European Journal of Combinatorics 33 (2012) 1265–1272

Contents lists available at SciVerse ScienceDirect

European Journal of Combinatorics

journal homepage: www.elsevier.com/locate/ejc

On a kind of two-weight code[☆]

Zihui Liu[a], Xiangyong Zeng[b]

[a] *Department of Mathematics, Beijing Institute of Technology, Beijing 100081, China*

[b] *Faculty of Mathematics and Computer Science, Hubei University, Wuhan 430062, China*

ARTICLE INFO

Article history:
Received 13 July 2011
Received in revised form
11 February 2012
Accepted 16 February 2012
Available online 28 March 2012

ABSTRACT

A special type of two-weight code is defined by using subcodes. The generalized Hamming weight and the chain property of this kind of two-weight code are determined. The higher-weight enumerators and an application of this kind of two-weight code are given.

1. Introduction

Two-weight codes, i.e., nonzero codewords that have only two different weights, are interesting in the area of coding theory (e.g., uniformly packed codes) and have been studied intensively [5].

Two-weight codes are also closely related to objects in different areas of mathematics such as strongly regular graphs, partial geometries, and projective point-sets. Delsarte [6] was the first to study the connections between two-weight codes, strongly regular graphs, and projective point-sets. A survey of this relationship was given later by Calderbank and Kantor [3]. Two-weight codes can also be used to construct secret sharing schemes, which is an interesting subject of cryptography; see [13].

In this paper, motivated by the research work in [8], a special kind of two-weight code is defined. Some properties and an application of this kind of two-weight code are given.

1.1. Notations and definitions

For any subcode D of a code C, the support $\chi(D)$ of D is defined as the set of positions where not all the codewords of D have zero coordinates. In particular, the support of any nonzero codeword consists of its nonzero coordinate positions.

Definition 1. For any subcode D of C, $w(D) := |\chi(D)|$ is called the *support weight* or *effective length* of D. In particular, $w(C)$ is called the effective length of C.

Let C be a linear $[n, k]$ code, that is, a k-dimensional code over the finite field $GF(q)$ with effective length n, and let C_1 be a k_1-dimensional subcode of C. Define $C \setminus C_1 = \{c \mid c \in C \text{ and } c \notin C_1\}$.

[☆] Z.H. Liu was supported by the National Natural Science Foundation of China (No. 11171366). X.Y. Zeng was supported by the National Natural Science Foundation of China (No. 61170257).

E-mail addresses: lzhui@bit.edu.cn (Z. Liu), xzeng@hubu.edu.cn (X. Zeng).

0195-6698/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ejc.2012.02.007

Definition 2. If both C_1 and $C \setminus C_1$ are constant-weight codes, then C is called a *relative two-weight* (RTW) code with respect to C_1.

Let C be an $[n, k]$ RTW code with respect to C_1, and assume that the weight of the nonzero codewords in C_1 is d, and that the weight of codewords in $C \setminus C_1$ is d^*; then we briefly use $(C, C_1)(n, d, d^*)$ or $C(n, d, d^*)$ (when C_1 is clear) to denote the RTW code C.

Definition 3 (*[12]*)**.** The *generalized Hamming weight* of an $[n, k]$ code C is a sequence $(d_1, d_2, \ldots, d_k)$, where

$$d_r = \min\{w(D) \mid D \text{ is an } r\text{-dimensional subcode of } C\}, \quad 1 \le r \le k.$$

Note that d_1 is exactly the traditional minimum Hamming weight of C, and that $d_k = n$ is exactly the effective length of C. C is said to satisfy the *chain condition* if there exist subcodes $D_i (1 \le i \le k)$ such that $\{0\} \subset D_1 \subset D_2 \subset \cdots \subset D_k = C$, $\dim(D_i) = i$, and $w(D_i) = d_i$, for each i with $1 \le i \le k$.

