q -ary Quasi-Cyclic Codes on Matroid Theory

Xiuli Li, Pengcheng Zhao and Dangsheng Zhou

School of Mathematics and Physics, Qingdao University of Science and Technology, Qingdao, China

Abstract. In this paper, rate $1/p$ q -ary systematic quasi-cyclic codes are constructed based on matroid theory. The relationship between the generator matrix and minimum distance d is derived. Examples and algorithm are presented.

1 INTRODUCTION

In 1967, quasi-cyclic codes were first found by Townsend and Weldon [1]. Quasi-cyclic codes have been extended by the authors ([2],[3]). Many good quasi-cyclic codes were discovered in [4]. Most of the works have concentrated on the algebraic-combinatorial computers search ([5]-[8]).

Definition 1.1 Let F_q be the Galois field with q elements. A subset C of F_q^{kp} is called a quasi-cyclic code of length kp and index p such that

(1) C is a subspace of F_q^{kp} ;

(2) If $(c_{0,0}, \dots, c_{0,p-1}, c_{1,0}, \dots, c_{1,p-1}, \dots, c_{k-1,0}, \dots, c_{k-1,p-1})$ is a codeword of C , then

$$(c_{k-1,0}, \dots, c_{k-1,p-1}, c_{0,0}, \dots, c_{0,p-1}, \dots, c_{k-2,0}, \dots, c_{k-2,p-1})$$

is also a codeword in C .

We also call C a rate $1/p$ quasi-cyclic code. It follows from [8] that the generator matrix of a quasi-cyclic code of length kp and index p is equivalent to a $k \times p$ generator matrix of the form

$$G = [G_0, G_1, \dots, G_{p-1}],$$

where G_i is a $k \times k$ circulate matrix, $0 \leq i \leq p-1$. To construct systematic quasi-cyclic codes, let $G_0 = I_k$, where I_k is a $k \times k$ identity matrix. Under the situation of without causing ambiguity, we also call such a matrix G a generator matrix of C .

In [9], by a use of the connections between block codes and their matroids, a matroid search algorithm is developed to construct the binary linear quasi-cyclic codes with a large minimum distance. In this paper, we generalize the method of [9] to q -ary quasi-cyclic codes and construct the q -ary linear quasi-cyclic codes with a large minimum distance.

This paper is organized as follows. Section 2 contains

a brief description of matroid theory and the relationship between matroid and coding. Section 3 proposes the method of constructing q -ary quasi-cyclic codes from matroid theory. Algorithm is presented in section 4.

2 PRELIMINARIES

Definition 2.1 A matroid M is an ordered pair (V, E) consisting of a finite set V and a collection

E of subsets of V satisfying the following three conditions:

(1) $\emptyset \in E$.

(2) If $I \in E$ and $I' \subseteq I$, then $I' \in E$.

(3) If I_1 and I_2 are in E and $|I_1| < |I_2|$, then there is an element v of $I_2 - I_1$ such that $I_1 \cup \{v\} \in E$.

Condition (3) is called the independence augmentation axiom. If M is a matroid (V, E) , then M is called a matroid on V . Let V be the ground set of M , and the members of E be the independent sets of M , denoted by $V(M)$ and $E(M)$ respectively. Any subset of V which is not in E is called a dependent set of M , and a minimal dependent set in M is called a circuit of M . Any one-element circuit is called a loop and the set of all circuits is denoted by $C(M)$. A maximal independent set in M must be a base of M and the set of all bases of M is represented as $B(M)$. The cardinality of any base of M is defined to be the rank of M , denoted as $r(M)$.

Definition 2.2 The rank function $r(X)$ is the size of the largest independent subset of X for $X \subseteq V$.

Definition 2.3 Let $M_1 = (V_1, E_1)$ and $M_2 = (V_2, E_2)$ be two matroids. If there exists a mapping $\sigma: V_1 \rightarrow V_2$ such that $\sigma(I_1) \in E_2$, where $I_1 \in E_1$, then M_1 and M_2 are isomorphic.

* Corresponding author: lixiuli2007@aliyun.com, 2975064983@qq.com, 467330867@qq.com

It is well known that matroids can be determined by their bases, circuits, rank function, respectively.

Many kinds of matroids can be constructed. For the finite field F_q , q -ary linear codes can be constructed from q -ary matroids. Let G^* be a q -ary $k \times n$ matrix whose rank is equal to k . Let $b_1, b_2, \dots, b_n$ be the column vectors of G^* . and $V = \{1, 2, \dots, n\}$. E is defined as the collection of the subsets $I = \{i_1, i_2, \dots, i_s\} \subseteq V$ such that the sequence of vectors $b_{i_1}, b_{i_2}, \dots, b_{i_s}$ is linearly independent over the finite field F_q . Obviously, (V, E) satisfies the definition of matroid, it is called a vector matroid, and denoted as $M[G^*]$. The vector matroid remains unchanged after any of the following operations:

- (1) Interchange any two rows of G^* .
- (2) Multiplies any row of G^* by a nonzero constant.
- (3) Replace a row with the sum of this row and non zero scalar multiplication of any other row of G^* .

