Pusan Kyŏngnam Math J 12(1996), No 2, pp 155–162

ON GENERALIZED HAMMING WEIGHTS OF CYCLIC LINEAR CODES GENERATED BY A WEIGHT 2 CODEWORD

SEON JEONG KIM AND MI JA YOO

1. Introduction and Preliminaries

Let F be a field with two elements. A binary code is simply a linear subspace C of F^n. The elements of a code are called codewords, the integer n is called the length of the code. An $[n,k]$-code means the code of length n, and of dimension k. The weight $w(v)$ of a codeword $v = (v_1, v_2, \cdots, v_n)$ is defined by $w(v) = \text{card}\{i \mid v_i \neq 0\}$. The weight $w(V)$ of a subcode V of a code C is defined by $w(V) = \text{card}\{i \mid v_i \neq 0 \text{ for some } v \in V\}$. In [W], Wei introduced the generalized Hamming weights which are defined as $d_r(C) = \min\{w(V) \mid V \text{ is an } r\text{-dimensional subspace of } C\}$, for $1 \leq r \leq \dim C$. Also it has been shown in [W] that the weight hierarchy of a linear code completely characterizes the performance of the code on a type II wire-tap channel. Here $d_1(C)$ is just the minimum distance of C which is one of important parameters of a code C.

A code C is said to be cyclic if $(v_2, v_3, \cdots, v_n, v_1) \in C$ for every $(v_1, v_2, \cdots, v_n) \in C$. A cyclic code C is said to be generated by a codeword v if C is the smallest cyclic code containing v. In this paper, we find the generalized Hamming weights of a cyclic code C which is generated by single codeword of weight 2.

The following are well-known facts on the generalized Hamming weights.

Received September 10,1996

Partially supported by KOSEF-GARC and by the Basic Research Institute Program, Ministry of Education. 1995, Project No BSRI-95-1406

THEOREM 1.1 (MONOTONICITY) [W]. *Let C be an $[n,k]$-code, then*

$$1 \leq d_1(C) < d_2(C) < \cdots < d_k(C) \leq n.$$

THEOREM 1.2 (DUALITY) [W]. *Let C be an $[n,k]$-code and $C^\perp$ be the dual code. Then*

$$\{d_r(C) \mid 1 \leq r \leq k\} = \{1,2,\cdots,n\} - \{n+1-d_r(C^\perp) \mid 1 \leq r \leq n-k\}.$$

The author would like to thank the referee for his/her comments and corrections to the previous version of this paper.

2. Main Results

Recall that there is a natural vector space homomorphism

$$\phi : F[x]/(x^n - 1) \longrightarrow F^n$$

defined by

$$\phi(a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + (x^n - 1)) = (a_0, a_1, \cdots, a_{n-1}),$$

and there is a one-to-one correspondence induced by ϕ between the set of ideals of $F[x]/\ (x^n - 1)$ and the set of cyclic codes in F^n. (See [L] for more detail.) Thus the cyclic code generated by a codeword $(a_0, a_1, \cdots, a_{n-1})$ corresponds to the ideal in $F[x]/(x^n - 1)$ generated by $a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + (x^n - 1)$. This ideal is also generated by the coset whose representative element is the greatest common divisor of $a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$ and $x^n - 1$. Note that $x^n - 1 = x^n + 1$ since we only deal with $F = \{0,1\}$.

