Published in IET Communications
Received on 29th July 2013
Revised on 18th November 2013
Accepted on 6th December 2013
doi: 10.1049/iet-com.2013.0671

ISSN 1751-8628

Use of matroid theory to construct a class of good binary linear codes

Guangfu Wu[1], Lin Wang[2], Trieu-Kien Truong[3]

[1]*Department of Information Engineering, Jiangxi University of Science and Technology, Ganzhou 341000, People's Republic of China*
[2]*Department of Communication Engineering, Xiamen Univ., Fujian 361005, People's Republic of China*
[3]*Department of Information Engineering, I-Shou University and Department of computer Science and engineering, National Sun Yat-Sen University Taiwan*
E-mail: wuguangfu@126.com

Abstract: It is still an open challenge in coding theory how to design a systematic linear (n, k) – code C over GF(2) with maximal minimum distance d. In this study, based on matroid theory (MT), a limited class of good systematic binary linear codes (n, k, d) is constructed, where $n = 2^{k-1} + \cdots + 2^{k-\delta}$ and $d = 2^{k-2} + \cdots + 2^{k-\delta-1}$ for $k \geq 4$, $1 \leq \delta < k$. These codes are well known as special cases of codes constructed by Solomon and Stiffler (SS) back in 1960s. Furthermore, a new shortening method is presented. By shortening the optimal codes, we can design new kinds of good systematic binary linear codes with parameters $n = 2^{k-1} + \cdots + 2^{k-\delta} - 3u$ and $d = 2^{k-2} + \cdots + 2^{k-\delta-1} - 2u$ for $2 \leq u \leq 4$, $2 \leq \delta < k$. The advantage of MT over the original SS construction is that it has an advantage in yielding generator matrix on systematic form. In addition, the dual code $C^{\perp}$ with relative high rate and optimal minimum distance can be obtained easily in this study.

1 Introduction

In 1948, Shannon [1] first initiated coding theory with the protection of information against errors. 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 and $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x. Generally, the constraint relation of parameters n, k and d can generate all kinds of bounds which play an important role in searching good codes. During the past decades, many bounds, such as the hamming bound, the singleton bound, the Plotkin bound, the Gilbert–Varshamov bound and the Griesmer bound (GB) are derived. Among them, the GB is only considered in this paper. It follows from Griesmer [2] showing that the condition given below is definitely satisfied for any binary linear (n, k, d) – code. That is

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{2^i} \right\rceil \tag{1}$$

which is the so-called GB, where $\lceil x \rceil$ denotes the smallest integer larger than or equal to x. It is well-known that a code whose minimum distance matches the GB, that is, the upper bound is called an optimal code. In fact, some of optimal codes are given in [3]. Actually, codes meeting the GB have been extensively studied by Solomon *et al.* [4], Belov [5] and Helleseth and van Tilborg [6–10]. It is found in [10, 11] that a finite projective geometry can be used in constructing those codes. Especially in [9], van Tilborg constructed the isomorphic codes with parameters $n = 2^{k-1} + \cdots + 2^{k-\delta}$, $d = 2^{k-2} + \cdots + 2^{k-\delta-1}$ or $n = 2^{k-1} + 2^{k-2} - 3$, $d = 2^{k-2} + 2^{k-3} - 2$ and proved that up to isomorphism they are unique. However, all the codes are unsystematic form. In this paper, matroid theory (MT) is shown to be utilised to construct a limited class of systematic codes which meet the GB. Generally speaking, a linear (n, k, d) code C is said to be a good code if it satisfies one of the following conditions.

(a) For a given n and k, d is maximised to maximise the code's error-correcting capability.
(b) For a given n and d (resp., k and d), k is maximised (resp., n is minimised) to maximise the transmission rate.

In this paper, MT can make it possible for constructing a new class of good binary linear (n, k, d)-codes C when $n = 2^{k-1} + \cdots + 2^{k-\delta} - 3u$ and $d = 2^{k-2} + \cdots + 2^{k-\delta-1} - 2u$ for $2 \leq u \leq 4$, $1 \leq \delta < k$ and $k \geq 6$. Although the matroid construction is more complicated than the Solomon–Stiffler construction [4], however, it has an advantage in obtaining generator matrix on systematic form. Furthermore, by choosing some special set B, 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 binary quasi-cyclic codes whose minimum distance is larger than those of the previous known codes have been obtained [12]. Although, in this paper, we found set B can be chosen

according to the bases of MT simply and the codes obtained are well known as a special cases of codes constructed by Solomon *et al.* With the presented shortening method based on the optimal codes, new kinds of good systematic binary linear codes can be obtained.

The structure of this paper is as follows: Section 2 contains a brief description of MT and the relationship between MT and coding. In Section 3, a limited class of good binary linear codes (n, k, d) is constructed through MT. In Section 4, a shortening method is presented and a new class binary linear codes is constructed. The dual codes of (n, k, d)-code is considered in Section 5. Finally, Section 6 concludes this paper with a brief summary.

