Pusan Kyŏngnam Math J 12(1996), No 2, pp. 147–153

ON GENERALIZED HAMMING WEIGHTS OF SOME CYCLIC LINEAR CODES

SEON JEONG KIM AND MI JA YOO

1. Introduction and Preliminaries

Let F_2 be a finite field with two elements, and F_2^n be the set of all n-tuples of elements in F_2. A binary linear code of length n means a subspace of F_2^n. If the binary linear code has dimension k as a subspace of F_2^n, then it is referred to as an $[n,k]$ code over F_2. A linear code C of length n is called cyclic if whenever $(a_1, a_2, \cdots, a_n)$ is an element of C, so is $(a_n, a_1, a_2, \cdots, a_{n-1})$. The dual code $C^\perp$ of a linear code C means the subspace

$$C^\perp = \{x \in F_2^n \mid x \cdot c = 0 \text{ for all } c \in C\},$$

where $x \cdot c = (x_1, x_2, \cdots, x_n) \cdot (c_1, c_2, \cdots, c_n) = x_1c_1 + x_2c_2 + \cdots + x_nc_n$.

In [W], 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 $[n,k]$ code. Let $\chi(C) = \{i \mid x_i \neq 0 \text{ for some } (x_1, x_2, \cdots, x_n) \in C\}$. The rth generalized Hamming weight of C is then defined as

$$d_r(C) = \min\{|\chi(D)| : D \text{ is an } r\text{-dimensional subcode of } C\}.$$

The weight hierarchy of C means the set of generalized Hamming weights $\{d_r(C) \mid 1 \leq r \leq k\}$. Obviously, $d_1(C)$ is just the minimum Hamming weight or minimum Hamming distance of the code.

In this paper, we find the generalized Hamming weights of some binary cyclic codes. Consider a natural vector space isomorphism

$$F_2^n \longrightarrow F_2[x]/(x^n - 1)$$

Received June 28,1996.

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

$$(a_0, a_1, \cdots, a_{n-1}) \mapsto a_0 + a_1\overline{x} + \cdots + a_{n-1}\overline{x}^{n-1},$$

where $\overline{x}$ is a coset $x + (x^n - 1)$. Using this map, we obtain the following theorem.

THEOREM 1.1 [L]. *There is an one to one correspondence between cyclic linear codes of length n and the ideals of $F_2[x]/(x^n - 1)$. Moreover, there is an one to one correspondence between cyclic codes and the factors of $x^n - 1$.*

Thus 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 $g(x) = a_0 + a_1x + \cdots + a_{l-1}x^{l-1} + x^l$, then the corresponding cyclic code is generated by the rows of the matrix

$$\begin{pmatrix} a_0 & a_1 & a_2 & \cdots & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_{l-1} & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & a_0 & \cdots & a_{l-2} & a_{l-1} & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_0 & a_1 & a_2 & a_3 & \cdots & 1 \end{pmatrix}.$$

For such $g(x)$, let $x^n - 1 = g(x)h(x)$. We call $h(x)$ the parity check polynomial of the cyclic code C. Let $h(x) = h_0 + h_1x + \cdots + h_{n-l-1}x^{n-l-1} + x^{n-l}$. Then the parity check matrix of the cyclic code C is

$$\begin{pmatrix} 1 & h_{n-l-1} & h_{n-l-2} & \cdots & h_0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & h_{n-l-1} & \cdots & h_1 & h_0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & h_2 & h_1 & h_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & h_{n-l-1} & h_{n-l-2} & h_{n-l-3} & \cdots & h_0 \end{pmatrix}.$$

Note that this matrix is the generator matrix of the dual code $C^{\perp}$ of C.

The following theorem is easy to prove.