LEMMA 2.1. *Let C be a cyclic code of length n generated by a codeword v of weight 2 Then it corresponds to the ideal in $F[x]/(x^n - 1)$ generated by $1 + x^l + (x^n - 1)$ for some divisor l of the integer n.*

Proof. By definition of cyclic code, we may assume that $v = (a_0, a_1, \cdots, a_{n-1})$, where $a_0 = 1$ and $a_m = 1$. By the above comment, C corresponds to the ideal of $F[x]/(x^n - 1)$ generated by $1 + x^m + (x^n - 1)$, then this ideal is also generated by a coset whose representative is the greatest common divisor of $1+x^m$ and x^n-1. Let $n=mq+r$ with $0\leq r\leq m-1$ Since

$$\begin{aligned} x^n-1 &= x^{mq+r}-1 \\ &= (x^{mq}-1)x^r+(x^r-1), \end{aligned}$$

by Euclidean Algorithm, we see that $\gcd\{1+x^m, x^n-1\} = 1+x^l$, where $l=\gcd\{m,n\}$. Thus the proof is complete

A matrix G is called a generator matrix of a code C if its rows form a basis of C. It is a well-known fact that a generator matrix of the cyclic code corresponding to the ideal generated by the coset with representative element $1+x^l$, where l is a divisor of n, is

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 & 1 & & 0 \\ & & & \ddots & & & & \ddots & \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 & . & 1 \end{pmatrix},$$

where the second 1 is in the $l+1$th place in the first row.

We use the following lemma to prove our main theorem.

LEMMA 2.2 *For $l, a\geq 2$, let G be a matrix*

$$G = \left(\begin{array}{c|c} & I_l \\ & I_l \\ I_{l(a-1)} & \vdots \\ & I_l \\ & I_l \end{array}\right)_{l(a-1)\times la},$$

where I_k denotes the $k\times k$ identity matrix. Then for any $ha-1$ $(1\leq h\leq l)$ columns of G, there exist linearly independent $ha-h$ columns

Proof. Let u_i denote the i-th column of G for $1\leq i\leq la$, and let B_1 and B_2 be the sets of columns of G such that

$$\begin{aligned} B_1 &= \{u_i \mid 1\leq i\leq l(a-1)\}, \\ B_2 &= \{u_i \mid l(a-1)+1\leq i\leq la\}. \end{aligned}$$

Note that each vector in B_1 has only one nonzero coordinate and that in B_2 has exactly $a-1$ nonzero coordinates. Also note that the vectors in each B_i, $i = 1,2$ are linearly independent.

First, we prove the case for $h = 1$. Let $A = \{u_{i_j} \mid 1 \leq j \leq a-1\}$ be a set with $a-1$ columns of G. If $A \cap B_2 = \emptyset$, then the elements in A are linearly independent. Suppose that $A \cap B_2 \neq \emptyset$, and let

$$b_1 u_{i_1} + b_2 u_{i_2} + \cdots + b_{a-1} u_{i_{a-1}} = 0, \quad b_i \in F,$$

where $u_{i_j} \in B_1$ for $1 \leq j \leq t$, $u_{i_j} \in B_2$ for $t+1 \leq j \leq a-1$, and $t \leq a-2$. Then we get

$$b_1 u_{i_1} + b_2 u_{i_2} + \cdots + b_t u_{i_t} = b_{t+1} u_{i_{t+1}} + \cdots + b_{a-1} u_{i_{a-1}}. \qquad (*)$$

Suppose that both sides are not equal to 0. Then the number of nonzero coordinates in the left side is less than or equal to $t \leq a-2$, and that in the right side is greater than or equal to $a-1$, which is a contradiction. Thus both sides are equal to 0 and hence all coefficients b_j are zero, or equivalently the elements in A are linearly independent.

Now we prove the cases for $2 \leq h \leq l$. Let $A = \{u_{i_j} \mid 1 \leq j \leq ha-1\}$ be a set of columns in G, and A' be the set of vectors in $A \cap B_2$ which are expressed as linear combinations of the vectors in $A \cap B_1$. Note that each vector in B_2 are expressed as a linear combination of the vectors in B_1;

$$u_{l(a-1)+j} = \sum_{t=0}^{a-2} u_{j+tl} \qquad \text{for } 1 \leq j \leq l.$$

Since the sets $\{u_{j+tl} \mid 0 \leq t \leq a-2\}$ for $1 \leq j \leq l$ are disjoint, A' has at most $[\frac{ha-1}{l}] \leq h-1$ vectors in $A \cap B_2$. Hence

