Des. Codes Cryptogr.
DOI 10.1007/s10623-012-9715-1

Constructing rate 1/p systematic binary quasi-cyclic codes based on the matroid theory

Guangfu Wu · Hsin-Chiu Chang · Lin Wang · T. K. Truong

Received: 28 October 2011 / Revised: 1 June 2012 / Accepted: 2 June 2012

Abstract In this paper, rate 1/p binary systematic quasi-cyclic (QC) codes are constructed based on Matroid Theory (MT). The relationship between the generator matrix and minimum distance d is derived through MT, which is benefit to find numbers of QC codes with large minimum distance by our Matroid search algorithm. More than seventy of QC codes that extend previously published results are presented. Among these codes, there are nine codes whose minimum distance is larger than those of the known codes found by Gulliver et al.

Keywords Matroid theory · Binary quasi-cyclic codes · Minimum distance · Matroid search algorithm

Mathematics Subject Classification (2010) 94B05

Communicated by J.-L. Kim.

G. Wu · L. Wang (✉)
Department of Communication Engineering, College of Information Science and Technology, Xiamen University, Xiamen 361005, Fujian Province, China
e-mail: wanglin@xmu.edu.cn

G. Wu
e-mail: wuguangfu@126.com

H.-C. Chang · T. K. Truong
Department of Information Engineering, I-Shou University, Kaohsiung, Taiwan
e-mail: newballch@gmail.com

T. K. Truong
Department of Computer Science and Engineering, National Sun Yat-Sen University, Kaohsiung, Taiwan
e-mail: truong@isu.edu.tw

Published online: 28 June 2012

1 Introduction

Coding theory with the protection of information against errors was first discovered by Shannon [1] in 1948. With the development of coding theory, one of the important issues is how to improve error-correcting capability, namely, $t = \lfloor (d-1)/2 \rfloor$ of linear codes, where d is the minimum distance of a code and $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x. In general, an optimal code is defined as one which has the maximum minimum distance with parameters n, k, where n is a code length and k is the number of information bits. During the past decades, many of good codes have been constructed. Among them, quasi-cyclic (QC) codes are known to be one of good codes [2].

In 1967, QC codes first found by Townsend and Weldon [3] have been extended by the authors [4–9]. Many good QC codes were discovered in [10]. Most of the works have concentrated on the algebraic-combinatorial computers search [11–18].

It follows from [11] that QC codes have a k × kp generator matrix of the form

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

where G_i is a k × k binary circulate matrix defined by

$$G_i = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{k-1} \\ g_{k-1} & g_0 & g_1 & \cdots & g_{k-2} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ g_1 & g_2 & g_3 & \cdots & g_0 \end{bmatrix} \tag{2}$$

To construct systematic QC code, let $G_0 = I_k$, where I_k is a k × k identity matrix.

In this paper, by a use of the connections between block codes and their matroids, a Matroid search algorithm is developed to construct the binary linear QC codes with a large minimum distance. More than seventy QC codes not included in Chen's table [10] are presented.

The structure of this paper is as follows: Sect. 2 contains a brief description of MT and the relationship between MT and coding. Section 3 proposes a new algorithm based on MT to construct binary linear QC codes. Some examples using this algorithm are presented and a new class of QC codes is constructed in Sect. 4. Finally, Sect. 5 concludes this paper with a brief summary.

2 Coding based on MT

2.1 A brief description of MT

In 1935, MT first suggested by Whitney [19] has been ignored for over 20 years until Tutte [20] introduced "matroids and graphs". Later, Edmonds and Fulkerson [21] recognized that matroids play an important role in transversal theory. In 1976, Greene [22] derived the MacWilliams identities from MT. Now, it has been extensively used in the aspects of combinatorial optimization [23], network theory [24,25], and coding theory [26,27]. Based on the ideas of Oxley's book [28], some useful definitions and notations of MT are given as below.

