THE GEOMETRIC STRUCTURE
OF RELATIVE ONE-WEIGHT CODES

ZHUI LIU*
Department of Mathematics
Beijing Institute of Technology
Beijing, 100081, China

XIANGYONG ZENG
Faculty of Mathematics and Statistics
Hubei Key Laboratory of Applied Mathematics
Hubei University
Wuhan, Hubei 430062, China

(Communicated by Marcus Greferath)

ABSTRACT. The geometric structure of any relative one-weight code is determined, and by using this geometric structure, the support weight distribution of subcodes of any relative one-weight code is presented. An application of relative one-weight codes to the wire-tap channel of type II with multiple users is given, and certain kinds of relative one-weight codes all of whose nonzero codewords are minimal are determined.

1. INTRODUCTION

A relative one-weight code was first introduced in [3] in order to study the relative generalized Hamming weight [6]. Let $C$ be a linear $q$-ary code, and $C_1$ be a linear subcode of $C$. If all the codewords in $C \setminus C_1$ have the same weight, where $C \setminus C_1 = \{c : c \in C \text{ and } c \notin C_1 \}$, then call $C$ a relative one-weight code with respect to the subcode $C_1$.

It is obvious that if $C_1 = \{0\}$, then a relative one-weight code $C$ becomes a linear constant-weight code. Thus, a relative one-weight code is a generalization of a constant-weight code.

The other two special classes of relative one-weight codes are two-weight codes and three-weight codes introduced in [4] and [5], and these two classes of codes are useful in the wire-tap channel of type II with multiple users [6] and secret sharing scheme based on a linear code [10]. A code $C$ is called two-weight with respect to a subcode $C_1$ if both $C_1 \setminus \{0\}$ and $C \setminus C_1$ are constant-weight codes, respectively, and $C$ is called three-weight with respect to two subcodes $C_1 \subset C_2$ if $C_1 \setminus \{0\}$ and $C_2 \setminus C_1$ and $C \setminus C_2$ are constant-weight codes, respectively.

Recently, Wood [9] has generalized relative one-weight codes over the finite field $GF(q)$ to that over finite Frobenius rings by using the homogeneous weight over
rings. Based on a property of the homogeneous weight over rings, Wood also gave a sufficient condition for a code to be relative one-weight.

Motivated by the result in [9], we first give in this paper a necessary and sufficient condition for a q-ary code to be relative one-weight. Such a necessary and sufficient condition is also called the geometric structure of a relative one-weight code. Any relative one-weight code can be constructed by using this geometric structure, and vice versa. We will also see that the geometric structure of a relative one-weight code is a generalization of that of a relative two-weight and three-weight code described in [5]. In addition, we will address the support weight distribution of subcodes of a relative one-weight code and give applications to the wire-tap channel of type II with multiple users and to secret sharing scheme.

2. Preliminaries

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

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 the effective length of \( C \), and \( w(c) \) is exactly the Hamming weight of a codeword \( c \in C \).

Let \( C \) always be a \( k \)-dimensional linear code with effective length \( n \) and let \( C_1 \) be a \( k_1 \)-dimensional subcode of \( C \) throughout this paper unless otherwise stated.

**Definition 1.** A subcode \( D \) of \( C \) is called a relative \( (r, r_1) \) subcode if it satisfies \( \dim D = r \), \( \dim D \cap C_1 = r_1 \).

The value assignment (also called the value function) introduced in [2] is our key tool to study relative one-weight codes.

**Definition 2.** A value assignment is a correspondence \( m(\cdot) : PG(k-1, q) \to N \), where \( N \) represents the set of nonnegative 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 \( m(S) = \sum_{p \in S} m(p) \).

Consider the columns of \( G \), 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 \( m(p) \) be the number of the times the point \( p \) occurs in the columns of \( G \). We thus obtain a value assignment \( m(\cdot) : PG(k-1, q) \to N \) such that \( m(\cdot) \geq 0 \). Obviously, such a value assignment defines a generator matrix and a code (up to equivalence).

For each subset \( L \subset \{1, 2, \cdots k\} \) and \( p = (u_1, \cdots u_k) \in PG(k-1, q) \), let \( P_L(p) = (v_1, \cdots v_k) \), where \( v_i = u_i \) if \( i \in L \), and \( v_i = 0 \) if \( i \notin L \). Define \( P_L(S) = \{P_L(p) : p \in S\} \) for a subset \( S \subset PG(k-1, q) \). Obviously, if \( S \) is a projective subspace, so is \( P_L(S) \) (except the zero vector if any).

**Definition 3 ([3]).** Let \( 0 < k_1 < k \). Then, a relative \( (\xi, \eta) \) subspace, denoted by \( P^\eta_\xi \), is a \( \xi \)-dimensional projective subspace \( P \) satisfying \( \dim P_L(P) = \eta \), where \( L \) denotes the set \( \{1, 2, \cdots, k_1\} \).

**Example 1.** \( P^0_{k_1} \) stands for a point whose first \( k_1 \) coordinate positions are all 0, and all such points constitute the relative projective subspace \( P^0_{k_1} \).