The value function (also called value assignment) and finite projective geometry methods are effective tools to study the support weights of subcodes [4,11]. In particular, the value function was first introduced in [4] to study the generalized Hamming weight of a linear code.

Definition 4. A *value function* is a correspondence $m(\cdot)$: $PG(k-1, q) \to Z$, where Z represents the integers and $PG(k-1, q)$ represents a $(k-1)$-dimensional projective space over the finite field $GF(q)$. For any point $p \in PG(k-1, q)$, call $m(p)$ the *value* of p.

Define the *value* of $S \subset PG(k-1, q)$ by $m(S) = \sum_{p \in S} m(p)$.

1.2. The value function and linear codes

To use the value function to study the generalized Hamming weight, we consider the columns of $\boldsymbol{G}$, a generator matrix of a k-dimensional q-ary linear code C, as projective points in $PG(k-1, q)$. For a point $p \in PG(k-1, q)$, let $m(p)$ mean the number of the times the point p occurs in the columns of $\boldsymbol{G}$. We thus obtain a value function $m(\cdot)$: $PG(k-1, q) \to Z$ such that $m(\cdot) \ge 0$. Obviously, such a value function defines a generator matrix and a code (up to equivalence).

Additionally, for each subset $L \subset \{1, 2, \ldots, k\}$ and $p = (u_1, \ldots, u_k) \in PG(k-1, q)$, let $P_L(p) = (v_1, \ldots, v_k)$, where $v_i = u_i$ if $i \in L$, and $v_i = 0$ if $i \notin L$. Define $P_L(S) = \{P_L(p) \mid p \in S\}$ for a subset $S \subset PG(k-1, q)$. Obviously, if S is a projective subspace, so is $P_L(S)$.

Lemma 1 (*[8]*)**.** *If C is an $[n, k]$ code and C_1 is a k_1-dimensional subcode, then there is a* 1–1 *correspondence between the r-dimensional subcodes D satisfying* $\dim(D \cap C_1) = \theta$ *and the $(k-r-1)$-dimensional projective subspaces P satisfying* $\dim P_L(P) = k_1 - \theta - 1$*, such that, if D corresponds to P, we will have $n - w(D) = m(P)$, where $L = \{1, 2, \ldots, k_1\}$. In particular, when $C_1 = \{0\}$, i.e., $k_1 = 0$, the conclusion is that there is a* 1–1 *correspondence between the r-dimensional subcodes D and the $(k-r-1)$-dimensional projective subspaces P such that, if D corresponds to P, we will have*

$$n - w(D) = m(P). \tag{1}$$

In the following text, let P_ξ^η denote a ξ-dimensional projective subspace P satisfying $\dim P_L(P) = \eta$*, and let L always denote the set $\{1, 2, \ldots, k_1\}$. For example, P_0^{-1} stands for a point whose first k_1 coordinate positions are all 0, and all such points constitute a projective subspace $P_{k-k_1-1}^{-1}$.*

2. The generalized Hamming weight of an RTW code

Lemma 2. *Assume that C is an RTW code with respect to a k_1-dimensional subcode C_1, and that $m(\cdot)$ is a value function of C; then $m(\cdot)$ has only two different values. Furthermore, the points p satisfying $P_L(p) = 0$ share one of the values with each other, whereas the points p satisfying $P_L(p) \neq 0$ share the other, where $L = \{1, 2, \ldots, k_1\}$.*

Proof. Since each nonzero codeword of C_1 spans a one-dimensional subcode D such that $\dim(D \cap C_1) = \dim(D) = 1$ and C is an RTW code, we get by Definition 2 that all the one-dimensional subcodes D satisfying $\dim(D \cap C_1) = 1$ have the same support weight, and that all the codewords in $C \setminus C_1$

have the same weight. So the assumptions in [8, Theorem 3] are satisfied, and then, using the proof of [8, Theorem 3 (Case 2)], we get the result. □

The importance of Lemma 2 is in that it gives a convenient way to construct an RTW code. See the following.