2 Coding based on MT

In 1935, MT first introduced by Whitney [13] has been ignored for over 20 years until Tutte [14] introduced 'matroids and graphs'. Later, Edmonds and Fulkerson [15] recognised that matroids are important in transversal theory. In 1976, Greene [16] derived the MacWilliams identities from MT. Now, it has been extensively used in the aspects of combinatorial optimisation [17], network theory [18, 19] and coding theory [20, 21]. Based on the ideas of Oxley's book [22], 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.

(a) $\emptyset \in I$.
(b) If $I \in I$ and $I' \subseteq I$, then $I' \in I$.
(c) If I_1 and I_2 are in I, if $|I_1| < |I_2|$, then here exists an element e of $I_2 - I_1$ such that $I_1 \cup e \in I$.

Condition (c) 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 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). 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 largest independent subset of X.

Definition 3: Let $M_1 = (E_1, I_1)$ and $M_2 = (E_2, I_2)$ be two matroids, respectively. If there exists a mapping $\varphi: E_1 \to E_2$ such that $\varphi(I_1) \in I_2$, where $I_1 \in I_2$, then M_1 and M_2 are isomorphic.

Note that matroids can be determined by their bases, circuits or rank function, respectively.

One of the most important matroids is the binary matroid which corresponds to a binary linear code. Let $\boldsymbol{G}$ be a binary $k \times n$ matrix whose rank is equal to k. Also, let v_1, v_2, …, v_n be the column vectors of $\boldsymbol{G}$ and $E = \{1,2,\ldots,n\}$. Additionally, I is defined as a collection of the subsets $I = \{i_1,\ldots, i_s\} \subseteq E$ such that the sequence of vectors v_{i1}, v_{i2}, …, v_{is} is linearly independent over the field GF(2). Obviously, (E, I) denoted by M[$\boldsymbol{G}$] satisfies the definition of a vector matroid given above. In general, M[$\boldsymbol{G}$] does not uniquely determine the matrix $\boldsymbol{G}$, but the vector matroid remains unchanged after any of the following operations:

(a) Interchange any two rows of $\boldsymbol{G}$.
(b) Interchange any two columns of $\boldsymbol{G}$.
(c) Replace a row with the sum of this row and any other row of $\boldsymbol{G}$.

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

Definition 4: Let $M_i = (E_i, I_i)$ for $1 \le i \le n$ 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 $G(K)$ be a $k \times (2^k - 1)$ matrix whose ith column is the binary k-tuples representation of integer i, where $i = 1,\ldots, (2^k-1)$. In particular, many different ways can be used to define Matroids. Here, we construct a serial of matroids $M_i^k = \left(E^k, I_i^k\right)$ 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 representation of elements in X is satisfied such that the product of its transpose with the ith column is an even number. For this case, X is also called an independent set. Every matriod having only one base is denoted as B_i^k for $i = 1, 2,\ldots,(2^k-1)$. Obviously, $\left|B_i^k\right| = 2^{k-1} - 1$. The base of B_i^{k+1} can be derived from B_i^k. Towards this end, the following theorems and corollaries are found to be useful.

Theorem 1: For a given integer e, let $\{e + X\} = \{e + x | \forall x \in X\}$. Thus, B_i^{k+1} for $k \ge 2$ can be derived explicitly via the following recursive equations:

$$B_i^{k+1} = \begin{cases} B_i^k \cup \{2^k\} \cup \{2^k + B_i^k\}, & 1 \le i \le 2^k - 1 \\ \{1, 2, 3, \ldots, 2^k - 1\}, & i = 2^k \\ B_j^k \cup \left\{2^k + \overline{B_j^k}\right\}, & 2^k < i < 2^{k+1}, j = i - 2^k \end{cases} \tag{2}$$

Where $\overline{B_j^k} = E^k - B_j^k = \left\{x | x \in E^k, x \notin B_j^k\right\}$

Proof: From the definition of $G(K)$, We have $G(K + 1)$

$$G(K+1) = \begin{pmatrix} G(K) & D_1^{\mathrm{T}} & G(K) \\ D_2 & 1 & P \end{pmatrix}_{(k+1)\times(2^{(k+1)}-1)}$$

where $P = (1, \ldots, 1)_{1\times(2^k-1)}$, $D_1 = (0, \ldots, 0)_{1 \times k}$,

doi: 10.1049/iet-com.2013.0671

$D_2 = (0, \ldots, 0)_{1\times(2^k-1)}$ and $G(K) = G_{k\times(2^k-1)}$. (2) can be obtained immediately from the definition of I_i^{k+1}. □
Theorem 1 can be used to compute the base with the increasing k.

Corollary 1: Let b is an integer, where $1 \le b \le 2^k-1$, such that $b \in B_i^k$. Then $b \in B_i^m$ for all $m \ge k$, $1 \le i \le 2^k-1$.

Proof: Corollary 1 can be obtained immediately from Theorem 1. □

Property: $m \in B_i^k$ if and only if $i \in B_m^k$ for $1 \le i \le 2^k-1$and $1 \le m \le 2^k-1$.

