\|A_i\|_{TR} = n$ and, therefore, $\|A\|_{TR} = n$. □

The analysis of the cases when $p(x)$ has more than three terms is much more complicated. But at least it is clear that not all $\mathcal{C}_{p(x)}$ with weight $p(x)$ is equal 4, i.e. $p(x) = x^n - p_t x^t - p_s x^s - p_0$, $0 < s < t < n$, are optimal. Indeed, let $q = 2$ and $p(x) = x^3 + x^2 + x + 1$. Then $p(x) = (x+1)^3$ and the following nonzero $p(x)$-circulant

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

corresponding to $x^2 + 1$ has term rank 2.

References

[1] H. J. Ryser, *Combinatorial Mathematics,* The Mathematical Association of America, Rahway, New Jersey, 1963.

[2] E. M. Gabidulin and B. I. Korjik, Lattice-error-correcting codes, *Izv. Vyssh. Uchebn. Zaved., Radioelectron.,* **15** (4), 492–498, 1972.

[3] E. M. Gabidulin, Theory of codes with maximum rank distance, *Probl. Inf. Transm.,* **21** (1), 3–16, 1985.

[4] E. M. Gabidulin, Optimum Codes Correcting Lattice Errors, *Probl. Inf. Transm.,* **21** (2), 103–108, 1985.

[5] R. M. Roth, Maximum-rank array codes and their applications to crisscross error correction, *IEEE Trans. Inf. Theory,* **37** (2), 328–336, 1991.

[6] V. Tarokh, H. Jafarkhani and A. R. Calderbank, Space-Time Codes for High Data Rate Wireless Communication: Performance Criterion and Code Construction, *IEEE Trans. Inf. Theory,* **44** (2), 744–765, 1998.

[7] D. Silva, F. R. Kschischang, R. Koetter, A Rank-Metric Approach to Error Control in Random Network Coding, *IEEE Trans. Inf. Theory,* **54** (9), 3951–3967, 2008.

[8] E. M. Gabidulin, A. V. Paramonov and O. V. Tretjakov, Ideals over a Non-commutative Ring and Their Application in Cryptology. *Advances in Cryptology – Eurocrypt'91,* LNCS No. 547, Berlin and Heidelberg: Springer-Verlag, 1991, 482–489.

[9] R. S. Selvaraj and J. Demamu, Steganographic protocols based on rank metric codes, in *Proc. ICUMT'11, Budapest, Hungary, 2011,* 1–4.

[10] V. V. Gritsenko, A. E. Maevskiy, $p(x)$-circulants over finite fields and probabilistic methods for its construction, *Math. Notes* (in appear).