Definition 1 A matroid M is an ordered pair (E, I) consisting of a finite set E and a collection I of subsets of E satisfying the following three conditions:

(i) $\emptyset \in \mathrm{I}$.
(ii) if $I \in \mathrm{I}$ and $I' \subseteq I$,then $I' \in \mathrm{I}$

(iii) If I_1 and I_2 are in I and $|I_1| < |I_2|$, then there is an element e of $I_2 - I_1$ such that $I_1 \cup e \in \mathrm{I}$

Condition (*iii*) is called the independence augmentation axiom. If M is a matroid (E, I), then M is called a matroid on E. First, let the members of I and E be the independent sets of M and the ground set of M such that E(M) and I(M) are denoted as the ground set and the collection of independent sets of the matroid M, respectively. Also, let any subset of E which is not in I and a minimal dependent set in any matroid M be called a dependent set and a circuit of M, respectively. Any one-element circuit is called a loop and the set of all circuits is denoted by C(M). A maximal independent set in any matroid M must be a base of M and the set of all bases of M is thus represented as B(M). Finally, the cardinality of any base of M is defined to be the rank of M, denoted as r(M).

Definition 2 The rank function r(X) is the size of the largest independent subset of X.

Definition 3 Let $\mathrm{M}_1 = (E_1, \mathrm{I}_1)$ and $\mathrm{M}_2 = (E_2, \mathrm{I}_2)$ be two matroids, respectively. If there exists a mapping $\varphi : E_1 \rightarrow E_2$ such that $\varphi(I_1) \in \mathrm{I}_2$, where $I_1 \in \mathrm{I}_1$, then M_1 and M_2 are isomorphic.

It is well known that Matroids can be determined by their bases, circuits, rank function, respectively. Some examples of matroids are given in the following:

(1) Let E be the edge set of graph $\boldsymbol{G}$. A set of edges is independent if its subsets are a connected graph with no cycles. It is clear that aforementioned three conditions are satisfied. Such a matroid is the so-called a graphic matroid.
(2) Let $\mathrm{m} \leq \mathrm{n}$, where m and n are two positive integers. Also, let E and I be any n-element set and the collection of all subsets X of E satisfied $|\mathrm{X}| \leq \mathrm{m}$, respectively. Such a matroid is, what is called, a uniform matroid, namely, $\mathrm{U}_{\mathrm{m,n}}$.

2.2 Basic principle of coding based on MT

Many kinds of matroids can be constructed. One of the most important matroids is the binary matroid which corresponds to a binary linear code. Let G^* be a binary $\mathrm{k} \times \mathrm{n}$ matrix whose rank is equal to k. Also, let $v_1, v_2, \ldots, v_n$ be the column vectors of G^* and $E = \{1, 2, \ldots, n\}$. Additionally, I is defined as the collection of the subsets $I = \{i_1, \ldots, i_s\} \subseteq E$ such that the sequence of vectors $v_{i_1}, v_{i_2}, \ldots, v_{i_s}$ is linearly independent over the binary field F_2. Obviously, (E, I) satisfies the definition of matroid, it is called a vector matriod, and denoted as $\mathrm{M}[\mathrm{G}^*]$. In general, $\mathrm{M}[\mathrm{G}^*]$ does not uniquely determine the matrix G^*, but the vector matroid remains unchanged after any of the following operations:

(1) Interchange any two rows of G^*.
(2) Interchange any two columns of G^*.
(3) Replace a row with the sum of this row and any other row of G^*.

A binary matrix G^* is also the generator matrix of some binary linear codes with dimension $\mathrm{r}(\mathrm{M}[\mathrm{G}^*]) = \mathrm{rank}\,(\mathrm{G}^*)$. Thus, the matrix G^* can be transformed into the matrix of the form $(\mathrm{I_k}|\mathrm{G}')$ called a standard representative matrix for M, where G' is a $\mathrm{k} \times (\mathrm{n} - \mathrm{k})$ matrix. An (n, k) linear code C is said to be a maximum distance separable (MDS) if its minimum distance is equal to $\mathrm{n} - \mathrm{k} + 1$.If a code generated by G^* in this manner is an MDS code, then the matroid $\mathrm{M}[\mathrm{G}^*]$ is evidently an uniform matroid. Now, we present a new relation between matroids and codes based on the following definition:

Definition 4 Let $M_i = (E, I_i)$ for i = 1, …, n be matroids on the ground set E and J be a subset of E. If there exists maximum subsets $J_1, \ldots, J_n$ of J, where $J = J_1 \cup \ldots \cup J_n$ and $J_i \in I_i$, then J and $d_i = r(J_i)$ are called the connection of n matroids and the ith matroid connection degree, respectively.