Example 1. Consider the four-dimensional binary linear code C generated by the matrix

$$\begin{pmatrix} 1&1&1&1&1&1&1&1&0&0&0&0\\ 0&0&0&0&1&1&1&1&1&1&1&1\\ 0&0&1&1&0&0&1&1&0&0&1&1\\ 0&1&0&1&0&1&0&1&0&1&0&1 \end{pmatrix},$$

and let C_1 be the two-dimensional subcode generated by the first two rows of the matrix. Then, $m(p) = 0$ for the point p satisfying $P_L(p) = 0$, whereas $m(p) = 1$ for the point p satisfying $P_L(p) \neq 0$, where $L = \{1, 2\}$. So, C is an RTW code according to Lemma 2. More concretely, since $d = 8$ and $d^* = 6$, C is a $(12, 8, 6)$ RTW code.

According to Lemma 2, we may get different RTW codes by simply changing the values $m(\cdot)$ takes on the points p such that $P_L(p) = 0$ and $P_L(p) \neq 0$. For instance, we may modify $m(\cdot)$ above as follows:

$$m(p) = \begin{cases} 1, & P_L(p) \neq 0, \\ 2, & P_L(p) = 0. \end{cases}$$

To satisfy the value function, we give a generator matrix of another RTW code:

$$\begin{pmatrix} 1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&0&0&0\\ 0&0&1&1&0&0&1&1&0&0&1&1&1&1&0&0&1&1\\ 0&1&0&1&0&1&0&1&0&1&0&1&0&0&1&1&1&1 \end{pmatrix}.$$

It can be checked that the code generated by the above matrix is a $(18, 8, 10)$ RTW code. If we modify $m(\cdot)$ as follows,

$$m(p) = \begin{cases} 2, & P_L(p) \neq 0, \\ 1, & P_L(p) = 0, \end{cases}$$

then we may obtain a $(27, 16, 14)$ RTW code generated by

$$\begin{pmatrix} 111111111111111100000000000\\ 000000001111111111111111000\\ 000011110000111100001111101\\ 001100110011001100110011011 \end{pmatrix}.$$

The generalized Hamming weight of an RTW code can be determined by using Lemmas 1 and 2. We first give the following.

Lemma 3. *For the RTW code $C(n, d, d^*)$, we have*

$$n = \frac{q^{k_1}(q^{k-k_1} - 1)d^* + (q^{k_1} - 1)d}{(q - 1)q^{k-1}}.$$

Remark 1. It can be easily deduced from the result of Lemma 3 that the length of C in Example 1 should be equal to 12, that the length of the second RTW code in Example 1 should be equal to 18, and that the length of the third RTW code in Example 1 should be equal to 27.

Proof of Lemma 3. From Definition 2 for an RTW code, we get that both C_1 and $C \setminus C_1$ are constant-weight codes. Since each nonzero codeword of C_1 spans a one-dimensional subcode D such that $\dim(D \cap C_1) = 1$ and each codeword in $C \setminus C_1$ spans a one-dimensional subcode D such that $\dim(D \cap C_1) = 0$, we get by using (1) in Lemma 1 that the value of each $P_{k-2}^{k_1-2}$ is equal to $n - d$ and that the value of each $P^{k_1-1}_{k-2}$ is equal to $n - d^*$. So $m(\cdot)$ should satisfy the following system of equations:

$$\begin{cases} m(P^{k_1-2}_{k-2}) = n - d \\ m(P^{k_1-1}_{k-2}) = n - d^* \\ m(PG(k-1,q)) = n. \end{cases} \tag{2}$$