Proof: Let column vector $\boldsymbol{g}_i$ and $\boldsymbol{g}_m$ be the binary k-tuples representation of integer i and m, respectively. From the definition of B_i^k, if $m \in B_i^k$, then $\boldsymbol{g}_m^{\mathrm{T}} \cdot \boldsymbol{g}_i \equiv 0(\mathrm{mod}\,2)$. However, $\boldsymbol{g}_i^{\mathrm{T}} \cdot \boldsymbol{g}_m \equiv 0(\mathrm{mod}\,2)$. Thus, $i \in B_m^k$ and vice versa.

Corollary 2:

$$\left|B_{i_1}^k \cap B_{i_2}^k\right| = 2^{k-2} - 1 \text{ for } i_1 \ne i_2,\ 1 \le i_1, i_2 \le 2^k - 1 \text{ and } k \ge 3 \tag{3}$$

Proof: We use induction on k. For $k=3$, we have $B_1^3 = \{2, 4, 6\}$, $B_2^3 = \{1, 4, 5\}$, $B_3^3 = \{3, 4, 7\}$, $B_4^3 = \{1, 2, 3\}$, $B_5^3 = \{2, 5, 7\}$, $B_6^3 = \{1, 6, 7\}$ and $B_7^3 = \{3, 5, 6\}$, then $\left|B_{i_1}^k \cap B_{i_2}^k\right| = 2^{3-2} - 1 = 1$.

Assuming the validity of Corollary 2 for $k=q$ $(q \ge 3)$. When $k=q+1$, according to Theorem 1, we have $\left|B_{i_1}^{q+1} \cap B_{i_2}^{q+1}\right| = 2^{q-2} - 1 + 1 + 2^{q-2} - 1 = 2^{q-1} - 1$, where $i_1 \ne i_2$, $1 \le i_1, i_2 \le 2^q-1$. If $i_1 \ne i_2$ and $2^q \le i_1, i_2 \le 2^{q+1}-1$, then

$$\left|B_{i_1}^{q+1} \cap B_{i_2}^{q+1}\right| = \left(2^{q-2} - 1\right) + \left(2^{q-1} - 1\right) - 2 \cdot \left(2^{q-2} - 1\right) + \left(2^{q-2} - 1\right) = 2^{q-1} - 1$$

If $i_1 = 2^q$ or $i_2 = 2^q$, then $\left|B_{i_1}^{q+1} \cap B_{i_2}^{q+1}\right| = \left|B_{i_1}^q\right| = \left|B_{i_2}^q\right| = 2^{q-1} - 1$.

Suppose $1 \le i_1 \le 2^q-1$ and $2^q < i_2 \le 2^{q+1}-1$. If $i_1 = i_2 - 2^q$, then

$$\left|B_{i_1}^{q+1} \cap B_{i_2}^{q+1}\right| = \left|B_{i_1}^q\right| = 2^{q-1} - 1$$

Otherwise, $\left|B_{i_1}^{q+1} \cap B_{i_2}^{q+1}\right| = \left|B_{i_1}^q \cap B_{i_2-2^q}^q\right| + \left|B_{i_1}^q \cap \overline{B_{i_2-2^q}^q}\right| = 2^{q-1} - 1$.

From the above results, Corollary 2 holds for $k=q+1$. The proof is thus complete. □

With the aid of Corollary 2, the intersection of any two different bases has the same cardinality $2^{k-2}-1$.

Theorem 2: Let B be a subset of E^k and satisfy $|B| = n$, $\max_{1\le j\le 2^k-1} \left|B \cap B_j^k\right| = t$. Let t be denoted as d_m and $\boldsymbol{G}^*$ be the matrix whose columns are the binary k-tuples representation of elements in B. Then the minimum distance d of code C generated by $\boldsymbol{G}^*$ satisfies $d = n\text{-}t$.

Proof: In a non-zero codeword $c = \left(a_1, \ldots, a_k\right) \times G_{k\times n}^* = \left(c_1, \ldots, c_n\right)$, where $a_i \in \{0,1\}$ for $1 \le i \le k$, it follows from the condition $d_m = t$ that the number of zeros of a codeword is no more than t. Meanwhile, at least one codeword C having the number of zeros is t. Hence, the minimum distance of code C is equal to $n\text{-}t$. □

As will be seen, Theorem 2 can be used to compute the minimum distance of code C.

For any integer q, where$1 \le q \le 2^k-1$, there is a unique binary sequence $a_1,\ldots, a_k$ denoted as A_q^k such that $q = \sum_{i=1}^k a_i 2^{i-1}$, where $a_i \in \{0,1\}$.

Theorem 3: $q \in B_{(2^k-1)}^k$ if and only if the weight of A_q^k are even.

Proof: If the weight of A_q^k is even, it is known the coordinates of the (2^k-1)th column of matrix $G(K)$ are all one. From the definition of independence, we have$q \in B_{(2^k-1)}^k$ and vice versa. □

According to Theorem 3, it is easily to express the base $B_{(2^k-1)}^k$.

Theorem 4: $\left|B_{i_1}^k \cap B_{i_2}^k \cap B_{i_3}^k\right| = 2^{k-2} - 1$ or $\left|B_{i_1}^k \cap B_{i_2}^k \cap B_{i_3}^k\right| = 2^{k-3} - 1$ for $1 \le i_1, i_2, i_3 \le 2^k - 1$ and $k \ge 3$.