Now, let G^* be a $k \times (2^k - 1)$ matrix whose ith column is a binary k-tuples representation of an integer i, where $i = 1, 2, \ldots, (2^k - 1)$. In particular, many different ways can be used to define Matroids. Here, we construct a serial of matroids $M_i^k = (E^k, I_i^k)$ for $i = 1, 2, \ldots, (2^k - 1)$, where $E^k = \{1, 2, \ldots, (2^k - 1)\}$ is the ground set, I_i^k is a collection of subsets X of E^k, and the binary k-tuples representations of elements in X are linearly independent over F_2 with the property that the product of its transpose with the i-th column of G^* (modulo 2) is zero. In this case, X is an independent set, for $i = 1, 2, \ldots, (2^k - 1)$. Note that the ground set of B_i^k is the set of elements j of E^k such that the product of the transpose of binary k-tuples representation of j with i-th column of G^* is zero. Obviously, $\left|B_i^k\right| = 2^{k-1} - 1$.

Theorem 1 Let G be a matrix whose columns are the binary k-tuples representation of elements in B. If a subset B of E^k satisfies $|B| = n$ and if $\max_{1 \le j \le 2^k - 1} \left|B \cap B_j^k\right| = t$, then the minimum distance d of a code C generated by G is $d = n - t$.

Proof Let $a = (a_1, a_2, \ldots, a_k)$ be a message vector, where $a_i \in \{0, 1\}$ for $1 \le i \le k$. In a codeword $c = a \cdot G_{k \times n} = (c_1, c_2, \ldots, c_n)$, it follows from the condition $\max_{1 \le j \le 2^k - 1} \left|B \cap B_j^k\right| = t$ that the number of zeros in such a codeword c are no more than t. Meanwhile, at least one codeword c having the number of zeros is t. Thus, the minimum distance of a code C is equal to $n - t$.

As will be seen, Theorem 1 can be used to compute the minimum distance of a code C.

3 Constructing binary linear QC codes

In this section, a new method is presented to search QC codes with a large minimum distance. Some useful definitions and theorems are given as below.

Definition 5 Let $E^k = \{1, 2, \ldots, (2^k - 1)\}$, E^k can be decomposited in terms of cyclotomic cosets $A_j^k = \{j \cdot 2^i \bmod (2^k - 1), i = 0, 1, \ldots, k-1\}$ which includes the set $A_{(2^k-1)}^k = \{2^k - 1\}$, where an odd j is less than 2^{k-1}. The index set denoted as J is also regarded as a vector. Finally $L^k = (|A_j^k|)$ is defined as a $1 \times |J|$ vector.

Example. For k = 4, we have $E^4 = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$. Thus $A_1^4 = \{1, 2, 4, 8\}$, $A_3^4 = \{3, 6, 12, 9\}$, $A_5^4 = \{5, 10\}$, $A_7^4 = \{7, 14, 13, 11\}$, and $A_{15}^4 = \{15\}$. Hence, we have $E^4 = A_1^4 \cup A_3^4 \cup A_5^4 \cup A_7^4 \cup A_{15}^4$, $L^4 = (4, 4, 2, 4, 1)$. $J = (1, 3, 5, 7, 15)$, and $|J| = 5$.

Theorem 2 For the given parameters k, m ∈ J, and i ∈ J, $|A_i^k \cap B_j^k|$ is invariable for all $j \in A_m^k$.

Proof The binary k-tuples representation of integer $j \in A_m^k$ is just cyclic shift of k-tuples representation of an integer m and the binary k-tuples representation of an integer $a \in A_i^k$ is just cyclic-shift of k-tuples representation of an integer i. According to the definition of B_j^k, the number of intersection $|A_i^k \cap B_j^k|$ is invariable, where $j \in A_m^k$.

Definition 6 The matrix R_k is defined as $R_k = (r_{i,j})$, where $r_{i,j} = |A^k_{J(i)} \cap B^k_{J(j)}|$ for J(i), J(j)∈J, $1 \le i \le |J|$, $1 \le j \le |J|$. J(i) and J(j) denote the ith coordinate of J, and the jth coordinate of J respectively.