Define $S_1 \subset PG(k-1,q)$ and $S_2 \subset PG(k-1,q)$ as

$$S_1 = \{p \mid P_L(p) = 0\},$$
$$S_2 = \{p \mid P_L(p) \neq 0\}.$$

Obviously, $PG(k-1,q) = S_1 \cup S_2$, $|S_1| = \frac{q^{k-k_1}-1}{q-1}$, and $|S_2| = \frac{q^k-1}{q-1} - \frac{q^{k-k_1}-1}{q-1} = \frac{q^{k-k_1}(q^{k_1}-1)}{q-1}$. One can also check that each $P^{k_1-2}_{k-2}$ contains $\frac{q^{k-k_1}-1}{q-1}$ points of S_1 and $\frac{q^{k-1}-1}{q-1} - \frac{q^{k-k_1}-1}{q-1} = \frac{q^{k-k_1}(q^{k_1-1}-1)}{q-1}$ points of S_2, and that each $P^{k_1-1}_{k-2}$ contains $\frac{q^{k-k_1-1}-1}{q-1}$ points of S_1 and $\frac{q^{k-1}-1}{q-1} - \frac{q^{k-k_1-1}-1}{q-1} = \frac{q^{k-k_1-1}(q^{k_1}-1)}{q-1}$ points of S_2. Note that by Lemma 2 all the points of S_1 have the same value and that all the points of S_2 have the same value. Consequently, (2) can be rewritten as

$$\begin{cases} \left(\dfrac{q^{k-k_1}-1}{q-1}\right) m(p_1) + \dfrac{q^{k-k_1}(q^{k_1-1}-1)}{q-1} m(p_2) = n - d \\ \left(\dfrac{q^{k-k_1-1}-1}{q-1}\right) m(p_1) + \dfrac{q^{k-k_1-1}(q^{k_1}-1)}{q-1} m(p_2) = n - d^* \\ \left(\dfrac{q^{k-k_1}-1}{q-1}\right) m(p_1) + \dfrac{q^{k-k_1}(q^{k_1}-1)}{q-1} m(p_2) = n, \end{cases} \tag{3}$$

where $p_1 \in S_1$ and $p_2 \in S_2$.

It is not difficult to check that (3) has a unique solution:

$$\begin{cases} m(p_1) = \dfrac{q^{k_1}d^* - (q^{k_1}-1)d}{q^{k-1}} \\ m(p_2) = \dfrac{d}{q^{k-1}} \\ n = \dfrac{q^{k_1}(q^{k-k_1}-1)d^* + (q^{k_1}-1)d}{(q-1)q^{k-1}}, \end{cases} \tag{4}$$

from which we get the result. □

Theorem 1. *Any RTW code $C(n,d,d^*)$ satisfies the chain condition. As regards the generalized Hamming weight, the result is as follows:*

$$\text{(I) } d > d^* \quad d_r = \begin{cases} \dfrac{q^{k-r}(q^r-1)}{(q-1)q^{k-1}} d^*, & 1 \le r \le k - k_1 - 1 \\ \dfrac{q^{k_1}(q^{k-k_1}-1)d^* + (q^{k_1}-q^{k-r})d}{(q-1)q^{k-1}}, & k - k_1 \le r \le k-1. \end{cases}$$

$$\text{(II) } d < d^* \quad d_r = \begin{cases} \dfrac{q^k - q^{k-r}}{(q-1)q^{k-1}} d, & 1 \le r \le k_1 - 1 \\ \dfrac{q^{k_1}(q^{k-k_1}-q^{k-r})d^* + q^{k-r}(q^{k_1}-1)d}{(q-1)q^{k-1}}, & k_1 \le r \le k-1. \end{cases}$$