Throughout this paper, let \( C \) be an \([n, k]\) code with a fixed \( k_1 \)-dimensional subcode \( C_1 \), and assume \( G \) is a fixed generator matrix of \( C \) with the first \( k_1 \) rows generating
the subcode $C_1$, and $m(\cdot)$ is determined by $G$. Then, for any relative $(r, r_1)$ subcode $D$, a generator matrix $G_D$ of $D$, with the first $r_1$ rows generating $D \cap C_1$, can be written as $G_D = YG$, where $Y$ is an $r \times k$ matrix. Denote $Y^\perp$ the set of all vectors $v \in GF(q)^k$ perpendicular to each row of $Y$. Then, it can be checked (see [3] for the details) that $Y^\perp$, as a projective subspace, is a relative $(k - r - 1, k_1 - r_1 - 1)$ subspace and is determined uniquely by the subcode $D$, and the value of $m(\cdot)$ on this relative subspace is equal to $n - w(D)$ since $w(D)$ is exactly the number of nonzero columns of the matrix $G_D$. Summing up the text, we thus have

**Lemma 1** ([3]). There is a one-to-one correspondence between the relative $(r, r_1)$ subcodes and the $(k - r - 1, k_1 - r_1 - 1)$ relative projective subspaces such that if $D$ corresponds to a $P_{k-1}^{k_1-r_1-1}$, we will have $n - w(D) = m(P_{k-1}^{k_1-r_1-1})$.

The following well known Gaussian binomial coefficient [7, Theorem 3 in Appendix B]

$$
\begin{align*}
\binom{\alpha + 1}{\beta + 1}_q &= \prod_{\ell=0}^{i=\beta} q^{i+1} - q^i,
\end{align*}
$$

denoted by $X(\alpha, \beta)$ in our paper, is the number of $\beta$-dimensional projective subspaces contained in some $\alpha$-dimensional subspace of $PG(k-1, q)$. By using (1), the number of the $\beta$-dimensional projective subspaces contained in some $\alpha$-dimensional subspace of $PG(k-1, q)$ and passing through a fixed point, denoted by $X1(\alpha, \beta)$, is [7, Theorem 4 in Appendix B]

$$
X1(\alpha, \beta) = \binom{\alpha}{\beta}_q = \prod_{\ell=1}^{i=\beta} q^{i+1} - q^i.
$$

The following Lemmas are from [4].

**Lemma 2.** For any two fixed subspaces $P_{s}^{-1}$ and $P_{s}^{0}$ such that $P_{s}^{0} \supset P_{s}^{-1}$, the number of $P_{s+t-1}^{s-t-1}$ satisfying $P_{s+t-1}^{s-t-1} \supset P_{s}^{0} \supset P_{s}^{-1}$, denoted by $N1(s, t)$, is

$$
N1(s, t) = \begin{cases} 
1 & t = 1 \\
q^{(t-1)(k-k_1-s)} \prod_{i=1}^{t-1} \left( q^{k_1-i} - 1 \right) / \left( q^{i+1} - 1 \right) & t > 1,
\end{cases}
$$

where $1 \leq s \leq k - k_1 - 1$ and $1 \leq t \leq k_1$.

**Lemma 3.** If $1 \leq s \leq k - k_1 - 1$, $1 \leq t \leq k_1$ and $m(P_{s+t-1}^{s-t-1}) = \text{constant}$, $\forall P_{s+t-1}^{s-t-1} \subset PG(k-1, q)$, then $m(P_{s+t-1}^{s-t-1}) = \text{constant}$, $\forall P_{s+t-1}^{s-t-1}$.

3. Main result

In this section, we will first give the geometric structure of a relative one-weight code by using the value assignment and then determine the support weight distribution of subcodes of a relative one-weight code by using its geometric structure.

First, by using similar counting arguments as given in the proof of Lemma 2 (see [4]), one gets

**Lemma 4.** For any two fixed subspaces $P_{s}^{-1}$ and $P_{s+1}^{1}$ such that $P_{s+1}^{1} \supset P_{s}^{-1}$, the number of $P_{s+t-1}^{s-t-1}$ satisfying $P_{s+t-1}^{s-t-1} \supset P_{s+1}^{1} \supset P_{s}^{-1}$, denoted by $N2(s, t)$, is

$$
N2(s, t) = \begin{cases} 
1 & t = 2 \\
q^{(t-2)(k-k_1-s)} \prod_{i=2}^{t-1} \left( q^{k_1-i} - 1 \right) / \left( q^{i+1} - 1 \right) & t > 2,
\end{cases}
$$
where $1 \leq s \leq k - k_1 - 1$ and $1 \leq t \leq k_1$.

Recall that the notation $P^0_{k-k_1}$ stands for a $(k - k_1)$-dimensional projective subspace $P$ such that $\dim P_L(P) = 0$, where $L$ denotes the set $\{1, 2, \cdots, k_1\}$.

It can be checked that the number of the relative subspaces $P^0_{k-k_1}$ is $\frac{q^{k_1} - 1}{q - 1}$.

Denote these $\frac{q^{k_1} - 1}{q - 1}$ subspaces by $P^0_{k-k_1}(i)$, $1 \leq i \leq \frac{q^{k_1} - 1}{q - 1}$, respectively.

Using above notations, we may present the geometric structure of a relative one-weight code.

**Theorem 1.** $C$ is a relative one-weight code with respect to $C_1$ if and only if $m(\cdot)$ satisfies the property: every point in $P^{-1}_{k-k_1-1}$ has the same value, and for every $i$ with $1 \leq i \leq \frac{q^{k_1} - 1}{q - 1}$, every point in $P^0_{k-k_1}(i) \setminus P^{-1}_{k-k_1-1}$ has the same value (the values may be different for different $i$).