Proof: Let column vector g_{i_r} and g_x be the binary k-tuples representation of integer i_r and x, respectively, for $r = 1$, 2, 3 and $k \ge 3$. A set of equations is given by

$$\begin{cases} g_{i_1}^{\mathrm{T}} \cdot g_x \equiv 0(\mathrm{mod}\,2) \\ g_{i_2}^{\mathrm{T}} \cdot g_x \equiv 0(\mathrm{mod}\,2) \\ g_{i_3}^{\mathrm{T}} \cdot g_x \equiv 0(\mathrm{mod}\,2) \end{cases} \tag{4}$$

When vectors g_{i_r} are independent, the number of solutions is $\left|B_{i_1}^k \cap B_{i_2}^k \cap B_{i_3}^k\right| = 2^{k-3} - 1$; otherwise, $\left|B_{i_1}^k \cap B_{i_2}^k \cap B_{i_3}^k\right| = 2^{k-2} - 1$. □

A generalisation of Theorem 4 is described in the following Theorem 5. □

Theorem 5: If $\left|B_{i_1}^k \cap \cdots \cap B_{i_\delta}^k\right| = 2^{k-\delta} - 1$, then $\left|B_{i_1}^k \cap \cdots \cap B_{i_\delta}^k \cap B_i^k\right| = 2^{k-\delta} - 1$ or $\left|B_{i_1}^k \cap \cdots \cap B_{i_\delta}^k \cap B_i^k\right| = 2^{k-\delta-1} - 1$ for $1 \le i \le 2^k-1$, $k > \delta$.

Proof: Because of $\left|B_{i_1}^k \cap \cdots \cap B_{i_\delta}^k\right| = 2^{k-\delta} - 1$, that is, the number of non-zero vector solutions given in (5) is $2^{k-\delta}-1$

$$\begin{cases} g_{i_1}^{\mathrm{T}} \cdot g_m \equiv 0(\mathrm{mod}\,2) \\ \quad\vdots \\ g_{i_\delta}^{\mathrm{T}} \cdot g_m \equiv 0(\mathrm{mod}\,2) \end{cases} \tag{5}$$

The rank of vector set $\boldsymbol{g}_{i_r}$ is δ, where $r = 1, \ldots, \delta$. If vector $\boldsymbol{g}_i$ can be linearly represented by the vector set $\boldsymbol{g}_{i_r}$, then the

number of non-zero vector solutions of the following equations is $2^{k-\delta}-1$

$$\begin{cases} \boldsymbol{g}_{i_1}^{\mathrm{T}} \cdot \boldsymbol{g}_x \equiv 0 (\mathrm{mod}\, 2) \\ \quad \vdots \\ \boldsymbol{g}_{i_\delta}^{\mathrm{T}} \cdot \boldsymbol{g}_x \equiv 0 (\mathrm{mod}\, 2) \\ \boldsymbol{g}_i^{\mathrm{T}} \cdot \boldsymbol{g}_x \equiv 0 (\mathrm{mod}\, 2) \end{cases} \tag{6}$$

Otherwise, the rank of vector set $\boldsymbol{g}_{i_r}$ and $\boldsymbol{g}_i$ is $\delta+1$ for $r=1, \ldots, \delta$. Thus, the number of non-zero vector solutions of (6) is equal to $2^{k-\delta-1}-1$. Thus,this completes the proof of the Theorem 5. □

The use of Theorem 5 for reconstructing linear systematic (n, k, d)-code C, where $n=2^{k-1}+\cdots+2^{k-\delta}$ and $d=2^{k-2}+\cdots+2^{k-\delta-1}$for $k\geq 2$, $1\leq\delta<k$ will be illustrated in Section 3.

3 Construction of several kinds of (*n, k, d*) linear codes

It is of some interest to construct binary linear codes with large minimum distance for a given code length n and the message length k. In the following, constructing a class of good binary linear codes (n, k, d) meeting the GB and $\delta\geq 1$ is given, where $n=2^{k-1}+\cdots+2^{k-\delta}$and $d=2^{k-2}+\cdots+2^{k-\delta-1}$ for $k\geq 4$, $1\leq\delta<k$.

For a given$\left|B_{i_1}^k\cap\cdots\cap B_{i_\delta}^k\right|=2^{k-\delta}-1$, where $1\leq i_1, \ldots, i_\delta\leq 2^k-1$, let $\boldsymbol{G}^*$ be the matrix whose columns are the binary k-tuples representation of elements in $\overline{B_{i_1}^k\cap\cdots\cap B_{i_\delta}^k}$. Then the code generated by $\boldsymbol{G}^*$ is the above code.

Analysis: the code length is $\left|\overline{B_{i_1}^k\cap\cdots\cap B_{i_\delta}^k}\right|=(2^k-1)-(2^{k-\delta}-1)=2^{k-1}+\cdots+2^{k-\delta}$.