Next, let $r = |\{i||A^k_{J(i)}| = k, 1 \le i \le |J|\}|$. $r*_{i,j}$ is defined by choosing the rows of R_k corresponding to $|A^k_{J(i)}| = k$, $1 \le i \le |J|$. Finally $R^*_k = (r*_{i,j})$ is defined by composing a new $r \times |J|$ submatrix corresponding to $L^{*k} = (|A^k_{J(i)}|)$, where $|A^k_{J(i)}| = k$ for $1 \le i \le |J|$

Example. For k = 4, we have

$$R_4 = \begin{pmatrix} 3\,2\,2\,1\,0 \\ 2\,2\,0\,2\,4 \\ 2\,0\,2\,1\,2 \\ 1\,2\,2\,3\,0 \\ 0\,1\,1\,0\,1 \end{pmatrix}, \quad R^*_4 = \begin{pmatrix} 3\,2\,2\,1\,0 \\ 2\,2\,0\,2\,4 \\ 1\,2\,2\,3\,0 \end{pmatrix}.$$

Theorem 3 If there is a vector $X = (x_1, x_2, \ldots, x_{|J|})$, where $x_i \in \{0, 1\}$ for $1 \le i \le |J|$, and a vector $Y = (y_1, y_2, \ldots, y_{|J|})$ satisfying

$$X \cdot R_k = Y \tag{4}$$
$$L^k \cdot X^T = n \tag{5}$$

then there exists a binary (n, k, d) code such that its minimum distance is equal to n-max$\{y_1, y_2, \ldots, y_{|J|}\}$.

Proof Let the set $I = \{i|x_i \ne 0, 1 \le i \le |J|\}$. Conditions (4) and (5) are satisfied. Then let G be the matrix such that whose columns are the binary k-tuples representation of elements in $B = \bigcup_{i \in I} A^k_{J(i)}$. Owing to the condition (5), we have $|B| = n$ which is the code length. Since condition (4) is hold, according to Theorem 1

$$\max_{1 \le j \le 2^k - 1} \left| B \cap B^k_j \right| = \max\{y_1, y_2, \ldots, y_{|J|}\}.$$

Thus, the minimum distance of a binary linear code is n- max$\{ y_1, y_2, \ldots, y_{|J|} \}$.

From Theorem 3, to construct QC code of the form $G = [G_0, G_1, \ldots, G_{p-1}]$, a serials of A^k_j should be chosen so that $|A^k_j| = k$. If only the systematic QC code is considered, A^k_1 must be chosen in the code.

Example. For k = 4, obviously, $A^4_1 = \{1, 2, 4, 8\}$, $A^4_3 = \{3, 6, 12, 9\}$, $A^4_5 = \{5, 10\}$, $A^4_7 = \{7, 14, 13, 11\}$, $A^4_{15} = \{15\}$. $|A^4_1| = |A^4_3| = |A^4_7| = 4$, $|A^4_5| = 2$, and $|A^4_{15}| = 1$. In this case, only A^4_1, A^4_3 and A^4_7 may be chosen so that $L^{*4} = (4, 4, 4)$, $X = (1, 1, 0)$ or (1,0,1). The generator matrix created by $A^k_{i_1} \cup A^k_{i_2} \cup \cdots \cup A^k_{i_p}$ can be represented as $G^k(i_1, i_2, \ldots, i_p)$. If we choose A^4_1 and A^4_3 then the (8, 4, 3) code is constructed. Similarly, the (8, 4, 4) code can be constructed by choosing A^4_1 and A^4_7. The two generator matrixes are given below.

$$G^4(1, 3) = [A^4_1, A^4_3] = \begin{bmatrix} 1\,0\,0\,0\,1\,0\,0\,1 \\ 0\,1\,0\,0\,1\,1\,0\,0 \\ 0\,0\,1\,0\,0\,1\,1\,0 \\ 0\,0\,0\,1\,0\,0\,1\,1 \end{bmatrix}$$

and

$$G^4(1,7) = [A_1^4, A_7^4] = \begin{bmatrix} 1\,0\,0\,0\,1\,0\,1\,1 \\ 0\,1\,0\,0\,1\,1\,0\,1 \\ 0\,0\,1\,0\,1\,1\,1\,0 \\ 0\,0\,0\,1\,0\,1\,1\,1 \end{bmatrix}$$

Again, from Theorem 3, the minimum distance of a code is easily obtained. Clearly, the code generated by $G^4(1,7)$ is better than the other from the above example.

4 Matroid search algorithm for systematic binary QC codes

In what follows, some mathematical notations needed in deriving the Matroid search algorithm are given; that is, | S| denotes the number of elements in set S, V^L and V^T denote the locations of vector V nonzero coordinates, and the transpose of a vector V respectively, and n_k^* denotes the k-tuples binary representation of an integer n.