Proof. Let S_1 and S_2 be defined as in Lemma 3. Assume that $d > d^*$; then $m(p_1) < m(p_2)$ by (4), where $p_1 \in S_1$ and $p_2 \in S_2$. By Lemma 1 (see (1)), determining d_r $(1 \leq r \leq k)$ is equivalent to determining the maximum value of the projective subspaces with dimension $k - r - 1$. So, to prove that $C(n, d, d^*)$ satisfies the chain condition, it is necessary to find a series of projective subspaces P_i $(0 \leq i \leq k - 1)$ such that $\dim(P_i) = i$, P_i has the maximum value among the i-dimensional subspaces, and $P_0 \subset P_1 \subset \cdots \subset P_{k-1}$. Since $m(p_1) < m(p_2)$, we obtain by Lemma 2 that the subspaces P_ξ^ξ $(0 \leq \xi \leq k_1 - 1)$ and the subspaces $P_\xi^{k_1-1}$ $(k_1 \leq \xi \leq k - 1)$ are exactly the maximum value subspaces. In addition, we also obtain by Lemma 2 that all the subspaces P_ξ^ξ have the same value for each fixed ξ, and so do the subspaces $P_\xi^{k_1-1}$. Thus, one can manage to choose such subspaces satisfying

$$P_0^0 \subset P_1^1 \subset \cdots \subset P_{k_1-1}^{k_1-1} \subset P_{k_1}^{k_1-1} \subset \cdots \subset P_{k-1}^{k_1-1} = PG(k-1, q).$$

So $C(n, d, d^*)$ satisfies the chain condition. To determine the generalized Hamming weight, it is necessary to compute the values of the subspaces in the above chain. Applying Lemmas 1–3, we have, for $k - k_1 \leq r \leq k - 1$,

$$\begin{aligned} d_r &= n - m(P_{k-r-1}^{k-r-1}) \\ &= n - \frac{q^{k-r} - 1}{q - 1} m(p_2), \quad (\text{where } p_2 \in S_2) \\ &= \frac{q^{k_1}(q^{k-k_1} - 1)d^* + (q^{k_1} - 1)d}{(q-1)q^{k-1}} - \frac{q^{k-r} - 1}{q - 1}\frac{d}{q^{k-1}}, \quad (\text{by (4)}) \\ &= \frac{q^{k_1}(q^{k-k_1} - 1)d^* + (q^{k_1} - q^{k-r})d}{(q-1)q^{k-1}}. \end{aligned}$$

For $1 \leq r \leq k - k_1 - 1$, we have

$$\begin{aligned} d_r &= n - m(P_{k-r-1}^{k_1-1}) \\ &= n - \frac{q^{k-k_1-r} - 1}{q - 1} m(p_1) - \left(\frac{q^{k-r} - 1}{q - 1} - \frac{q^{k-k_1-r} - 1}{q - 1}\right) m(p_2) \quad (p_1 \in S_1, p_2 \in S_2) \\ &= \frac{q^{k-r}(q^r - 1)}{(q-1)q^{k-1}} d^* \quad (\text{by (4)}). \end{aligned}$$

An almost similar computation gives the result for the case $d < d^*$, and the only difference is the subspaces chain. Since $d < d^*$ means that $m(p_1) > m(p_2)$ by (4), the maximum value subspaces chain can be chosen as

$$P_0^{-1} \subset P_1^{-1} \subset \cdots \subset P_{k-k_1-1}^{-1} \subset P_{k-k_1}^0 \subset P_{k-k_1+1}^1 \subset \cdots \subset P_{k-1}^{k_1-1} = PG(k-1, q).$$

So, the generalized Hamming weight is computed according to whether $1 \leq r \leq k_1 - 1$ or $k_1 \leq r \leq k - 1$. For $1 \leq r \leq k_1 - 1$,

$$\begin{aligned} d_r &= n - m(P_{k-r-1}^{k_1-r-1}) \\ &= \frac{q^k - q^{k-r}}{(q-1)q^{k-1}} d, \end{aligned}$$

and for $k_1 \leq r \leq k - 1$,

$$\begin{aligned} d_r &= n - m(P_{k-r-1}^{-1}) \\ &= \frac{q^{k_1}(q^{k-k_1} - q^{k-r})d^* + q^{k-r}(q^{k_1} - 1)d}{(q-1)q^{k-1}}. \quad \square \end{aligned}$$