For $i\neq i_1, \ldots, i_\delta$ and$1\leq i<2^k-1$, By Theorem 5, we have $\left|\overline{B_{i_1}^k\cap\cdots\cap B_{i_\delta}^k}\cap B_i^k\right|=\left|B_i^k\right|-\left|B_{i_1}^k\cap\cdots\cap B_{i_\delta}^k\cap B_i^k\right|=2^{k-2}+\cdots+2^{k-\delta}$ or $2^{k-2}+\cdots+2^{k-\delta-1}$. Otherwise, i equals to one of $i_1, \ldots, i_\delta$. Then $\left|\overline{B_{i_1}^k\cap\cdots\cap B_{i_\delta}^k}\cap B_i^k\right|=2^{k-2}+\cdots+2^{k-\delta}$. It follows from Theorem 2 that the minimum distance d is equal to $\left(2^{k-1}+\cdots+2^{k-\delta}\right)-\left(2^{k-2}+\cdots+2^{k-\delta}+2^{k-\delta-1}\right)=2^{k-2}+\cdots+2^{k-\delta-1}$.
According to Theorem 2, the weight distribution $\{w_0, w_1, \ldots, w_n\}$ is known by computing the number of codeword with the same weight.

The weight distributions are $w_0=1$, $w_{2^{k-2}+\cdots+2^{k-\delta-1}}=2^k-2^\delta$ and $w_{2^{k-1}}=2^\delta-1$; otherwise, $w_i=0$.

For instance, when $k=6$ and $\delta=2$, the corresponding code is $C(48, 6, 24)$. The weight distribution of C is $w_0=1$, $w_{24}=60$ and $w_{32}=3$. Otherwise, $w_i=0$. If we chose the base B_1^6 and B_{63}^6, then the generator matrix columns are the binary 6-tuples representation of elements in $\overline{B_1^6\cap B_{63}^6}=E^6-\{6, 10, 12, 18, 20, 24, 30, 34, 36, 40, 46, 48, 54, 58, 60\}$.
In general, in order to construct the systematic generator matrix, the base $B_{(2^k-1)}^k$ must be chosen.

4 Constructing new class binary linear codes

Constructing new binary linear codes with parameters $n=2^{k-1}+\cdots+2^{k-\delta}-3u$ and $d=2^{k-2}+\cdots+2^{k-\delta-1}-2u$ for $2\leq u\leq 4$, $1\leq\delta<k$ and $k\geq 6$ are given in this section.

In Section 3, a class of optimal binary linear codes (n, k, d) meeting the GB be constructed. Then, we present a shortening method based on the above codes.New binary linear codes can be obtained by shortening. An example is given below.

With $\delta=2$, the kind of codes $C(2^{k-1}+2^{k-2}, k, 2^{k-2}+2^{k-3})$ is construted. Moreover, some interesting properties are found for small parameter k. For instance, parameter $k=6$, the base B_1^6 and $B_{63}^6$are chosen such that some subsets of $\overline{B_1^6\cap B_{63}^6}$ denoted as $S_1, \ldots, S_v$,satisfy the following conditions.

(1) $|S_i|=3$, $i=1,\ldots,v$.
(2) $|S_i\cap S_j|=0$, $i\neq j$.
(3) $\min_{j\in E^6}|S_i\cap B_j^6|=1$ for every $i=1,\ldots,v$.

By using the computer search method, we can found S_i for $1\leq i\leq v$ satisfying the above conditions.

$S_1=\{3, 13, 14\}$, $S_2=\{5, 19, 22\}$, $S_3=\{7, 26, 29\}$, $S_4=\{9, 21, 28\}$, $S_5=\{11, 33, 42\}$, $S_6=\{15, 35, 44\}$, $S_7=\{17, 37, 52\}$ and $S_8=\{31, 45, 50\}$. Here $v=8$. Note that v may be greater than 8.

Let $B_u=\overline{B_1^6\cap B_{63}^6}-\bigcup_{j=1}^{u}S_j$ for $u=1,\ldots, v$. According to Theorem 2, its columns in the systematic generator matrix is the binary 6-tuples representation of elements in set B for constructing $(n, 6, d)$ code with parameters $n=48-3u$ and $d=24-2u$. However, with the increasing of u, the minimum distance of the code may not be optimal. For a good code, u must be no more than$2^{k-\delta-1}$. In this particular example, for $k=6$ and $\delta=2$,the codes still remain good when $u=1$, 2, 3, 4. Some details of those codes weight distributions are given as below.

The weight distribution of the (45, 6, 22) code is $w_0=1$, $w_{22}=45$, $w_{24}=15$ and $w_{30}=3$. Otherwise, $w_i=0$.

The weight distribution of the (42, 6, 20) code is $w_0=1$, $w_{20}=33$, $w_{22}=24$, $w_{24}=3$ and $w_{28}=3$. Otherwise, $w_i=0$.

The weight distribution of the (39, 6, 18) code is $w_0=1$, $w_{18}=23$, $w_{20}=30$, $w_{22}=6$, $w_{24}=1$ and $w_{26}=3$. Otherwise, $w_i=0$.

The weight distribution of the (36, 6, 16) code is $w_0=1$, $w_{16}=15$, $w_{18}=32$, $w_{20}=12$ and $w_{24}=4$. Otherwise, $w_i=0$.

The weight distribution of codes may be different with the change of S_i.

