East Asian Math. J. 17(2001), No. 1, pp 167-174

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

Mi Ja Yoo

Abstract We find the generalized Hamming weights of cyclic linear q-ary codes which are generated by a codeword of weight 2, and of any length.

1. Introduction and preliminaries

This paper is a continuity of [1]. Let F_q be a field with q elements. A *code* is simply a linear subspace C of F_q^n. The elements of a code are called *codewords*, the integer n is called the *length* of the code. An $[n,k]_q$-code means the code of length n, and of dimension k. In [3], Wei introduced the notion of generalized Hamming weights and weight hierarchy for a linear code, which has been motivated by several applications in cryptography. Let C be an $[n,k]_q$ code. The *weight* $w(c)$ of a codeword $c=(c_1,c_2,\cdots,c_n)$ is defined by $w(c)=\mathrm{card}\{i \mid c_i \neq 0\}$ The weight $w(D)$ of a subcode D of a code C is defined by

$$w(D)=\mathrm{card}\{i \mid c_i \neq 0 \text{ for some } c \in D\}.$$

The *generalized Hamming weights* of C are defined as

$$d_r(C)=\min\{w(D) \mid D \text{ is an } r\text{-dimensional subspace of } C\},$$

This work was supported by Korea Research Foundation Grant (KRF-99-005-D00003).

Received November 12, 2000 Revised June 5, 2001

2000 Mathematics Subject Classification. 94B05, 51E20, 05B25

Key words and phrases: linear code, cyclic code, generalized Hamming weight

for $1 \leq r \leq \dim C$. The *weight hierarchy* of a linear code C means the set of generalized Hamming weights $\{d_r(C) \mid 1 \leq r \leq \dim C\}$. Also it has been shown in [3] 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.

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

THEOREM 1.1 (MONOTONICITY) [3]. *Let C be an $[n,k]_q$-code, then*

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

THEOREM 1.2 (DUALITY) [3]. *Let C be an $[n,k]_q$-code and let $C^\perp$ be the dual code. Then*

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

A matrix G is called a *generator matrix* of a code C if its rows form a basis of C. Two codes C_1 and C_2 with generating matrices G_1 and G_2, respectively, are called *equivalent* if G_1 can be transformed into G_2 by elementary row operations, by permuting the columns of G_1 and by multiplying the columns of G_1, by nonzero scalars.

REMARK. *Let C_1 and C_2 be $[n,k]_q$ codes. If two codes C_1 and C_2 are equivalent, then $d_r(C_1) = d_r(C_2)$ for $1 \leq r \leq k$.*

A code C is said to be *cyclic* if $(c_1, c_2, \cdots, c_{n-1}, c_0) \in C$ for any $(c_0, c_1, \cdots, c_{n-1}) \in C$. A cyclic code C is said to be *generated* by a codeword c if C is the smallest cyclic code containing c. In this paper, we find the generalized Hamming weights of a cyclic code C which is generated by single codeword of weight 2.

Consider a natural vector space homomorphism

$$\phi : F_q[x]/(x^n - 1) \longrightarrow {F_q}^n$$

defined by

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

Using this map we obtain the following theorems.

THEOREM 1 3 [2] *There is an one-to-one correspondence between cyclic codes of length n and the ideals of $F_q[x]/(x^n-1)$. Moreover, there is an one-to-one correspondence between cyclic codes and the factors of x^n-1.*

THEOREM 1.4 [1] *Let C be a cyclic code of length n generated by a codeword $(c_0, c_1, \cdots, c_{n-1})$. Then C corresponds to the ideal in $F_q[x]/(x^n-1)$ generated by $g(x)+(x^n-1)$, where $g(x) = gcd\{c_0 + c_1x + \cdots + c_{n-1}x^{n-1}, x^n-1\}$.*

Each cyclic code C of length n corresponds to the unique polynomial $g(x)$, a divisor of x^n-1. We call this polynomial $g(x)$ the *generator polynomial* of the cyclic code C. More precisely, if $g(x) = a_0 + a_1 + \cdots + a_{l-1}x^{l-1} + x^l$, then the cyclic code C is generated by the rows of the matrix

$$\begin{pmatrix} a_0 & a_1 & a_2 & \dots & 1 & 0 & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_{l-1} & 1 & 0 & \dots & 0 \\ 0 & 0 & a_0 & \dots & a_{l-2} & a_{l-1} & 1 & \dots & 0 \\ & & & \ddots & & & & \ddots & \\ 0 & 0 & 0 & \dots & a_0 & a_1 & a_2 & \dots & 1 \end{pmatrix}.$$

2. Main Remarks

We use the following lemmas to prove our main theorem.