To construct the optimal systematic QC codes of rate 1/p, using Theorem 3, the minimum distance of the code generated by $A_{i_1}^k \cup A_{i_2}^k \cup \cdots \cup A_{i_p}^k$ is related to the maximum of the row sums of the corresponding columns of R_k^*. Because n=kp and the chosen A_1^k, we can set $X^* = \{x_r^* \,|\, |x_r^{*L}| = p, x_r^{*L} \cap 1_r^{*L} = \{1\}, 1 \le x \le 2^r - 1\}$ this fact leads to reduce the computational complexity of constructing the QC code, where$|X^*| = \binom{r-1}{p-1}$. The Matroid search algorithm is described in the following four steps.

(1) Given two parameters k and p, create R_k^*, L^{*k}, and the corresponding vectorX^*,
(2) According to Theorem 3, compute $y_i = \max\{x_r^* \cdot R_k^*\}$, where $x_r^* \in X^*, i = 1, \ldots, |X^*|$.
(3) To construct the largest minimum distance, according to Theorem 1, choose $d_0 = \min\{y_1, y_2, \ldots, y_{|X^*|}\}$.
(4) Compute kp- d_0.

With the aid of Theorem 3, the code can be constructed such that its largest minimum distance is equal to kp- d_0.

The Matroid search algorithm can not only guarantee to find all the systematic QC codes for the given parameters k and p, but also more easily carried out paralleling computation owning to its decomposition. Simulation results show that many good systematic QC codes have been obtained. More than seventy systematic QC codes not included in Chen's table [10] are found in this paper. Among these codes, the (78, 13, 31), (130, 13, 55), (156, 13, 67), (182, 13, 80), (126, 14, 52), (140, 14, 58), (210, 14, 90),(238, 14, 104) and (252, 14, 110) systematic QC codes whose minimum distance is larger than those of the (78, 13, 30), (130, 13, 54), (156, 13, 66), (182, 13, 78), (126, 14, 50), (140, 14, 57), (210, 14, 89), (238, 14, 102) and (252, 14, 108) systematic QC codes are given respectively, in the table of [12,15].

Table 1 lists the number of systematic QC codes by using an exhaustive search. Table 2 is the results of systematic QC codes through the Matroid search algorithm. Here some parameters of systematic QC codes listed in Table 1 are found in the table of [15]. Most of our new systematic QC codes marked by boldface are presented in Tables 1 and 2.

According to the code bounds given in [29], some optimal systematic QC codes are given in Table 3. Generator matrix representation can be used to eliminate the uncertainty of minimum distance from the systematic QC codes.

In Table 4, systematic QC codes whose minimum distance is larger than that of systematic codes in [12,15] are given.

Table 1 Number of systematic QC codes with maximum minimum distance d

(pk, k) code	d	Number of codes with distance d	(pk, k) code	d	Number of codes with distance d
(14, 7)	4	12	(160, 8)	78	16
(21, 7)	8	23	(168, 8)	81	52
(28, 7)	12	14	(176, 8)	86	64
(35, 7)	16	10	(184, 8)	90	32
(42, 7)	19	11	(192, 8)	96	1
(49, 7)	22	140	(200, 8)	98	50
(56, 7)	26	6	**(208, 8)**	**102**	74
(63, 7)	31	1	**(216, 8)**	**106**	59
(70, 7)	33	7	**(224, 8)**	**112**	1
(77, 7)	36	723	**(232, 8)**	**114**	14
(84, 7)	40	251	**(240, 8)**	**120**	1
(91, 7)	44	64	(18, 9)	6	3
(98, 7)	48	7	(27, 9)	10	39
(105, 7)	52	2	(36, 9)	14	177
(112, 7)	56	2	(45, 9)	18	4776
(119, 7)	59	1	(54, 9)	23	465
(126, 7)	63	1	(63, 9)	28	201
(16, 8)	5	4	(72, 9)	32	9147
(24, 8)	8	204	(81, 9)	36	185916
(32, 8)	12	802	(90, 9)	40	628470
(40, 8)	16	2798	(99, 9)	46	540
(48, 8)	22	8	**(423, 9)**	**208**	31221
(56, 8)	24	13938	**(432, 9)**	**213**	33
(64, 8)	28	24896	**(441, 9)**	**218**	22
(72, 8)	32	58122	**(450, 9)**	**222**	17
(80, 8)	37	14	**(459, 9)**	**228**	21
(88, 8)	40	123874	**(468, 9)**	**232**	74
(96, 8)	46	16	**(477, 9)**	**236**	91
(104, 8)	48	271574	**(486, 9)**	**241**	20
(112, 8)	54	24	**(495, 9)**	**246**	7
(120, 8)	57	15	**(504, 9)**	**252**	1
(128, 8)	64	1	(20, 10)	6	17
(136, 8)	66	8	(30, 10)	10	614
(144, 8)	70	48	(40, 10)	16	171
(152, 8)	74	8	(50, 10)	20	8237