For $k\geq 6$, according to Corollary 1, the above sets are still subsets of $\overline{B_{i_1}^k\cap\cdots\cap B_{i_\delta}^k}$ and $\left|B_{i_1}^k\cap\cdots\cap B_{i_\delta}^k\right|=2^{k-\delta}-1$, where $i_1=1$and $i_\delta=2^k-1$. Meanwhile , the sets also satisfy condition (1), (2) and the following condition.

(4) $\min_{j\in E^k}|S_i\cap B_j^k|=1$for every $i=1,\ldots,$v.

Let $B_u=\overline{B_{i_1}^k\cap\cdots\cap B_{i_\delta}^k}-\bigcup_{j=1}^{u}S_j$ for $1\leq u\leq 4$. For constructing the (n, k, d) code with parameters $n=2^{k-1}+\cdots+2^{k-\delta}-3u$ and $d=2^{k-2}+\cdots+2^{k-\delta-1}-2u$, by Theorem 2, the systematic generator matrix columns are the binary k-tuples representation of elements in set B. For $u=1$, the weight distributions are $w_0=1$, $w_{2^{k-2}+\cdots+2^{k-\delta-1}-2}=2^{k-1}+2^{k-2}-2^\delta+1$, $w_{2^{k-2}+\cdots+2^{k-\delta-1}}=2^{k-2}-1$ and $w_{2^{k-1}}=2^\delta-1$; otherwise, $w_i=0$.

For $u=2$, the weight distributions are $w_0=1$, $w_{2^{k-2}+\cdots+2^{k-\delta-1}-4}=2^{k-1}+2^{k-4}-2^\delta+1$, $w_{2^{k-2}+\cdots+2^{k-\delta-1}-2}=2^{k-2}+2^{k-3}$, $w_{2^{k-2}+\cdots+2^{k-\delta-1}}=2^{k-4}-1$ and $w_{2^{k-1}}=2^\delta-1$; otherwise, $w_i=0$.

For $u=3$, the weight distributions are $w_0=1$, $w_{2^{k-2}+\cdots+2^{k-\delta-1}-6}=2^{k-2}+2^{k-3}+2^{k-5}-2^\delta+1$, $w_{2^{k-2}+\cdots+2^{k-\delta-1}-2}=2^{k-4}+2^{k-5}$, $w_{2^{k-2}+\cdots+2^{k-\delta-1}-4}=2^{k-1}-2^{k-5}$, $w_{2^{k-2}+\cdots+2^{k-\delta-1}}=2^{k-5}-1$ and $w_{2^{k-1}-6}=2^\delta-1$; otherwise, $w_i=0$.

doi: 10.1049/iet-com.2013.0671

For $u=4$, the weight distributions are $w_0=1$, $w_{2^{k-2}+\cdots+2^{k-\delta-1}-8}=2^{k-2}+2^{k-5}-2^{\delta}+1$, $w_{2^{k-2}+\cdots+2^{k-\delta-1}-6}=2^{k-1}$, $w_{2^{k-2}+\cdots+2^{k-\delta-1}-4}=2^{k-3}+2^{k-4}$, $w_{2^{k-2}+\cdots+2^{k-\delta-1}}=2^{k-5}-1$ and $w_{2^{k-1}-8}=2^{\delta}-1$; otherwise, $w_i=0$.

For example $\delta=2$ and $k\geq 6$, the weight distributions mentioned above are given as below.

The weight distribution of the $(2^{k-1}+2^{k-2}-3,\ k,\ 2^{k-2}+2^{k-3}-2)$ code is $w_0=1$,

$w_{2^{k-2}+2^{k-3}-2}=2^{k-1}+2^{k-2}-3$, $w_{2^{k-2}+2^{k-3}}=2^{k-2}-1$ and $w_{2^{k-1}-2}=3$. Otherwise, $w_i=0$. This result can also be found in [10].

The weight distribution of the $(2^{k-1}+2^{k-2}-6,\ k,\ 2^{k-2}+2^{k-3}-4)$ code is $w_0=1$,

$$w_{2^{k-2}+2^{k-3}-4}=2^{k-1}+2^{k-4}-3,$$
$$w_{2^{k-2}+2^{k-3}-2}=2^{k-2}+2^{k-3},\quad w_{2^{k-2}+2^{k-3}}=2^{k-4}-1$$

and $w_{2^{k-1}-4}=3$. Otherwise, $w_i=0$.

The weight distribution of the $(2^{k-1}+2^{k-2}-9,\ k,\ 2^{k-2}+2^{k-3}-6)$ code is $w_0=1$,

$$w_{2^{k-2}+2^{k-3}-6}=2^{k-2}+2^{k-3}+2^{k-5}-3,$$
$$w_{2^{k-2}+2^{k-3}-4}=2^{k-1}-2^{k-5},\quad w_{2^{k-2}+2^{k-3}-2}=2^{k-4}+2^{k-5},$$
$$w_{2^{k-2}+2^{k-3}}=2^{k-5}-1$$

and $w_{2^{k-1}-6}=3$. Otherwise, $w_i=0$.