LEMMA 2 1 [1] *Let C be a cyclic code with the generator matrix G*

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

where the integers $a, l \geq 2$, I_k denotes the $k \times k$ identity matrix. Then

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

Let C be a cyclic code of length n with the generator polynomial $g(x) = x^l - \alpha$. We will prove that a generator matrix of C is equivalent to the matrix in Lemma 2.1.

LEMMA 2.2 *Let C be a cyclic code of length n with the generator polynomial $x^l - \alpha$, where $\alpha \in F_q$. Then*

(1) If i is the order of α, then n is a multiple of il.

(2) A generator matrix G' of C is

$$G' = \left(\begin{array}{c|c} & (\alpha^{-1})^{i-2}I_l \\ & (\alpha^{-1})^{i-3}I_l \\ & \vdots \\ & I_l \\ & (\alpha^{-1})^{i-1}I_l \\ -\alpha I_{(im-1)l} & \cdot \\ & I_l \\ & \vdots \\ & (\alpha^{-1})^{i-1}I_l \\ & I_l \end{array}\right)_{(im-1)l \times iml},$$

where $m = \frac{n}{il}$.

PROOF (1) Let $n = ld + r$ with $0 \leq r \leq l$. Then

$$\begin{aligned} x^n - 1 &= x^{ld+r} - 1 \\ &= (x^l)^d x^r - 1 \\ &= (x^l - \alpha + \alpha)^d x^r - 1 \\ &\equiv \alpha^d x^r - 1 \pmod{x^l - \alpha}. \end{aligned}$$

Since $x^l - \alpha$ is the generator polynomial of C and $r \leq l$, $\alpha^d x^r - 1 = 0$. Hence $r = 0$, $\alpha^d = 1$. On the other hand, the order of α is i and so d is a multiple of i. Therefore n is a multiple of il.

(2) Since $x^l - \alpha$ is the generator polynomial of C and a generator matrix G for C is

$$\begin{pmatrix} -\alpha & 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 \\ 0 & -\alpha & 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & -\alpha & \dots & 0 & 0 & 1 & \dots & 0 \\ & & & \cdot & & & & \ddots & \\ 0 & 0 & 0 & \dots & -\alpha & 0 & 0 & \dots & 1 \end{pmatrix},$$

where the number 1 is in the $(l+1)$-th place in the first row. We perform the following elementary row operation on the matrix G ;

$$v'_j = v_j + \alpha^{-1}v_{j+l} + (\alpha^{-1})^2 v_{j+2l} + \cdots$$

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

$$G' = \left(\begin{array}{c|c} & (\alpha^{-1})^{i-2}I_l \\ & (\alpha^{-1})^{i-3}I_l \\ & \vdots \\ & I_l \\ & (\alpha^{-1})^{i-1}I_l \\ -\alpha I_{(im-1)l} & \vdots \\ & I_l \\ & \vdots \\ & (\alpha^{-1})^{i-1}I_l \\ & I_l \end{array}\right)_{(im-1)l \times iml.}$$

LEMMA 2 3 *The followng two matrices G and G'' are equivalent*

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

$$G'' = \left(\begin{array}{c|c} & \alpha_1 I_l \\ & \alpha_2 I_l \\ \alpha I_{l(a-1)} & \vdots \\ & \alpha_{a-2} I_l \\ & \alpha_{a-1} I_l \end{array}\right)_{l(a-1)\times la,}$$

where $\alpha, \alpha_i \in F_q$, the integers $l, a \geq 2$.