3. The higher-weight enumerators

The higher-weight enumerators (also called support weight enumerators) were first introduced in [7], where a proof was presented to MacWilliams-type identities relating the support weight distributions of a linear code and its dual. For a linear code, the higher-weight enumerators are defined as the set of integers indicating the number of subcodes of the same dimension and the same effective length. Many researchers have investigated the higher-weight enumerators for various classes of linear code [2]. For the RTW code defined in the present paper, the higher-weight enumerators can be completely determined. Let C and C_1 be given as before. Since the subspaces P_{k-r-1}^{t-1} have the same value for an RTW code by Lemma 2, all the r-dimensional subcodes D satisfying $\dim(D \cap C_1) = t$ have the same support weight by Lemma 1; furthermore,

$$\begin{aligned} w(D) &= n - m(P_{k-r-1}^{t-1}) \\ &= \frac{(q^k - q^{k+k_1-r-t})d^* + (q^{k+k_1-r-t} - q^{k-r})d}{(q-1)q^{k-1}} \quad \text{(by (4))}. \end{aligned}$$

So, to determine the higher-weight enumerators, it is necessary to determine the number of r-dimensional subcodes D satisfying $\dim(D \cap C_1) = t$.

Theorem 2. *The number of r-dimensional subcodes D satisfying* $\dim(D \cap C_1) = t$ *is*

$$\prod_{i=0}^{i=t-1} \frac{q^{k_1} - q^i}{q^t - q^i} \cdot \prod_{i=0}^{i=r-t-1} \frac{q^k - q^{k_1+i}}{q^r - q^{t+i}}.$$

Proof. The number of r-dimensional subcodes D satisfying $\dim(D \cap C_1) = t$ is equal to the one obtained from enumerating choices of the basis elements of D divided by a factor enumerating different choices of basis elements that give rise to the same subcode D. Note that $\dim(D \cap C_1) = t$ means that there are t basis elements of D that come from the k_1-dimensional subcode C_1; so, the number of ways of choosing the first basis element should be $q^{k_1} - 1$, and the number of ways of choosing the second basis element should be $q^{k_1} - q, \ldots$, and the number of ways of choosing the t-th basis element should be $q^{k_1} - q^{t-1}$. The $(t + 1)$-th basis element should be from the set $C \setminus C_1$, due to the fact $\dim(D \cap C_1) = t$, so the number of ways of choosing the $(t + 1)$-th basis element is $q^k - q^{k_1}$. The $(t+2)$-th basis element, on the one hand, is not a linear combination of the former $t+1$ basis elements, and is also, on the other hand, in the set $C \setminus C_1$ due to the fact $\dim(D \cap C_1) = t$, so the $(t+2)$-th basis element is not a linear combination of the elements of C_1 and the $(t+1)$-th basis element, so the number of ways of choosing the $(t+2)$-th element is $q^k - q^{k_1+1}$. Similarly, the number of ways of choosing the $(t+3)$-th basis element is $q^k - q^{k_1+2}, \ldots$, and the number of ways of choosing the last basis element (the r-th basis element) is $q^k - q^{k_1+r-t-1}$. So, the total number of all the choices of the basis elements of the r-dimensional subcodes D satisfying $\dim(D \cap C_1) = t$ is equal to

$$\prod_{i=0}^{i=t-1} (q^{k_1} - q^i) \cdot \prod_{i=0}^{i=r-t-1} (q^k - q^{k_1+i}). \tag{5}$$