The weight distribution of the $(2^{k-1}+2^{k-2}-12,\ k,\ 2^{k-2}+2^{k-3}-8)$ code is $w_0=1$, $w_{2^{k-2}+2^{k-3}-8}=2^{k-2}+2^{k-5}-3$, $w_{2^{k-2}+2^{k-3}-6}=2^{k-1}$, $w_{2^{k-2}+2^{k-3}-4}=2^{k-3}+2^{k-4}$, $w_{2^{k-2}+2^{k-3}}=2^{k-5}-1$ and $w_{2^{k-1}-8}=3$. Otherwise, $w_i=0$. For $k=7$ or 8, eight optimal codes (93, 7, 46), (90, 7, 44), (87, 7, 42), (84, 7, 40), (189, 8, 94), (186, 8, 92), (183, 8, 90) and (181, 8, 88) are thus constructed. The above codes could be applied to the DVB-S2 system [23].

5 Dual codes of $C(n, k, d)$

It is well known that if C is a (n, k)-code, then the dual code of C is $(n, n\text{-}k)$. If the (n, k)-code's generator matrix has the form $(I_{k\times k}|\boldsymbol{G}_{k\times(n-k)})$, where $I_{k\times k}$ is identity matrix, then the generator matrix of the dual code C is $\left(G^{\mathrm{T}}_{(n-k)\times k}|I_{(n-k)\times(n-k)}\right)$, where $G^{\mathrm{T}}_{(n-k)\times k}$ denotes the transpose of $\boldsymbol{G}_{k\times(n-k)}$.

In order to construct the dual code of $C\left(2^{k-1}+\cdots+2^{k-\delta},\ k,\ 2^{k-2}+\cdots+2^{k-\delta-1}\right)$, the systematic generator matrix must be constructed. When $\delta=1$, the code is $C(2^{k-1},\ k,\ 2^{k-2})$. Thus, the base $B^k_{(2^k-1)}$ is chosen such that $\overline{B^k_{(2^k-1)}}$ can be computed. Interchanging the columns of the generator matrix whose columns are the binary k-tuples representation of elements in $\overline{B^k_{(2^k-1)}}$ yields a systematic matrix. As a consequence, the dual codes of $C(2^{k-1},\ k,\ 2^{k-2})$, that is, codes $C^{\perp}$ are constructed. According to MacWilliam's identities, the minimum distance of $C^{\perp}$ is four. For example, for a given $k=5$, the generator matrix of the (16, 11, 4)-code is given as follows: (see equation at the bottom of the page)

The weight distribution of $C^{\perp}_{11\times 16}$ is $w_0=1$, $w_4=140$, $w_6=448$, $w_8=870$, $w_{10}=448$, $w_{12}=140$ and $w_{16}=1$; otherwise, $w_i=0$.

When $\delta=2$, the code is $C(2^{k-1}+2^{k-2},\ k,\ 2^{k-2}+2^{k-3})$. The base B^k_1 and $B^k_{(2^k-1)}$ are chosen such that the systematic generator matrix can be constructed. Thus, its dual codes can be constructed. The generator matrix of the (24, 19, 3)-code is given as follows: (see equation at the bottom of the next page)

Here, the weight distribution of $C^{\perp}_{19\times 24}$ is $w_0=1$, $w_3=67$, $w_4=371$, $w_5=1324$, $w_6=4088$, $w_7=10805$, $w_8=23242$, $w_9=40896$, $w_{10}=60880$, $w_{11}=77966$, $w_{12}=84966$, $w_{13}=78008$, $w_{14}=60928$, $w_{15}=40890$, $w_{16}=23173$, $w_{17}=10784$, $w_{18}=4144$, $w_{19}=1343$, $w_{20}=343$, $w_{21}=60$, $w_{22}=8$ and $w_{23}=1$; otherwise, $w_i=0$.

According to MacWilliam's identities, the minimum distances of the dual codes of the (n, k, d) code with two pair parameters $n=2^{k-1}+\cdots+2^{k-\delta}$ and $d=2^{k-2}+\cdots+2^{k-\delta-1}$ for $k\geq 4$, $2\leq\delta<k$ or $n=2^{k-1}+\cdots+2^{k-\delta}-3u$ and $d=2^{k-2}+\cdots+2^{k-\delta-1}-2u$ for $2\leq u<2^{k-\delta-2}$, $1\leq\delta<k$ and $k\geq 6$, both are three. Therefore the codes are optimal.

6 Conclusion

Matroids may be used extensively in error corrected codes. In this paper, a new relationship between MT and coding theory is derived, that is, minimum distance d can be computed based on MT. Based on the relationship, several kinds of linear codes are constructed. A new shortening code method is presented, meanwhile by shortening the constructed codes, new class binary linear codes are obtained. The codes constructed in this paper can be used to DVB-S2 system. Obviously, how to design good binary linear codes is of interest in coding theory. It is expected that an extension of the idea proposed in this paper can be used to construct more good codes.