In Tables 3 and 4, the weight enumerators of seventeen codes are given as follows:

(1) The weight enumerators of (176, 8, 86) QC code are 0_1, 86_144, 88_56, 94_48, 96_3, 104_4.
(2) The weight enumerators of (184, 8, 90) QC code are 0_1, 90_128, 92_48, 94_32, 96_14, 98_32, 128_1.

Table 2 Maximum minimum distance for (pk, k) systematic QC codes

k	p 19	20	21	22	23	24	25	26	27	28	29	30
9	81	87	92	96	100	104	110	**112**	**118**	**122**	**126**	**130**
10	88	94	97	104	108	112	**118**	**122**	**128**	**132**	**138**	**142**
11	**96**	**100**	**106**	**112**	**116**	**123**	**128**	**132**	**138**	**144**	**148**	**155**
12	**102**	**108**	**114**	**120**	**126**	**132**	**138**	**144**	**148**	**156**	**160**	**166**
13	**110**	**116**	**122**	**128**	**135**	**140**	**148**	**152**	**160**	**167**	**172**	**180**
14	**116**	**124**	**130**	**136**	**144**	**150**	**156**	**164**	**170**	**176**	**184**	**192**

Table 3 Their generator matrixes of some optimal systematic QC codes

Code	d_{min}	Generator matrix representation
(176, 8)	86	1, 13, 15, 19, 21, 23, 25, 27, 29, 37, 43, 45, 53, 55, 59, 61, 63, 87, 91, 95, 111, 127
(184, 8)	90	1, 3, 5, 7, 11, 13, 15, 19, 21, 23, 25, 31, 37, 39, 47, 53, 55, 59, 61, 87, 91, 111, 127
(192, 8)	96	1, 3, 7, 9, 11, 13, 19, 21, 23, 25, 29, 31, 37, 43, 47, 53, 55, 59, 61, 63, 87, 91, 111, 127
(200,8)	98	1, 3, 5, 7, 9, 11, 13, 15, 19, 21, 23, 25, 31, 37, 43, 47, 53, 55, 59, 61, 63, 87, 91, 111, 127
(208, 8)	102	1, 7, 11, 13, 15, 19, 21, 23, 25, 27, 29, 31, 37, 43, 45, 47, 53, 55, 59, 61, 63, 87, 91, 95, 111, 127
(224, 8)	112	1, 3, 5, 7, 9, 11, 13, 19, 21, 23, 25, 27, 29, 31, 37, 39, 43, 47, 53, 55, 59, 61, 63, 87, 91, 95, 111, 127
(198, 9)	96	1, 5, 11, 13, 15, 23, 25, 35, 41, 47, 53, 59, 61, 77, 79, 91, 109, 117, 127, 187, 191, 239
(216,9)	104	1, 3, 7, 13, 17, 21, 23, 29, 31, 43, 51, 53, 55, 57, 79, 85, 93, 95, 103, 111, 123, 171, 191, 239.

Table 4 Larger minimum distance systematic QC codes and their generator matrix representation

Code	d_{min}	Generator matrix representation
(78, 13)	31	1, 219, 279, 685, 691, 1491
(130, 13)	55	1, 173, 571, 613, 829, 845, 875, 1267, 1661, 1877
(156, 13)	67	1, 127, 241, 301, 433, 463, 1237, 1367, 1755, 1771, 1919, 3007
(182, 13)	80	1, 145, 171, 231, 295, 319, 731, 851, 1323, 1525, 1783, 1851, 2027, 2747
(126, 14)	52	1, 25, 319, 753, 885, 1235, 1383, 1405, 1881
(140, 14)	58	1, 57, 933, 1359, 1383, 1693, 1915, 2011, 2429, 6071
(210, 14)	90	1, 31, 115, 117, 125, 349, 485, 727, 783, 1391, 1395, 2381, 1551, 3029, 3323
(238, 14)	104	1, 245, 411, 719, 887, 1099, 1305, 1533, 1639, 1999, 2655, 2783, 3071, 3563, 4091, 5819, 7935
(252, 14)	110	1, 115, 283, 339, 395, 451, 591, 787, 817, 1403, 1493, 1593, 1839, 2003, 2023, 2397, 2715, 3387