A q -ary matrix G^* is the generator matrix of some q -ary linear code with dimension $r(M[G^*]) = \text{rank}(G^*)$. The matrix G^* can be transformed into the matrix of the form $(I_k | G')$ which is called a standard representative matrix for M , where G' is a $k \times (n-k)$ matrix.

Let $F_q = \{0, \xi, \xi^2, \dots, \xi^{q-1} = 1\}$ where ξ is the generating element of F_q . For any $i \in \{1, 2, \dots, (q^k - 1)\}$, there exist $a_{i,0}, a_{i,1}, \dots, a_{i,k-1} \in \{0, 1, \dots, q-1\}$ such that $a_{i,0} + a_{i,1}q + \dots + a_{i,k-1}q^{k-1} = i$ and $a_{i,0}, a_{i,1}, \dots, a_{i,k-1}$ are unique. Let φ be a mapping from $\{0, 1, \dots, q-1\}$ to F_q defined by

$$\varphi(0) = 0 \text{ and } \varphi(t) = \xi^t, 1 \leq t \leq q-1.$$

φ is a isomorphic mapping. Then for any $i \in \{1, 2, \dots, (q^k - 1)\}$, there exists a q -ary vector $\tau(i) = (\varphi(a_{i,0}), \varphi(a_{i,1}), \dots, \varphi(a_{i,k-1}))$. $\tau(i)$ is uniquely determined by i .

Definition 2.4 $\tau(i)$ is called the q -ary k -tuple representation of i .

Now, let G^* be a $k \times (q^k - 1)$ matrix whose i -th column is the q -ary k -tuple representation of the integer i , where $i = 1, 2, \dots, q^k - 1$. We construct a serial of matroids $M_i(k, q) = (V(k, q), E_i(k, q))$ for $i = 1, 2, \dots, q^k - 1$, where $V(k, q) = \{1, 2, \dots, q^k - 1\}$ is the ground set, $E_i(k, q)$ is a collection of subsets X of $V(k, q)$, and the q -ary k -tuple representations of elements in X are linearly independent over F_q with the property that the product of its transpose with the i -th column of G^* is zero. In this case, X is an independent set, for $i = 1, 2, \dots, q^k - 1$. Note that the ground set of $M_i(k, q)$ (denoted by $V_i(k, q)$) is the set of elements j of $V(k, q)$ such that the product of the transpose of q -ary k -tuple representation of j with the

i -th column of G^* is zero. Obviously, $|V_i(k, q)| = q^{k-1} - 1$.

Theorem 2.5 Let G be a matrix whose columns are the q -ary k -tuple representations of elements

in a subset B of $V(k, q)$. If B satisfies $|B| = n$ and $\max_{1 \leq j \leq q^k - 1} |B \cap V_j(k, q)| = t$, then the minimum distance d of the code C generated by G is $n - t$.

Proof. Let $a = (a_1, a_2, \dots, a_k)$ be a message vector, where $a_i \in F_q$ for $i = 1, 2, \dots, k$. For a codeword $c = a \cdot G = (c_1, c_2, \dots, c_n)$, it follows from the condition $\max_{1 \leq j \leq q^k - 1} |B \cap V_j(k, q)| = t$ that the number of zeros in such a codeword c are no more than t . Meanwhile, there exists at least one codeword c in which the number of zeros is t . Thus, the minimum distance of C is equal to $n - t$.

Theorem 2.5 can be used to compute the minimum distance of a code C .

3 CONSTRUCTION OF q -ARY QUASI-CYCLIC CODES

Let $V(k, q) = \{1, 2, \dots, q^k - 1\}$. Let G^* be a $k \times (q^k - 1)$ matrix whose i -th column is the q -ary k -tuple representation of the integer i , where $i \in V(k, q)$. Let $V_i(k, q)$ be the set of elements j of $V(k, q)$ such that the product of the transpose of q -ary k -tuple representation of j with the i -th column of G^* is zero, $i \in V(k, q)$.

Definition 3.1 $V(k, q)$ can be decomposed in terms of cyclotomic cosets

$$C_j(k, q) = \{j \cdot q^i, i = 0, 1, \dots, k-1\}, j \in V(k, q).$$

Let $A_j(k, q) = \{\tau(t) : t \in C_j(k, q)\}$. In particular we denote $A_{q^k-1}(k, q) = \{\tau(q^k - 1)\}$. The representative element index set is denoted as S . Finally $L(k, q) = (|C_j(k, q)|)$ is defined as a $1 \times |S|$ vector.