In such a manner, the different choices of basis elements that give rise to the same subcode D are as follows: the number of ways of choosing the first basis element is $q^t - 1$, the number of ways of choosing the second basis element is $q^t - q, \ldots$, and the number of ways of choosing the t-th basis element is $q^t - q^{t-1}$. The $(t + 1)$-th basis element should be in the set $D \setminus (D \cap C_1)$, so the number of ways of choosing the $(t + 1)$-th basis element is $q^r - q^t$. The $(t + 2)$-th basis element is not a linear combination of the former $t + 1$ basis elements, so the number of ways of choosing the $(t + 2)$-th basis element is $q^r - q^{t+1}$. Similarly, the number of ways of choosing the $(t + 3)$-th basis element is $q^r - q^{t+2}, \ldots$, and the number of ways of choosing the last basis element is $q^r - q^{r-1}$. So, the number of different choices of basis elements that give rise to the same subcode D is equal to

$$\prod_{i=0}^{i=t-1} (q^t - q^i) \cdot \prod_{i=0}^{i=r-t-1} (q^r - q^{t+i}). \tag{6}$$

From (5) and (6), we get the result. □

4. An application

An application of an RTW code is for the construction of secret sharing schemes first introduced in [10]. There are several approaches to the construction of secret sharing schemes, and one of them is based on the use of linear codes. Massey [9] found that the construction of secret sharing schemes was closely related to the complete characterization of the minimal codewords of the underlying linear code.

A codeword *covers* another one if the support of the codeword contains that of the other. A nonzero codeword is called a *minimal codeword* if it covers only its scalar multiples, but no other nonzero codewords.

Unfortunately, determining the minimal codewords is extremely hard for general linear codes. Several authors have investigated the minimal codewords and the corresponding secret sharing schemes for certain codes [13,14,1]. In [1], a useful judging rule for determining the minimal codewords was given as follows: in any linear code, let $\omega_{\min}$ and $\omega_{\max}$ be the minimum and maximum nonzero weights, respectively. If

$$\frac{\omega_{\min}}{\omega_{\max}} > \frac{q-1}{q}, \tag{7}$$

then all nonzero codewords of the code are minimal.

By using (7), the minimal codewords can be completely determined for certain RTW codes constructed in the present paper.

From (4), we get

$$\begin{aligned}\frac{d^*}{d} &= \frac{d-(m(p_2)-m(p_1))q^{k-k_1-1}}{d}\\ &= \frac{m(p_2)q^{k-1}-(m(p_2)-m(p_1))q^{k-k_1-1}}{m(p_2)q^{k-1}} \quad \text{(see (4))}\\ &= 1-\frac{m(p_2)-m(p_1)}{m(p_2)}q^{-k_1}.\end{aligned}$$

Using the above equation, we can manage to preserve $m(p_2)-m(p_1)$ to be any positive constant, e.g., $m(p_2)-m(p_1)=1$, and then let $m(p_2)$ be properly large. Then

$$\frac{d^*}{d} > \frac{q-1}{q}$$

can always hold, and then by (7) we get that all the nonzero codewords in the RTW code are minimal codewords. In such a manner, we can construct many RTW codes all of whose nonzero codewords are minimal codewords.

Example 2. Consider the four-dimensional linear code C over $GF(3)$ with a generator matrix

$$\begin{pmatrix}111111111111111111111111111000000000\\000000000111111111222222222111111111\\000111222000111222000111222000111222\\012012012012012012012012012012012012\end{pmatrix},$$

and let C_1 be the two-dimensional subcode generated by the first two rows of the matrix. Then all the nonzero codewords of C_1 have the same weight, $d=27$, and all the codewords of $C\setminus C_1$ have the same weight, $d^*=24$. So C is a $(36, 27, 24)$ RTW code. Since

$$\frac{d^*}{d}=\frac{24}{27}>\frac{q-1}{q}=\frac{2}{3},$$

all the nonzero codewords of C are minimal codewords by (7).