(3) The weight enumerators of (192, 8, 96) QC code are 0_1,96_252, 128_3.
(4) The weight enumerators of (200, 8, 98) QC code are 0_1,98_104,100_68,102_40,104_40,120_2,128_1.
(5) The weight enumerators of (208, 8, 102) QC code are 0_1,102_112,104_52,106_64,110_16,112_10,128_1.

(6) The weight enumerators of (224, 8, 112) QC code are 0_1, 112_248,128_7.
(7) The weight enumerators of (198, 9, 96) QC code are 0_1, 96_345, 104_144, 120_12, 144_1.
(8) The weight enumerators of (216, 9, 104) QC code are 0_1, 104_252, 108_100,112_108, 120_30, 128_9, 132_3.
(9) The weight enumerators of (78,13, 31) QC code are 0_1, 31_377, 32_585, 35_1001, 36_1066, 39_1314, 40_1456, 43_1066, 44_780, 47_325, 48_182, 51_13, 52_26.
(10) The weight enumerators of (130,13, 55) QC code are 0_1, 55_351, 56_494, 59_676, 60_780, 63_1079, 64_1066, 67_962, 68_988, 71_689, 72_520, 75_273, 76_208, 79_65, 80_39, 91_1.
(11) The weight enumerators of (156,13, 67) QC code are 0_1, 67_247, 68_429, 71_767, 72_741, 75_871, 76_858, 79_871, 80_988, 83_741, 84_689,87_429,88_273, 91_157,92_104,95_13,96_13
(12) The weight enumerators of (182,13, 80) QC code are 0_1, 79_338, 80_299, 83_533, 84_806, 87_741, 88_715, 91_755_92_949, 95_936,96_728, 99_559, 100_364, 103_169,104_169,107_65,108_65.
(13) The weight enumerators of (126, 14, 52) QC code are 0_1, 52_896, 56_2256, 60_3843, 64_4487, 68_3283, 72_1232, 76_329, 80_56, 84_1.
(14) The weight enumerators of (140, 14, 58) QC code are 0_1, 58_406, 60_693, 62_994, 64_1470,66_1610,68_1967, 70_2046,72_2058, 74_1918, 76_1239 78_826, 80_623,82_322,84_141,86_70.
(15) The weight enumerators of (210, 14, 90) QC code are 0_1, 80_793, 84_1261, 88_1573, 92_1937, 96_1352, 100_871, 104_287, 108_91, 112_26.
(16) The weight enumerators of (238,14,104) QC code are 0_1, 104_665,108_1400,112_2452,116_2968,120_3024,124_2828,128_1827, 132_784,136_350,140_84,168_1.
(17) The weight enumerators of (252,14,110) QC code are 0_1,110_364, 112_364,114_658,116_910,118_896,120_1302,122_1274, 124_1610,126_1778,128_1652,130_1386,132_1176,134_910,136_693,138_462, 140_380,142_266,144_189,146_28,148_14,150_42, 152_14,156_14,168_1.

5 Conclusion

Matroids may be used extensively in error corrected codes. In this paper, based on MT, a Matroid search algorithm through the derived relationship between the generator matrix and minimum distance d is proposed to construct the systematic QC code with a larger minimum distance when the parameters (k, p) are given. It can be easily decomposed for computer simulation relative to other search algorithms due to our algorithm paralleling characteristics. It is found that more than seventy new systematic QC codes are constructed through the proposed algorithm, and exist eight these codes in possession of larger minimum distance than the previous known systematic QC codes. Obviously, how to design good systematic QC codes is of interest in coding theory. It is expected that an extension of the idea proposed in this paper can be used to faster construct rate δ/p systematic codes for integer $\delta > 1$.

Acknowledgments This work was supported by the National Science foundation of China, under Grant No. 60972053.