**Proof.** The sufficient condition.

The conditions in the theorem yield that if $P_L(p_1) = P_L(p_2)$, then $m(p_1) = m(p_2)$. Thus, $m(P^n_{\xi_1}) = m(P^n_{\xi_2})$ whenever $\xi_1 = \xi_2$ and $\eta_1 = \eta_2$ and $P_L(P^n_{\xi_1}) = P_L(P^n_{\xi_2})$.

Fix a $P^{k_1-1}_{k-2}$. Since

$$\max \{\dim(P_L(P^n_{\xi})) \mid P^n_{\xi} \text{ is any relative projective subspace} \} \leq k_1 - 1,$$

it follows that $P_L(P^n_{\xi}) = P_L(P^{k_1-1}_{k-2})$ for any $P^n_{\xi}$ with $\eta = k_1 - 1$. Thus, $m(P^n_{\xi}) = m(P^{k_1-1}_{k-2})$ whenever $\xi = k - 2$ and $\eta = k_1 - 1$, which means $m(P^n_{\xi})$ is constant for $\xi = k - 2$ and $\eta = k_1 - 1$, and thus $w(c) = m(PG(k - 1, q)) - m(P^{k_1-1}_{k-2})$ is constant for any $c \in (C \setminus C_1)$ by Lemma 1, that is, $C$ is a relative one-weight code with respect to $C_1$.

The necessary condition.

Assume the weight of the codewords of $C \setminus C_1$ is $d'$ and the effective length of $C$ is $n$. Then for any $P^{k_1-1}_{k-2}$, we have $m(P^{k_1-1}_{k-2}) = n - d'$ by Lemma 1, and thus $m(P^{k_1-1}_{k-k_1-2})$ is constant, $\forall P^{k_1-1}_{k-k_1-2}$, by Lemma 3.

Similarly to (2), the number of $\beta$-dimensional projective subspaces contained in some $\alpha$-dimensional subspace of $PG(k - 1, q)$ and passing through two fixed points, denoted by $X2(\alpha, \beta)$, may be written as $[7, \text{Theorem 4 in Appendix B}]$

$$X2(\alpha, \beta) = \left[ \begin{array}{c} \alpha - 1 \\ \beta - 1 \end{array} \right] = \prod_{i=2}^{\alpha} \frac{q^{\alpha+1} - q^i}{q^{\beta+1} - q^i}.$$

To prove $m(\cdot)$ takes the same value at each point of $P^{k-k_1-1}_{k-1}$, we fix a point $p_0 \in P^{k-k_1-1}_{k-1}$ and will show $m(p) = m(p_0)$ for any point $p \in P^{k-k_1-1}_{k-1}$. The method is to sum $m(P^{k-k_1-2}_{k-1})$ is constant over all the subspaces $P^{k-k_1-2}_{k-1} \subset P^{k-k_1-1}_{k-1}$ such that $p_0 \in P^{k-k_1-2}_{k-1}$. During the above summing process, on the one hand, $p_0$ will occur $X1(k - k_1 - 1, k - k_1 - 2)$ times, i.e., the number of subspaces $P^{k-k_1-2}_{k-1} \subset P^{k-k_1-1}_{k-1}$ such that $p_0 \in P^{k-k_1-2}_{k-1}$ (see (2)), on the other hand, each point $p \in (P^{k-k_1-1}_{k-1}\setminus\{p_0\})$ will occur $X2(k - k_1 - 1, k - k_1 - 2)$ times, i.e., the number of subspaces $P^{k-k_1-2}_{k-1} \subset P^{k-k_1-1}_{k-1}$ such that $p_0 \in P^{k-k_1-2}_{k-1}$ and $p \in P^{k-k_1-2}_{k-1}$ (see (5)). We thus have
\[
\sum_{p_0 \in P_{k-k_1-2}} m(P_{k-k_1-2})^{-1} = X_1(k - k_1 - 1, k - k_1 - 2) m(P_{k-k_1-2})^{-1}
\]

\[
= X_1(k - k_1 - 1, k - k_1 - 2) m(p_0) + X_2(k - k_1 - 1, k - k_1 - 2) m(P_{k-k_1-1}^{-1} \setminus \{p_0\})
\]

\[
= (X_1(k - k_1 - 1, k - k_1 - 2) - X_2(k - k_1 - 1, k - k_1 - 2)) m(P_{k-k_1-2})^{-1}
\]

Since \(m(P_{k-k_1-2})^{-1} = \text{constant}\) and (6) always holds for any other point \(p_0' \in P_{k-k_1-1}^{-1}\), we obtain

\[
(X_1(k - k_1 - 1, k - k_1 - 2) - X_2(k - k_1 - 1, k - k_1 - 2)) m(p_0')
\]

It follows from (7) that \(m(p_0') = m(p_0)\) since \(X_1(k - k_1 - 1, k - k_1 - 2) - X_2(k - k_1 - 1, k - k_1 - 2) \neq 0\) by (2) and (5). Thus, \(m(p) = m(p_0), \forall p \in P_{k-k_1-2}^{-1}\).