Example 3.2 For $k = 3$, $q = 3$, we have

$V(3, 3) = \{1, 2, \dots, 26\}$. Thus

$$\begin{aligned} C_1(3, 3) &= \{1, 3, 9\}, & C_2(3, 3) &= \{2, 6, 18\}, \\ C_4(3, 3) &= \{4, 12, 10\}, & C_5(3, 3) &= \{5, 15, 19\}, \\ C_7(3, 3) &= \{7, 21, 11\}, & C_8(3, 3) &= \{8, 24, 20\}, \\ C_{13}(3, 3) &= \{13\}, & C_{14}(3, 3) &= \{14, 16, 22\}, \\ C_{17}(3, 3) &= \{17, 25, 23\}, & C_{26}(3, 3) &= \{26\}. \end{aligned}$$

Hence

$$L(3, 3) = \{3, 3, 3, 3, 3, 1, 3, 3, 1\}, S = \{1, 2, 4, 5, 7, 8, 13, 14, 17, 26\}, \text{ and } |S| = 10.$$

Since $F_q = \{0, 1, 2\}$ and 2 is its generating element, then $\tau(1) = (2, 0, 0)$, $\tau(3) = (0, 2, 0)$ and $\tau(9) = (0, 0, 2)$. Thus $A_1(3, 3) = \{(2, 0, 0), (0, 2, 0), (0, 0, 2)\}$. Others are given similarly, $j \in S$.

Theorem 3.3 For any given $i, m \in S$, $C_i(k, q) \cap V_j(k, q)$ is invariable for all $j \in C_m(k, q)$.

Proof. The q -ary k -tuple representation of integer $j \in C_m(k, q)$ is just the cyclic shift of k -tuple

representation of the integer m and the q -ary k -tuple representation of an integer $a \in C_i(k, q)$ is just cyclic-shift of k -tuple representation of the integer i . According to the definition of $V_j(k, q)$ the number of intersection $C_i(k, q) \cap V_j(k, q)$ is invariable for all $j \in C_m(k, q)$.

Definition 3.4 The matrix $R(k, q)$ is defined as (r_{ij}) , where $r_{ij} = C_{S_i}(k, q) \cap V_{S_j}(k, q)$ for $S_i, S_j \in S$. S_i and S_j denote the i -th and j -th coordinate of S respectively.

Let $r = \left\{ i : |C_{S_i}(k, q)| = k, 1 \leq i \leq |S| \right\}$. r_{ij}^* is defined by choosing the rows of $R(k, q)$ corresponding to $|C_{S_i}(k, q)| = k, 1 \leq i \leq |S|$. $R^*(k, q) = (r_{ij}^*)$ is defined by composing a new $r \times |S|$ submatrix corresponding to $L^*(k, q) = (|C_{S_i}(k, q)|)$, where $|C_{S_i}(k, q)| = k, 1 \leq i \leq |S|$.

Example 3.5 For $k=3, q=3$.

$$R(3,3) = \begin{pmatrix} 2 & 2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 2 & 2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 2 & 2 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 3 & 1 & 1 & 3 \\ 1 & 1 & 1 & 0 & 0 & 1 & 3 & 1 & 1 & 3 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 2 & 1 & 1 & 2 & 0 & 1 & 1 & 0 \\ 0 & 0 & 2 & 1 & 1 & 2 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix},$$

$$R^*(3,3) = \begin{pmatrix} 2 & 2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 2 & 2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 2 & 2 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 3 & 1 & 1 & 3 \\ 1 & 1 & 1 & 0 & 0 & 1 & 3 & 1 & 1 & 3 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 2 & 2 & 0 \\ 0 & 0 & 2 & 1 & 1 & 2 & 0 & 1 & 1 & 0 \\ 0 & 0 & 2 & 1 & 1 & 2 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Theorem 3.6 Let F_q be a finite field and k a positive number. Let $X = x_1, x_2, \dots, x_{|S|}$, where $x_i \in 0, 1$ for $1 \leq i \leq |S|$. Let $X \cdot R(k, q) = Y$, $L(k, q) \cdot X^T = n$, where $Y = y_1, y_2, \dots, y_{|S|}$. Then there exists a q -ary n, k, d code such that its minimum distance is equal to $n - \max y_1, y_2, \dots, y_{|S|}$.

Proof. Let the set $I = \{i : x_i = 1, 1 \leq i \leq |S|\}$. Let G be the matrix such that whose columns are the q -ary k -tuple representation of elements in $B = \bigcup_{i \in I} C_{S_i}(k, q)$. Let C be the q -ary linear code whose generating matrix is G .

Owing to the condition $L(k, q) \cdot X^T = n$, we have $|B| = n$ which is the code length. Since $X \cdot R(k, q) = Y$, then $\max_{1 \leq j \leq q^{k-1}} |B \cap V_j(k, q)| = \max y_1, y_2, \dots, y_{|S|}$. From Theorem 2.5 it follows that the minimum distance of C is $n - \max y_1, y_2, \dots, y_{|S|}$.