$$\mathrm{card}(A - A') \geq ha - 1 - (h-1) = ha - h.$$

Now we shall claim that any $ha-h$ vectors in $A - A'$ are linearly independent. Let $u_{i_1}, u_{i_2}, \cdots, u_{i_{ha-h}}$ be elements in $A - A'$ and suppose that

$$b_1 u_{i_1} + b_2 u_{i_2} + \cdots + b_{ha-h} u_{i_{ha-h}} = 0, \quad b_i \in F,$$

where $u_{i_j} \in B_1$ for $1 \leq j \leq t$, $u_{i_j} \in B_2$ for $t+1 \leq j \leq ha-h$. For each j with $t+1 \leq j \leq ha-h$, there is at least one nonzero coordinate of u_j where the coordinates of the other vectors in A are 0. Because such u_j can not be expressed as a linear combination of vectors in $A \cap B_1$ and all vectors in B_2 has nonzero coordinates at distinct places. Hence the above equation implies that $b_j = 0$ for all $t+1 \leq j \leq ha-h$. Since all vectors in B_1 are linearly independent, the other coefficients are also zero. Thus $u_{i_1}, u_{i_2}, \cdots, u_{i_{ha-h}}$ are linearly independent, and we have proved the lemma.

Finally we prove the main theorem.

THEOREM 2.3. *Let C be a cyclic code of length n generated by weight 2 codeword $(a_0, a_1, \cdots, a_{n-1})$ with $a_i = a_j = 1$. Then the dimension of C is $l(a-1)$ and the generalized Hamming weights are*

$$d_r(C) = r + \lceil \frac{r}{a-1} \rceil \text{ for } 1 \leq r \leq l(a-1),$$

where $l = \gcd\{j-i, n\}$, $a = \frac{n}{l}$.

Proof. As in the proof of Lemma 2.1, we may assume that $a_0 = a_l = 1$. Hence a generator matrix of the cyclic code C is

$$G = \begin{pmatrix} 1 & 0 & \dots & 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & & & & & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 1 & \dots & 0 & 1 \end{pmatrix}_{l(a-1) \times la},$$

where the second 1 is in the $l+1$th place in the first row.

We perform the following elementary row operation on the matrix G;

$$v_i' = v_i + (v_{i+l} + v_{i+2l} + v_{i+3l} + \cdots)$$

for each $i = 1, 2, \cdots, l(a-2)$, where v_i denotes the i-th row of G. Then we obtain another generator matrix G' whose rows are v_i';

$$G' = \begin{pmatrix} & \mid & I_l \\ & \mid & I_l \\ I_{l(a-1)} & \mid & \vdots \\ & \mid & I_l \\ & \mid & I_l \end{pmatrix}_{l(a-1)\times la.}$$

Now we use induction on h to prove that for any h, $0 \le h \le l-1$,

$$d_r(C) = r + (h+1) \ \text{ for } \ h(a-1)+1 \le r \le (h+1)(a-1),$$

which is equivalent to the theorem.

Let $h = 0$. Since the dimension of the code is less than n, clearly the minimun distance $d_1(C) \ge 2$. On the other hand we see $w(v_1') = 2$, hence $d_1(C) = 2$. For $1 < r \le a-1$, we have

$$w(D_r(1, l+1, 2l+1, \cdots, (r-1)l+1)) = r+1,$$

where the notation $D_r(i_1, \cdots, i_r)$ means r-dimensional subcode generated by the rows $v_{i_1}', \cdots, v_{i_r}'$ of G'. Hence $d_r(C) \le r+1$. Using Theorem 1.1, we conclude that $d_r(C) = r+1$.