Fix any \(P_{k-k_1}^0(i)\), say \(P_{k-k_1}^0(1)\), among \(1 \leq i \leq \frac{q^{k_1} - 1}{q-1}\). To prove \(m(p) = \text{constant}\) for any \(p \in (P_{k-k_1}^0)_{P_{k-k_1-1}^{-1}}\), we first fix a point \(p_0 \in (P_{k-k_1}^0)_{P_{k-k_1-1}^{-1}}\) and enumerate the projective subspaces \(P_{k-k_2}^{k_1-1}\) passing through \(p_0\).

Consider a fixed \(P_{k-k_1-2}^{-1} \subset P_{k-k_1-1}^{-1}\) and denote the subspace generated by the point \(p_0\) and the points of \(P_{k-k_1-2}^{-1}\) by \(P_{k-k_1-1}^0\). Then, by substituting \(s = k - k_1 - 1\) and \(t = k_1\) into Lemma 2, we obtain that the number of \(P_{k-k_2}^{k_1-1}\) satisfying \(P_{k-k_2}^{k_1-1} \supset (P_{k-k_1}^0)_{P_{k-k_1-1}^{-1}}\) is \(N1(k - k_1 - 1, k_1)\), which should be the number of all \(P_{k-k_2}^{k_1-1}\) passing through the point \(p_0\) and containing the fixed \(P_{k-k_1-2}^{-1}\). Since the number of \(P_{k-k_1-2}^{-1}\) contained in \(P_{k-k_1-1}^{-1}\) is \(X(k - k_1 - 1, k - k_1 - 2)\) by (1), it follows that the total number of \(P_{k-k_2}^{k_1-1}\) passing through \(p_0\) should be

\[
\pi_1 := N1(k - k_1 - 1, k_1) X(k - k_1 - 1, k - k_1 - 2).
\]

As a next step, we compute the number of \(P_{k-k_2}^{k_1-1}\) passing through \(p_0\) and a fixed point \(p' \in (PG(k-1, q) \setminus P_{k-k_1}^0)_{P_{k-k_1-1}^{-1}}\). Still, fix a \(P_{k-k_1-2}^{-1} \subset P_{k-k_1-1}^{-1}\) and compute the number of \(P_{k-k_2}^{k_1-1}\) passing through \(p_0\) and \(p'\) and containing the fixed \(P_{k-k_1-2}^{-1}\). Denote the subspace generated by \(p_0, p'\) and the points of \(P_{k-k_1-2}^{-1}\) by \(P_{k-k_1-1}^1\). Then, such a computation is equivalent to counting the number of \(P_{k-k_2}^{k_1-1}\) such that \(P_{k-k_2}^{k_1-1} \supset P_{k-k_1}^1 \supset P_{k-k_1-2}^{-1}\), and this counting can be achieved by substituting \(s = k - k_1 - 1\) and \(t = k_1\) in Lemma 4. Thus, the number of \(P_{k-k_2}^{k_1-1}\) such that \(P_{k-k_2}^{k_1-1} \supset P_{k-k_1}^1 \supset P_{k-k_1-2}^{-1}\) is \(N2(k - k_1 - 1, k_1)\). Since the number of \(P_{k-k_1-2}^{-1}\) contained in \(P_{k-k_1-1}^{-1}\) is \(X(k - k_1 - 1, k - k_1 - 2)\) by (1), it follows that the total number of \(P_{k-k_2}^{k_1-1}\) passing through \(p_0\) and \(p'\) should be

\[
\pi_2 := N2(k - k_1 - 1, k_1) X(k - k_1 - 1, k - k_1 - 2).
\]

Now we enumerate \(P_{k-k_2}^{k_1-1}\) passing through \(p_0\) and a fixed point \(p' \in (P_{k-k_1}^0(1) \setminus \{p_0\})\). Assume \(p_0p' \cap P_{k-k_1-1}^{-1} = p''\), where \(p_0p''\) stands for the subspace (or the line) generated by \(p_0\) and \(p'\). Then, enumerating \(P_{k-k_2}^{k_1-1}\) passing through
$p_0$ and $p'$ is equivalent to enumerating $P_{k-2}^{k_1-1}$ passing through $p_0$ and $p''$, which is also equivalent to enumerating $P_{k-2}^{k_1-1}$ passing through $p_0$ and containing a subspace $P_{k-1-k_1-2}^{-1}$ with $p'' \in P_{k-1-k_1-2}^{-1}$. We still fix a $P_{k-1-k_1-2}^{-1}$ with $p'' \in P_{k-1-k_1-2}^{-1}$ and denote the subspace generated by $p_0$ and the points of the fixed $P_{k-1-k_1-2}^{-1}$ by $P_{k-1-k_1-2}^{0}$, and then we enumerate $P_{k-2}^{k_1-1}$ passing through $p_0$ and containing the fixed $P_{k-1-k_1-2}^{-1}$ with $p'' \in P_{k-1-k_1-2}^{-1}$, i.e., the subspaces $P_{k-2}^{k_1-1}$ such that $P_{k-2}^{k_1-1} \supset P_{k-1-k_1-2}^{0} \supset P_{k-1-k_1-2}^{-1}$. Again, substituting $s = k - k_1 - 1$ and $t = k_1$ into Lemma 2, we obtain that the enumeration should be equal to $N1(k - k_1 - 1, k_1)$. Since the number of $P_{k-1-k_1-2}^{-1} \subset P_{k-1-k_1-2}^{-1}$ with $p'' \in P_{k-1-k_1-2}^{-1}$ is equal to $X1(k - k_1 - 1, k - k_1 - 2)$ by (2), it follows that the total number of $P_{k-1-k_1-2}^{1}$ passing through $p_0$ and $p''$, i.e., passing through $p_0$ and the fixed point $p' \in (P_{k-1-k_1-2}^{0}(1) \{p_0\})$, is