Remark 2. More generally, taking $m(p_2) = 1, m(p_1) = 0, d = q^{k-1}, d^* = q^{k-1} - q^{k-k_1-1}$, and $k_1 \geq 2$, we get an RTW code $C(\frac{q^{k-k_1}(q^{k_1}-1)}{q-1}, q^{k-1}, q^{k-1} - q^{k-k_1-1})$ such that

$$\frac{d^*}{d} = \frac{q^{k_1} - 1}{q^{k_1}} > \frac{q-1}{q}.$$

So, any RTW code $C(\frac{q^{k-k_1}(q^{k_1}-1)}{q-1}, q^{k-1}, q^{k-1} - q^{k-k_1-1})$ for $k_1 \geq 2$, has all the nonzero codewords as the minimal codewords by (7).

Remark 3. An RTW code is a special type of two-weight code. In particular, all the codewords with one of weights in an RTW code must constitute a linear constant-weight subcode according to Definition 2. Thus, the statement that every two-weight linear code is an RTW one is not true. An example is as follows.

Example 3. Consider the four-dimensional binary linear code C generated by the matrix

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

It can be checked that C is a two-weight linear code with weights 8 and 6. However, all the codewords with weight 8 cannot form a linear subcode. To see this, we choose codewords $c_1 = x\boldsymbol{G}$ and $c_2 = y\boldsymbol{G}$, where $x = (0001)$ and $y = (0011)$. Then $c_1 = (01010101010111)$ and $c_2 = (01100110011011)$ are both codewords with weight 8. Since $c_1 - c_2$ is the codeword (00110011001100) with weight 6, all the codewords with weight 8 fail to constitute a subcode. Similarly, we are able to show that all the codewords with weight 6 also fail to constitute a subcode by choosing two codewords with weight 6, say $c_1 = x\boldsymbol{G}$ and $c_2 = y\boldsymbol{G}$, where $x = (0010)$ and $y = (0110)$. This shows that C is not an RTW code.

References

[1] A. Ashikhmin, A. Barg, Minimal vectors in linear codes, IEEE Trans. Inform. Theory 44 (1998) 2010–2017.

[2] D. Britz, T. Britz, K. Shiromoto, H.K. Sørensen, The higher weight enumerators of the doubly-even, self-dual code, IEEE Trans. Inform. Theory 53 (2007) 2567–2571.

[3] R. Calderbank, W.M. Kantor, The geometry of two-weight codes, Bull. London Math. Soc. 18 (1986) 97–122.

[4] W.D. Chen, T. Kløve, The weight hierarchies of q-ary codes of dimension 4, IEEE Trans. Inform. Theory 42 (1996) 2265–2272.

[5] F. De Clerk, M. Delanote, Two-weight codes, partial geometries and Steiner systems, Des. Codes Cryptogr. 21 (2000) 87–98.

[6] P. Delsarte, Weights of linear codes and strongly regular normed spaces, Discrete Math. 3 (1972) 47–64.

[7] T. Kløve, Support weight distribution of linear codes, Discrete Math. 106/107 (1992) 311–313.

[8] Z.H. Liu, W.D. Chen, Notes on the value function, Des. Codes Cryptogr. 54 (2010) 11–19.

[9] J.L. Massey, Minimal codewords and secret sharing, in: Proc. 6th Joint Swedish–Russian Workshop on Information Theory, Mölle, Sweden, Aug. 1993, pp. 276–279.

[10] A. Shamir, How to share a secret, Commun. Assoc. Comp. Mach. 22 (1979) 612–613.

[11] M.A. Tsfasman, S. Vladuts, Geometric approach to higher weights, IEEE Trans. Inform. Theory 41 (1995) 1564–1588.

[12] V.K. Wei, Generalized Hamming weight for linear codes, IEEE Trans. Inform. Theory 37 (1991) 1412–1418.

[13] J. Yuan, C. Ding, Secret sharing schemes from two-weight codes, in: Proc. R.C. Bose Centenary Symp., Discrete Mathematics and Applications, Kolkata, India, Dec. 2002.

[14] J. Yuan, C. Ding, Secret sharing schemes from three classes of linear codes, IEEE Trans. Inform. Theory 52 (2006) 206–212.