Assume, as an induction hypothesis, that the following holds;

$$d_r(C) = r + (s+1) \ \text{ for } \ s(a-1)+1 \le r \le (s+1)(a-1).$$

For $r = (s+1)(a-1)+1$, by assumption, we have $d_{r-1}(C) = (s+1)a$. So we have the inequality $d_r(C) \ge (s+1)a+1$, here we prove that the equality does not hold. If $d_r(C) = (s+1)a+1$, then there exists a subcode D of C such that $w(D) = (s+1)a+1$ and $\dim(D) = (s+1)(a-1)+1$.

By definition of $w(D)$, all vectors in D have zero coordinates at $la - ((s+1)a+1) = (l-s-1)a-1$ places, simultaneously. That is, the following inclusion holds;

$$D \subset \{(c_1, c_2, \cdots, c_{la}) \in C \mid c_{i_j} = 0 \text{ for } j = 1, 2, \cdots, (l-s-1)a-1\}, (*)$$

for fixed $c_{i_j} = 0$ for $j = 1, 2, \cdots, (l-s-1)a-1$. Since the rows of G' form a basis of C, every element of D is also expressed as a linear combination of them. Since

$$a_1 v_1' + \cdots + a_{l(a-1)} v_{l(a-1)}' = (\, a_1 \cdots a_{l(a-1)} \,) \begin{pmatrix} v_1' \\ \vdots \\ v_{l(a-1)}' \end{pmatrix} = (a \cdot u_1, \cdots, a \cdot u_{la}),$$

where v_i', u_i are rows and columns of G' respectively, and $a \cdot u_i$ means the usual scalar product of $a = (a_1, \cdots, a_{l(a-1)})$ and u_i, the above inclusion $(*)$ is equivalent to

$$D \subset \{a_1 v_1' + \cdots + a_{l(a-1)} v_{l(a-1)}' \mid a \cdot u_{i_j} = 0 \text{ for } j = 1, 2, \cdots, (l-s-1)a-1\}.$$

Hence we obtain

$$\begin{aligned} &\dim D \\ &\le \dim\{a_1 v_1' + \cdots + a_{l(a-1)} v_{l(a-1)}' \mid a \cdot u_{i_j} = 0 \text{ for } j = 1, 2, \cdots, (l-s-1)a-1\} \\ &= \dim\{(a_1, \cdots, a_{l(a-1)}) \mid a \cdot u_{i_j} = 0 \text{ for } j = 1, 2, \cdots, (l-s-1)a-1\}. \end{aligned}$$

By Lemma 2.2, the rank of the matrix $(u_{i_1}, \cdots, u_{i_{(l-s-1)a-1}})$ is at least $(l-s-1)a-(l-s-1)$, using the dimension theorem in Linear Algebra, we have

$$\begin{aligned} \dim D &\le l(a-1) - ((l-s-1)a - (l-s-1)) \\ &= (s+1)(a-1), \end{aligned}$$

which contradicts the fact that $\dim D = (s+1)(a-1)+1$. Thus $d_r(C) \ge (s+1)a+2$.

On the other hand, since

$$\begin{aligned} &w(D_r(\{bl + c \mid 0 \le b \le a-2,\ 1 \le c \le s+1\} \cup \{s+2\})) \\ &\quad = (s+1)a+2, \end{aligned}$$

we conclude that $d_r(C) = (s+1)a+2$.

For r, $(s+1)a - s < r \le (s+2)a - (s+2)$, we have $w(D_r(\{bl + c \mid 0 \le b \le a-2,\ 1 \le c \le s+1\} \cup \{(s+2) + bl \mid 0 \le b \le r+s-(s+1)a\}))$ noindent $= r + (s+2)$. Then, by Theorem 1.1, we have $d_r(C) = r + (s+2)$. Thus the proof is complete.

References

[L] R. F. Lax, *Modern Algrbra and Discrete Structures*, Harper Collins Publishers Inc., 1991.

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

Department of Mathematics
and Research Institute of Natural Science
Gyeongsang National University
Chinju, 660-701, Korea
E-mail : skim@nongae.gsnu.ac.kr