$$\pi_3 := N1(k - k_1 - 1, k_1)X1(k - k_1 - 1, k - k_1 - 2).$$

Summing $m(P_{k-2}^{k_1-1}) = \text{constant over all the possible } P_{k-2}^{k_1-1}$ with $p_0 \in P_{k-2}^{k_1-1}$, and making use of (8), (9) and (10), we obtain

$$\sum_{p_0 \in P_{k-2}^{k_1-1}} m(P_{k-2}^{k_1-1}) = \pi_1 m(P_{k-2}^{k_1-1})$$

$$= \pi_1 m(p_0) + \pi_3 m(P_{k-1-k_1-2}^{0}(1) \{p_0\}) + \pi_2 m(PG(k - 1, q) \{P_{k-1-k_1-2}^{0}(1)\})$$

$$= (\pi_1 - \pi_3)m(p_0) + \pi_3 m(P_{k-1-k_1-2}^{0}(1)) + \pi_2 m(PG(k - 1, q) \{P_{k-1-k_1-2}^{0}(1)\}).$$

Note that (11) always holds whenever the point $p_0$ is replaced by any other point $p' \in (P_{k-1-k_1-2}^{0}(1) \{P_{k-1-k_1-2}^{0}\})$. It follows that $(\pi_1 - \pi_3)m(p'_0) = (\pi_1 - \pi_3)m(p_0)$. Thus, we obtain $m(p'_0) = m(p_0)$ since $\pi_1 - \pi_3 \neq 0$ by (8) and (10), and thus $m(p) = m(p_0)$, $\forall p \in (P_{k-1-k_1-2}^{0}(1) \{P_{k-1-k_1-2}^{0}\})$.

In [9, Theorem 18], Wood gave a judging criterion for a relative one-weight code of a module with respect to one of its submodules over rings, whereas the result of Theorem 1 gives an equivalent condition for a relative one-weight code over finite fields. The annihilators of the submodule in [9, Theorem 18] amount to the relative subspaces $P_{k-1-k_1-2}^{-1}$ in our paper, and those cosets of the annihilators of the submodule therein amount to the relative subspaces $P_{k-1-k_1-2}^{0}(i)$, $1 \leq i \leq \frac{q^{k_1-1} - 1}{q - 1}$, in our paper. Motivated by the result of [9, Theorem 18], we obtain Theorem 1.

If $C$ is a relative one-weight code with the value assignment $m(\cdot)$, then according to Theorem 1, one may assume that $m(p) = v_0$, $\forall p \in P_{k-1-k_1-2}^{-1}$ and $m(p) = v_i$, $\forall p \in P_{k-1-k_1-2}^{0}(i) \{P_{k-1-k_1-2}^{-1}\}$, $i = 1, \ldots, \frac{q^{k_1-1} - 1}{q - 1}$. Using such a value assignment, we may obtain $w(c), c \in (C \setminus C_1)$, as follows.

**Corollary 1.** If $C$ is a relative one-weight code with respect to $C_1$, then

$$w(c) = \frac{q^{k_1-1} - 1}{q - 1} v_0 + (q - 1) q^{k_1-1} \sum_{i = 1}^{\frac{q^{k_1-1} - 1}{q - 1}} v_i, \quad c \in (C \setminus C_1).$$

**Proof.** It follows from Lemma 1 that

$$w(c) = n - m(P_{k-1-k_1-2}^{k_1-1}).$$
The geometric structure of relative one-weight codes

Remark 1. Let the notations be as before. Then, the geometric structures of a relative two-weight code and a relative three-weight code [5] can be considered as special cases of the result of Theorem 1. In fact, if there exists some $1 \leq \theta \leq k_1$ and a subspace $P^k_{k-\theta}$ such that all $v_i$ are equal whenever $P^0_{k-k_1}(i) \subset P^k_{k-\theta}$, and all $v_i$ are equal whenever $P^0_{k-k_1}(i) \subset (PG(k-1,q) \setminus P^k_{k-\theta})$, then the result of Theorem 1 is exactly the geometric structure of a relative three-weight code. Particularly, when $\theta = 1$, such a relative three-weight code becomes a relative two-weight code. When $\theta = 1$ and $v_0 = v_1$, namely, all the points in $PG(k-1,q)$ have the same value, such a relative three-weight code becomes a linear constant-weight code.

Using the geometric structure of a relative one-weight code, one may determine the support weight distribution of its subcodes.

Theorem 2. Assume $C$ is a relative one-weight code with respect to $C_1$. Then,

i) any two $(r,r_1)$ subcodes $E$ and $E'$ have the same support weight if and only if $w(E \cap C_1) = w(E' \cap C_1)$;

ii) any two $(r,r_1)$ subcodes $E$ and $E'$ satisfy $w(E) > w(E')$ if and only if $w(E \cap C_1) > w(E' \cap C_1)$;

iii) the number of all $(r,r_1)$ subcodes $E$ such that $w(E \cap C_1) = t$ is

$$A^t_r = \prod_{i=0}^{r-r_1-1} \frac{q^k - q^{k_1+i}}{q^r - q^{r_1+i}},$$

where $A^t_r$ represents the number of the $r_1$-dimensional subcodes of $C_1$ with support weight $t$.