$$G^{\perp}_{11\times 16}=\begin{pmatrix}
1&1&1&0&0&1&0&0&0&0&0&0&0&0&0&0\\
1&1&0&1&0&0&1&0&0&0&0&0&0&0&0&0\\
1&0&1&1&0&0&0&1&0&0&0&0&0&0&0&0\\
0&1&1&1&0&0&0&0&1&0&0&0&0&0&0&0\\
1&1&0&0&1&0&0&0&0&1&0&0&0&0&0&0\\
1&0&1&0&1&0&0&0&0&0&1&0&0&0&0&0\\
0&1&1&0&1&0&0&0&0&0&0&1&0&0&0&0\\
1&0&0&1&1&0&0&0&0&0&0&0&1&0&0&0\\
0&1&0&1&1&0&0&0&0&0&0&0&0&1&0&0\\
0&0&1&1&1&0&0&0&0&0&0&0&0&0&1&0\\
1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&1
\end{pmatrix}$$

7 Acknowledgments

The authors wish to thank Prof. Tor Helleseth for advising and proof reading the article. Authors are also grateful to the editor and the anonymous reviewers, who provided valuable comments and suggestion which significantly helped to improve the quality of this paper.This work was supported by the National Science foundation of China, under grant no. 60972053. Meanwhile,this work was supported by Startup foundation for Doctor of Jiangxi university of Science and Technology, under grant no. 3401222021.

8 References

1 Shannon, C.: 'A mathematical theory of communication', *Bell Syst. Tech.* 1948, **27**, pp. 379–423 and 623–656
2 Griesmer, J.H.: 'A bound for error-correcting codes', *IBM J. Res. Develop.*, 1960, **4**, pp. 532–542
3 Grassl, M.: 'Tables of linear codes and quantum codes', [Online]. Available at http://www.codetables.de (accessed January 2013)
4 Solomon, G., Stiffler, J.J.: 'Algebraically punctured cyclic codes', *Inf. Contr.*, 1965, **8**, pp. 170–179
5 Belov, B.I.: 'A conjecture on the Griesmer bound'. Optimization Methods and Their Applications, (Russian), Sibirsk. Energet. Inst. Sibirsk. Otdel. Akad. Nauk SSSR, Irkutsk, 1974, 182, pp. 100–106
6 Helleseth, T., van Tilborg, H.C.A.: 'The classification of all (145, 7, 72) binary linear codes', Eindhoven University Technical, T. H. Report April 1980 80-WSK-01
7 Helleseth, T., van Tilborg, H.C.A: 'A new class of codes meeting the Griesmer bound', *IEEE Trans. Inf. Theory, Sept.*, 1981, **27**, pp. 548–555
8 Helleseth, T.: 'New constructions of codes meeting the Griesmer bound', *IEEE Trans. Inf. Theory*, 1983, **29**, pp. 434–439
9 van Tilborg, H.C.A.: 'on the uniqueness resp. nonexistence of certain codes meeting the Griesmer bound', *Inf. Contr.*, 1980, **44**, pp. 16–35
10 Helleseth, T.: 'Projective codes meeting the Griesmer bound', *Discrete Math.*, 1992, **106**, (107), pp. 265–271
11 Hamada, N.: 'A characterization of some [n, k, d; q]-codes meeting the Griesmer bound using a minihyper in a finite projective geometry', *Discrete Math.*, 1993, **116**, pp. 229–268
12 wu, G., Chang, H.-C., Wang, L., Truong, T.K.: 'Constructing rate 1/p systematic binary quasi-cyclic codes based on the matroid theory', *Des. Codes Cryptogr*, 2012, DOI: 10.1007/s10623-012-9715-1
13 Whitney, H.: 'On the abstract properties of linear dependence', *Am. J. Math.*, 1935, **57**, pp. 509–533
14 Tutte, W.T.: 'Matroids and graphs', *Trans. Am. Math. Soc*, 1959, **90**, pp. 527–552
15 Edmonds, J., Fulkerson, D.R.: 'Transversals and matroid partition', *J. Res. Nat. Bur. Stand.*, 1965, **69 B**, pp. 147–153
16 Greene, C.: 'Weight enumeration and the geometry of linear codes', *Studia Appl. Math.*, 1976, **55**, pp. 119–128
17 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)
18 Ahlswede, R., Cai, N., Li, S.-Y.R., Yeung, R.W.: 'Network information flow', *IEEE Trans. Inf. Theory*, 2000, **46**, (4), pp. 1204–1216
19 Dougherty, R., Freiling, C., Zeger, K.: 'Networks, matroids, and non-Shannon information inequalities', *IEEE Trans. Inf. Theory*, 2007, **53**, (6), pp. 1949–1969
20 Barg, A.: 'The matroid of supports of a linear code', *Appl. Algebra Eng. Commun.Comput.*, 1997, **8**, (2), pp. 165–172
21 Feldman, J., Wainwright, M.J., Karger, D.R.: 'Using linear programming to decode binary linear codes', *IEEE Trans. Inf. Theory*, 2005, **51**, (3), pp. 954–972
22 Oxley, J.G.: 'Matroid theory' (Oxford Univ. Press, Oxford, Uk, 1992)
23 Morello, A., Mignone, V.: 'DVB-S2: the second generation standard for satellite broad-band services', *Proc. IEEE*, 2006, **94**, (1), pp. 210–227

$$G^{\perp}_{19\times 24} = \begin{pmatrix}
1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
1&1&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
1&0&1&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&1&1&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
1&1&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
1&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&1&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
1&1&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
1&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1
\end{pmatrix}$$