From Theorem 3.6, to construct quasi-cyclic code of the form $G = [G_0, G_1, \dots, G_{p-1}]$, a series of $C_j(k, q)$ should be chosen so that $|C_j(k, q)| = k$. If only systematic quasi-cyclic code is considered, $C_{q-1}(k, q)$ must be chosen in the code.

Example 3.7 For $k=3, q=3$. $C_1(3,3)$, $C_2(3,3)$, $C_4(3,3)$, $C_5(3,3)$, $C_7(3,3)$, $C_8(3,3)$, $C_{14}(3,3)$, $C_{17}(3,3)$ may be chosen so that $L^*(3,3) = 3, 3, 3, 3, 3, 3, 3, 3$.

If we choose $C_2(3,3)$ and $C_8(3,3)$ then the $6, 3, 3$ code is constructed from $A_2(3,3)$ and $A_8(3,3)$. If we choose $C_2(3,3)$, $C_7(3,3)$ and $C_8(3,3)$, then the $9, 3, 5$ code is constructed from $A_2(3,3)$, $A_7(3,3)$ and $A_8(3,3)$. The generator matrices are

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

and

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 2 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 2 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 2 & 0 & 1 & 1 \end{pmatrix}$$

respectively.

4 ALGORITHM

Let F_q be a finite field and k a positive number. Matroid search algorithm is described in the following steps. We provide a algorithm to construct the optimal system quasi-cyclic codes of rate $1/p$.

(1) Given two parameters k and kp , create $R^*(k, q)$, $L^*(k, q)$, and compute $r = |L^*(k, q)|$.

(2) Let

$$X^* = x^* | x^* = x_1, x_2, \dots, x_r, x_i \in 0, 1, 2 \leq i \leq r, x_1 = 1, x^* \cdot 1_r = p.$$

$$\text{Then } |X^*| = \begin{pmatrix} r-1 \\ p-1 \end{pmatrix}.$$

(3) According to Theorem 3.6, compute $y_i = \max x^* \cdot R^*(k, q)$, where $x^* \in X^*$, $i = 1, 2, \dots, |X^*|$.

(4) To construct the largest minimum distance, according to Theorem 2.5, choose $d_0 = \min y_1, y_2, \dots, y_{|X^*|}$. Then we construct a q -ary quasi-cyclic code with parameters $kp, k, kp - d_0$.

Example 4.1 For $k=3, q=3$. Let $p=3$. Then $r = |L^*(k, q)| = 8$, and $|X^*| = 21$. We may construct 21 q -

ary system quasi-cyclic codes of rate $1/3$. The optimal system quasi-cyclic code in them is a $9,3,6$ code which is constructed from A_2 $3,3$, A_8 $3,3$ and A_{17} $3,3$. The generator matrix is

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

ACKNOWLEDGEMENTS

This work is supported by National Natural Science Foundation (NNSF) of China under Grant 11671235 and Qingdao postdoctoral fund under Grant 861605040007.

REFERENCES

1. Townsend R.L., Weldon E.J. Jr., Self-orthogonal quasi-cyclic codes, *IEEE Trans. Inf. Theory*, IT-13(2):183-195, 1967.
2. Chen C.L., Peterson W.W., Weldon E.J. Jr., results on quasi-cyclic codes, *Inf. Control*, 15:407-423, 1969.
3. Hoffner C.W., Reddy S.M., Circulant bases for cyclic codes, *IEEE Trans. Inf. Theory*, IT-16(4):511-512, 1970
4. Chen Z., Available: <http://www.tec.hkr.se/~chen/research/codes/>. Accessed February, 2013.
5. Chen Z., On Computer Search for Good Quasi-Cyclic Codes, *IEEE Symp. on Information Theory*, Norway, 1994.
6. Gulliver T.A., Bhargava V.K., Some best rate $1/p$ and rate $p-1/p$ systematic quasi-cyclic codes, *IEEE Trans. Inf. Theory*, IT-37(3):552- 555, 1991.
7. Gulliver T.A., Bhargava V.K., Twelve good rate $m-r/pm$ binary quasi-cyclic codes, *IEEE Trans. Inf. Theory*, IT-39(5):1750-1751, 1993.
8. Van Tilborg H.C.A., On quasi-cyclic codes with rate $1/m$, *IEEE Trans. Inf. Theory*, IT-24(5):628-629, 1978.
9. Guangfu Wu, Hsin-Chiu Chang, Lin Wang and T. K. Truong, Constructing rate $1/p$ systematic binary quasi-cyclic codes based on the matroid theory, *Des. Codes Cryptogr.*, 71(1):47-56, 2014.