PROOF We perform the following elementary row operation on G'';

$$v'_j = \alpha_1^{-1} v''_j \quad \text{for} \quad 1 \le j \le l,$$

$$v'_j = \alpha_{i+1}^{-1} v''_j \quad \text{for} \quad il < j \le (i+1)l,$$

for each $i = 1, 2, \cdots, a-2$, where v''_i denotes the i-th row of G''. Then we obtain the generator matrix G' whose rows are v'_j;

$$G' = \left(\begin{array}{cccc|c} \alpha_1^{-1}\alpha I_l & & & & I_l \\ & \alpha_2^{-1}\alpha I_l & & & I_l \\ & & \ddots & & \vdots \\ & & & \alpha_{a-1}^{-1}\alpha I_l & I_l \end{array}\right)_{l(a-1)\times la.}$$

Once more, we perform the following elementary column operation on the matrix G';

$$w_j = \alpha^{-1}\alpha_1 w'_j \quad \text{for} \quad 1 \le j \le l,$$

$$w_j = \alpha^{-1}\alpha_i w'_j \quad \text{for} \quad il < j \le (i+1)j,$$

for each $i = 1, 2, \cdots, a-2$, where w'_j denotes the j-th column of G'. Then we obtain the generator matrix G whose columns are w_j;

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

THEOREM 2 4. *Let C be a cyclic code of length n generated by weight 2 codeword $(c_0, c_1, \cdots, c_{n-1})$ with $c_s = -\beta, c_t = 1$ for $s < t$. Then the generalized Hamming weights of C are as follows;*

$$d_r(C) = \begin{cases} r + \lceil \frac{r}{a-1} \rceil & \text{for } 1 \le r \le l(a-1) \text{ or} \\ r, & \text{for } 1 \le r \le n, \end{cases}$$

where $l = gcd\{t-s, n\}, a = \frac{n}{l}$.

PROOF By the definition of cyclic code, we may assume that $(c_0, c_1, \cdots, c_{n-1})$ where $c_0 = -\beta$, $c_j = 1$ and $j = t - s$. By Theorem 1.4, C corresponds to the ideal of $F_q[x]/(x^n - 1)$ generated by $g(x) = \gcd\{x^j - \beta, x^n - 1\}$. Let $n = jd + r$ with $0 \leq r \leq j - 1$. Since

$$\begin{aligned} x^n - 1 &= x^{jd+r} - 1 \\ &= (x^j - \beta + \beta)^d x^r - 1 \\ &\equiv \beta^d x^r - 1 \ (\bmod\ x^j - \beta) \\ &\equiv x^r - \beta^{-d} \ (\bmod\ x^j - \beta), \end{aligned}$$

by Euclidean Algorithm, we see that $\gcd\{x^j - \beta, x^n - 1\}$ is $x^l - \alpha$ or 1, where $\alpha \in F_q, l = \gcd\{j, n\}$. Hence the generator polynomial $g(x)$ of C is $x^l - \alpha$ or 1.

Case 1. If $g(x) = 1$, then $d_r(C) = r$ for $1 \leq r \leq n$.

Case 2. Let $g(x) = x^l - \alpha$ and let i be the order of α. Then by Lemma 2.2, $n = ilm$ for some integer m and a generator matrix G for C is

$$G = \left(\begin{array}{c|c} & (\alpha^{-1})^{i-2} I_l \\ & (\alpha^{-1})^{i-3} I_l \\ & \vdots \\ & I_l \\ & (\alpha^{-1})^{i-1} I_l \\ -\alpha I_{(im-1)l} & \vdots \\ & I_l \\ & \vdots \\ & (\alpha^{-1})^{i-1} I_l \\ & I_l \end{array}\right)_{(im-1)l \times iml.}$$

By Lemma 2.3, the generator matrix G for C is equivalent to the

following matrix G';

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

Puting $a = im$, by Lemma 2.1 we obtain

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

REFERENCES

[1] S J Kim and M J Yoo, *On Generalized Hamming weights of cyclic linear codes generated by a weight 2 codeword*, Pusan Kyongnam Math **12** (1996), 155–162

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

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

Department of Mathematics
Gyeongsang National University
Chinju 660-701, Korea