Proof. i) Assume $E \cap C_1 = D$ and $E' \cap C_1 = D'$. Then, $\dim D = \dim D' = r_1$. Note by Lemma 1 that $D$ corresponds to a $P^k_{k-r_1-1}$, and $E$ corresponds to a $P^k_{k-r_1-1}$ such that $P^k_{k-r_1-1} \subset P^k_{k-r_1-1}$. Similarly, $D'$ corresponds to a $P^k_{k-r_1-1}$ and $E'$ corresponds to a $P^k_{k-r_1-1}$ such that $P^k_{k-r_1-1} \subset P^k_{k-r_1-1}$.

$w(D) = w(D')$ is equivalent to $m(P^k_{k-r_1-1}) = m(P^k_{k-r_1-1})$. Similarly, $w(E) = w(E')$ is equivalent to $m(P^k_{k-r_1-1}) = m(P^k_{k-r_1-1})$. Thus, it suffices to show that $m(P^k_{k-r_1-1}) = m(P^k_{k-r_1-1})$ if and only if $m(P^k_{k-r_1-1}) = m(P^k_{k-r_1-1})$.

For any $P^k_{k-r_1-1}$, one may compute according to the result of Theorem 1 that

$$m(P^k_{k-r_1-1}) = \frac{q^{k-r_1-1} - 1}{q - 1} v_0 + \left(\frac{q^{k-r_1-1} - 1}{q - 1} - \frac{q^{k-r_1-1} - 1}{q - 1}\right) m(P^k_{k-r_1-1})$$

$$= \frac{q^{k-r_1-1} - 1}{q - 1} v_0 + q^{k-r_1-1} m\left(P^k_{k-r_1-1}\right), \quad (v_0 \text{ is defined as before})$$

Advances in Mathematics of Communications Volume 10, No. 2 (2016), 367–377
Using (12), we get

\[ m(P^k_{k-r_1-1}) = q^{k-k_1} - 1 \choose q - 1} v_0 + q^{k-k_1} m\left(P_L(P^k_{k-r_1-1})\right) \]

(13)

\[ m(P_{k-r_1-1}) = q^{k-k_1} - 1 \choose q - 1} v_0 + q^{k-k_1} m\left(P_L(P^k_{k-r_1-1})\right) \]

Since \( P^k_{k-r_1-1} \subset P^k_{k-r_1-1} \) and \( P^k_{k-r_1-1} \subset P^k_{k-r_1-1} \), it follows that

\[ P_L(P^k_{k-r_1-1}) = P_L(P^k_{k-r_1-1}) \]

(14)

From (13) and (14), we get that \( m(P^k_{k-r_1-1}) = m(P^k_{k-r_1-1}) \) if and only if \( m(P^k_{k-r_1-1}) = m(P^k_{k-r_1-1}) \).

ii) Similarly to the proof of i), one obtains that \( m(P^k_{k-r_1-1}) > m(P^k_{k-r_1-1}) \) if and only if \( m(P^k_{k-r_1-1}) > m(P^k_{k-r_1-1}) \) by using (13) and (14). Then, ii) holds due to Lemma 1.

iii) Let \( D \) be any fixed \( r_1 \)-dimensional subcode of \( C_1 \). To get the result of iii), it suffices to compute the number of the \((r, r_1)\) relative subcodes containing \( D \). We count the number of independent \( r - r_1 \) codewords of \( C \backslash C_1 \) such that the subcode generated by these \( r - r_1 \) codewords and \( D \) is a relative \((r, r_1)\) subcode. The first chosen codeword can be any codeword of the set \( C \backslash C_1 \). Thus, the ways to choose the first codeword are \( q^k - q^{k_1} \), the second codeword should not be a linear combination of the elements of \( C_1 \) and the first chosen codeword, so, the number of ways of choosing the second codeword is \( q^k - q^{k_1+1} \). Similarly, the number of ways of choosing the third codeword are \( q^k - q^{k_1+2}, \ldots \), and the number of ways of choosing the \((r - r_1)\)th codeword is \( q^k - q^{k_1+r_1-1} \). To get a relative \((r, r_1)\) subcode containing \( D \) in the above way, the repeated times of the first codeword is \( q^r - q^{r_1} \), and the repeated times of the second codeword is \( q^r - q^{r_1+1} \), similarly, the repeated times of the \((r-r_1)\)th codeword is \( q^r - q^{r-1} \). So, the number of relative \((r, r_1)\) subcodes containing \( D \) is

\[ \prod_{i=0}^{r-r_1-1} \frac{q^k - q^{k_1+i}}{q^r - q^{r_1+i}}, \]

and thus iii) holds.