References

1. Shannon C.: A mathematical theory of communication. Bell Syst. Tech. J. **27**, 379–423 and 623–656 (1948).
2. Weldon E.J. Jr.: Long quasi-cyclic codes are good. IEEE Trans. Inf. Theory **IT-13**(1), 130 (1970).
3. Townsend R.L., Weldon E.J. Jr.: Self-orthogonal quasi-cyclic codes. IEEE Trans. Inf. Theory **IT-13**(2), 183–195 (1967).
4. Karlin M.: New binary coding results by circulants. IEEE Trans. Inf. Theory **IT-15**(1), 81–92 (1969).
5. Karlin M.: Decoding of circulant codes. IEEE Trans. Inf. Theory **IT-16**(6), 797–802 (1970).
6. Chen C.L., Peterson W.W., Weldon E.J. Jr.: Some results on quasi-cyclic codes. Inf. Control **15**, 407–423 (1969).
7. Hoffner C.W., Reddy S.M.: Circulant bases for cyclic codes. IEEE Trans. Inf. Theory **IT-16**(4), 511–512 (1970).
8. Tavares S.E., Bhargava V.K., Shiva S.G.S.: Some rate-p/(p + 1) quasi-cyclic codes. IEEE Trans. Inf. Theory **IT-20**(1), 133–135 (1974).
9. Bhargava V.K., Seguin G.E., Stein J.M.: Some (mk, k) cyclic codes in quasi-cyclic form. IEEE Trans. Inf. Theory **IT-24**(5), 630–632 (1978).
10. Chen Z.: [Online].(2011), Available: http://www.tec.hkr.se/~chen/research/codes/. Accessed Septemper 2011).
11. van Tilborg H.C.A.: On quasi-cyclic codes with rate 1/m. IEEE Trans. Inf. Theory **IT-24**(5), 628–629 (1978).
12. 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).
13. Gulliver T.A., Bhargava V.K.: Nine good (m-1)/pm quasi-cyclic codes. IEEE Trans. Inf. Theory **IT-38**(4), 1366–1369 (1992).
14. 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).
15. Gulliver T.A., Bhargava V.K.: An updated table of rate 1/p binary Quasi-Cyclic codes. Appl. Math. Lett. **8**(5), 81–86 (1995).
16. Chen Z.: Six new binary quasi-cyclic codes. IEEE Trans. Inf. Theory **IT-40**(5), 1666–1667 (1994).
17. Chen Z.: On Computer Search for Good Quasi-Cyclic Codes. IEEE Symp. on Information Theory, Norway (1994).
18. Zhi C.: New results on binary quasi-cyclic codes. Proceeding IEEE Intern. Symp. on Information Theory, ISIT2000, Sorrento, Italy (2000).
19. Whitney H.: On the abstract properties of linear dependence. Am. J. Math. **57**, 509–533 (1935).
20. Tutte W.T.: Matroids and graphs. Trans. Am. Math. Soc. **90**, 527–552 (1959).
21. Edmonds J., Fulkerson D.R.: Transversals and matroid partition. J. Res. Natl. Bur. Stand. **69B**, 147–153 (1965).
22. Greene C.: Weight enumeration and the geometry of linear codes. Studia Appl. Math. **55**, 119–128 (1976).
23. Geelen J., Gerards B., Whittle G.: Towards a matroid-minor structure theory. In: Grimmett G., McDiarmid C. (eds.) Combinatorics, Complexity and Chance. A Tribute to Dominic Welsh. Oxford University Press (2007).
24. Ahlswede R., Cai N., Li S.-Y.R., Yeung R.W.: Network information flow. IEEE Trans. Inf. Theory **46**, 1204–1216 (2000).
25. Dougherty R., Freiling C., Zeger K.: Networks, matroids, and non-Shannon information inequalities. IEEE Trans. Inf. Theory **53**(6), 1949–1969 (2007).
26. Feldman J., Wainwright M.J., Karger D.R.: Using linear programming to decode binary linear codes. IEEE Trans. Inf. Theory **51**(3), 954–972 (2005).
27. Barg A.: The matroid of supports of a linear code. Appl. Algebra Eng. Commun. Comput. **8**(2), 165–172 (1997).
28. Oxley J.G.: Matroid Theory. Oxford University Press, Oxford (1992).
29. Grassl M.: Tables of linear codes and quantum codes. [Online]. Available at http://www.codetables.de. Accessed Septemper 2011.