4. AN APPLICATION OF RELATIVE ONE-WEIGHT CODES IN THE WIRE-TAP CHANNEL OF TYPE II

The aim of this section is to present a property of relative subcodes of a relative one-weight code, and then to give an application of the property in the wire-tap channel of type II with multiple users introduced in [6]. Let \( C_J \) be the shortened subcode of \( C \) supported by \( J \), that is, \( C_J = \{ c = (c_1, \cdots, c_n) \in C : c_i = 0 \text{ when } i \notin J \} \), where, \( J \) is a subset of the coordinate positions. Then, a property of relative subcodes is
The geometric structure of relative one-weight codes

**Theorem 3.** If \( C \) is a relative one-weight code with length \( n \) and \( D \) is any \((r,r_1)\) subcode with \( w(D) < n \), then \( C_{\chi(D)} \) is a relative \((r',r'_1)\) subcode with \( r' - r'_1 = r - r_1 \).

**Proof.** By the definition of relative subcodes, it can be checked that \( C_{\chi(D)} \supseteq D \), \( r' \geq r \), \( r'_1 \geq r_1 \), and \( r' - r'_1 \geq r - r_1 \). Furthermore, \( w(C_{\chi(D)}) = w(D) = |\chi(D)| \).

Since there are relative subspaces \( P_{k-r-1}^{k_1-r_1-1} \) and \( P_{k-r'-1}^{k_1-r'_1-1} \) corresponding to \( D \) and \( C_{\chi(D)} \), respectively, and

\[
\begin{align*}
n - w(D) &= m(P_{k-r-1}^{k_1-r_1-1}) \\
n - w(C_{\chi(D)}) &= m(P_{k-r'-1}^{k_1-r'_1-1}),
\end{align*}
\]

by Lemma 1 and \( w(D) < n \), one gets that \( m(P_{k-r-1}^{k_1-r_1-1}) = m(P_{k-r'-1}^{k_1-r'_1-1}) > 0 \) and \( P_{k-r-1}^{k_1-r_1-1} \supseteq P_{k-r'-1}^{k_1-r'_1-1} \). It follows from (12) that

\[
\begin{align*}
m(P_{k-r-1}^{k_1-r_1-1}) &= \frac{q^{k-k_1-r+r_1} - 1}{q - 1} v_0 + q^{k-k_1-r+r_1} m(PL(P_{k-r-1}^{k_1-r_1-1})) \\
=m(P_{k-r'-1}^{k_1-r'_1-1}) &= \frac{q^{k-k_1-r'+r'_1} - 1}{q - 1} v_0 + q^{k-k_1-r'+r'_1} m(PL(P_{k-r'-1}^{k_1-r'_1-1})).
\end{align*}
\]

Thus,

\[
0 = \frac{q^{k-k_1-r+r_1} - q^{k-k_1-r'+r'_1}}{q - 1} v_0 + q^{k-k_1-r+r_1} m(PL(P_{k-r-1}^{k_1-r_1-1})) - q^{k-k_1-r'+r'_1} m(PL(P_{k-r'-1}^{k_1-r'_1-1})) \\
\geq \frac{q^{k-k_1-r+r_1} - q^{k-k_1-r'+r'_1}}{q - 1} v_0 + (q^{k-k_1-r+r_1} - q^{k-k_1-r'+r'_1}) m(PL(P_{k-r-1}^{k_1-r_1-1})) \\
\geq 0.
\]

Thus,

\[
\frac{q^{k-k_1-r+r_1} - q^{k-k_1-r'+r'_1}}{q - 1} v_0 = 0
\]

and

\[
(q^{k-k_1-r+r_1} - q^{k-k_1-r'+r'_1}) m(PL(P_{k-r-1}^{k_1-r_1-1})) = 0.
\]

If \( r' - r'_1 > r - r_1 \), then since \( q^{k-k_1-r+r_1} - q^{k-k_1-r'+r'_1} > 0 \), we get \( v_0 = 0 \) and \( m(PL(P_{k-r-1}^{k_1-r_1-1})) = 0 \), and then \( m(P_{k-r-1}^{k_1-r_1-1}) = 0 \) by (16). Thus, \( w(D) = n \) by (15), a contradiction to the fact \( w(D) < n \). Thus, \( r' - r'_1 = r - r_1 \). \( \square \)

**Remark 2.** The concept of relative subcodes is useful in the wire-tap channel of type II with two parties (or users) and an adversary introduced in [6]. When a linear code \( C \) and one of its subcodes \( C_1 \) are used in such a channel, one may explain an \((r,r_1)\) relative subcode \( D \) as follows: whenever the adversary taps the symbols given by \( \chi(D) \), he will retrieve at least \( r \) data symbols, and in these data symbols, the adversary may get at least \( r - r_1 \) data symbols which are from the legitimate party, and the remaining data symbols are from the nonlegitimate party (i.e., the party’s data symbols are leaked to the adversary). Thus, \( C \) and \( C_1 \) should be encoded such that the adversary can get as few of the legitimate party’s data symbols as possible. Whenever a relative one-weight code is used in the wire-tap channel of type II with two parties, the above theorem yields that, for any relative \((r,r_1)\) subcode \( D \) \( (w(D) < n) \), the adversary can get no more data symbols than
Definition 4. A codeword covers a codeword', if the support of c contains that of c'. If a nonzero codeword c covers only its nonzero scalar multiples, but no other nonzero codewords, then c is called minimal.

All the minimal codewords of a relative two-weight code and a relative three-weight code are determined in [5]. For an arbitrary relative one-weight code, it is difficult to determine all the minimal codewords. But it is possible to determine all the minimal codewords for some special classes of relative one-weight codes.

Assume A is a subset of PG(k − 1, q). Use ⟨A⟩ to represent the subspace generated by the points in A and use ⟨A⟩⊥ to represent the subspace perpendicular to ⟨A⟩ according to the usual inner product. In addition, let C be a relative one-weight code (with respect to a k1-dimensional subspace C1) with the value assignment m(·), and let L = {1, · · · , k1} and vj, 1 ≤ j ≤ qk1 − 1 − 1 be defined as in Section 3. Then, the result is

Theorem 4. All the nonzero codewords of a relative one-weight code C are minimal if one of the following conditions holds

i) |{j : vj = 0, 1 ≤ j ≤ qk1 − 1 − 1}| ≤ qk1 − 2 − 1;

ii) There exists a group of basis points pj, 1 ≤ j ≤ k1, of PL(PG(k − 1, q)), such that m(p) > 0 for any p ∈ ⟨{pj, pj+1}⟩ for 1 ≤ j1 < j2 ≤ k1.

Proof. The arguments for i) and ii) are similar. We only give the proof of ii) in detail.

Let G be the generator matrix of C determined by m(·) and let c and c' be any two nonzero codewords. Then, one may write

c = xG, c' = x'G.

for some x, x' ∈ GF(q)k. If c covers c', then

(17) \{p : p ∈ ⟨{x}⟩⊥ and m(p) > 0\} ⊂ \{p : p ∈ ⟨{x'}⟩⊥ and m(p) > 0\}.

Since both ⟨{x}⟩⊥ and ⟨{x'}⟩⊥ are (k − 2)-dimensional projective subspaces, it follows from (17) that ⟨{x}⟩⊥ = ⟨{x'}⟩⊥ if one can prove that any (k − 2)-dimensional subspace P is generated by the points p ∈ P such that m(p) > 0. Then, the fact ⟨{x}⟩⊥ = ⟨{x'}⟩⊥ yields that c and c' differ only by a nonzero multiple, or equivalently, c is minimal.

Thus, it suffices to prove that any (k − 2)-dimensional subspace P is generated by the points p ∈ P such that m(p) > 0. Note that a (k − 2)-dimensional subspace P is either Pk2,2 or Pk2,2−1.
1. Thus, (19) and Theorem 1 again yield that

Furthermore, it can be checked that

\[ m(P_{k-2}^{k_1-2}) = \{ p : p \in P_{k-1}^{-1} \} \]

due to the fact

\[ P_{k-2}^{k_1-2} = \{ s_j : 2 \leq j \leq k_1 \} \cup \{ p : p \in P_{k-1}^{-1} \} \]

by (18).

2. Then, since \( \dim(P_{L}(PG(k-1, q))) = k_1 - 1 \) and \( p_j, 1 \leq j \leq k_1 \), is a group of basis points of \( P_{L}(PG(k-1, q)) \), there exist points \( p_j', 1 \leq j \leq k_1 \), such that \( P_{L}(p_j') = P_{L}(p_j) \) for \( 1 \leq j \leq k_1 \) and

\[ P_{k-2}^{k_1-1} = \{ p_j' : 1 \leq j \leq k_1 \} \cup \{ p \in (P_{k-2}^{k_1-1} \cap P_{k-1}^{-1}) \} \].

Furthermore, it can be checked that \( m(p_j') = m(p_j) > 0 \) for \( 1 \leq j \leq k_1 \) by Theorem 1. Thus, (19) and Theorem 1 again yield that

\[ P_{k-2}^{k_1-1} = \{ p : p \in P_{k-2}^{k_1-2} \} \]

We would like to thank the referees very much for their valuable comments and suggestions.

Acknowledgments

References

[1] A. Ashikhmin and A. Barg, Minimal vectors in linear codes, IEEE Trans. Inf. Theory, 44 (1998), 2010–2017.
[2] W. D. Chen and T. Kløve, The weight hierarchies of q-ary codes of dimension 4, IEEE Trans. Inf. Theory, 42 (1996), 2265–2272.
[3] Z. H. Liu and W. D. Chen, Notes on the value function, Des. Codes Crypt., 54 (2010), 11–19.
[4] Z. H. Liu, W. D. Chen, Z. M. Sun and X. Y. Zeng, Further results on support weights of certain subcodes, Des. Codes Crypt., 61 (2011), 119–129.
[5] Z. H. Liu and X. W. Wu, On relative constant-weight codes, Des. Codes Crypt., 75 (2015), 127–144.
[6] Y. Luo, C. Mitraptant, A. J. H. Vinck and K. Chen, Some new characters on the wire-tap channel of type II, IEEE Trans. Inf. Theory, 51 (2005), 1222–1229.
[7] F. J. MacWilliams, N. J. A. Sloane, The Theory of Error Correcting Codes, North Holland, Amsterdam, 1977.
[8] V. V. Wei, Generalized Hamming weight for linear codes, IEEE Trans. Inf. Theory, 37 (1991), 1412–1418.
[9] J. A. Wood, Relative one-weight linear codes, Des. Codes Crypt., 72 (2014), 331–344.
[10] J. Yuan and C. Ding, Secret sharing schemes from three classes of linear codes, IEEE Trans. Inf. Theory, 52 (2006), 206–212.

Received July 2014; revised August 2015.

E-mail address: lzhui@bit.edu.cn
E-mail address: xiangyongzeng@aliyun.com