THEOREM 1.2. *Let C be a cyclic code of length n with the generator polynomial $g(x) = (x + 1)^l$, $0 \leq l < n$. Then*

(1) $\dim C = n - l$.
(2) $\dim C^{\perp} = l$.
(3) If $h(x) = (x^n - 1)/g(x)$, *then the polynomial* $x^{\deg h(x)} h(1/x)$ *is the generator polynomial of the dual code of a cyclic code with generator polynomial* $g(x)$.

The following theorems are well-known basic tools used in the next section.

THEOREM 1.3 (MONOTONICITY) [W]. *Let* C *be an* $[n, k]$ *code, then*

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

Remark. When C is nondegenerate, i.e., there is no always-zero bit position, then $d_k(C) = n$.

THEOREM 1.4 (DUALITY) [W]. *Let* C *be an* $[n, k]$ *code and* $C^{\perp}$ *be its dual code. Then*

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

2. A cyclic code with the generator polynomial $g(x) = (1 + x)^l$

Let C be a cyclic code of length n with the generator polynomial $g(x)$. Recall that $g(x)$ is a divisor of $x^n - 1$. In this section, we consider the case $g(x) = (1 + x)^l$ for some $l \geq 0$.

THEOREM 2.1. *Let* C *be a cyclic* $[n, k]$ *code with* $k < n$. *Then* $d_1(C) \geq 2$.

Proof. If $d_1(C) = 1$, then there exists a codeword of weight 1 in C. Since C is cyclic, all vectors $(1, 0, 0, \cdots, 0)$, $(0, 1, 0, \cdots, 0)$, $\cdots$, $(0, 0, \cdots, 0, 1)$ are in C, and so $C = F_2^n$. This contradicts the assumption $k < n$.

THEOREM 2.2. *Let C be a binary cyclic code of length n and $g(x)$ be its generator polynomial. Then the following hold:*

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

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

(3) If $g(x) = x^{n-1} + x^{n-2} + \cdots + x + 1$, then $d_1(C) = n$.

Proof. (1) and (3) are obvious. For (2), since $\dim C = n-1$, $d_1(C) \geq 2$ by Theorem 2.1. Now the result follows from Theorem 1.1.

For convenience, we use a notation, for each integer $r \geq 1$,

$$\gamma_r(C) = \{(\underbrace{c, c, \cdots, c}_{r \text{ times}}) \mid c \in C\}.$$

Obviously, if C is $[n, k, d]$ code, then $\gamma_r(C)$ is an $[rn, k, rd]$ code. Using these notation, we can decompose cyclic codes into those with shorter length.

THEOREM 2.3. *Let C be a binary cyclic code with length 2^i, $i \geq 1$ and $g(x) = (1 + x)^l$ be the generator polynomial of C. The following hold:*

(1) If $l \geq 2^{i-1}$, then $C = \gamma_2(C_1)$, where C_1 is the cyclic code of length 2^{i-1} with the generator polynomial $(x + 1)^{l-2^{i-1}}$.

(2) If $l < 2^{i-1}$, then $C^{\perp} = \gamma_2(C_2)$, where C_2 is the cyclic code of length 2^{i-1} with the generator polynomial $(x + 1)^{2^{i-1}-l}$.

Proof. (1) Let $l = 2^{i-1} + a$, $0 \leq a < 2^{i-1}$. Then

$$\begin{aligned} g(x) &= (1 + x)^l \\ &= (1 + x)^a \cdot (1 + x^{2^{i-1}}) \\ &= (1 + x)^a + (1 + x)^a \cdot x^{2^{i-1}}. \end{aligned}$$

If we set C_1 the cyclic code of length 2^{i-1} with the generator polynomial $(1+x)^a$, then, comparing the generator matrices of C and C_1, we obtain the desired result.

(2) By Theorem 1.2, the generator polynomial of $C^{\perp}$ is $x^{n-l}(1/x + 1)^{n-l} = (1 + x)^{n-l}$. Since $n - l > 2^{i-1}$, we can use (1).

To use Theorem 2.3 effectively, we find new expression for natural numbers.

THEOREM 2.4. *For a given integer $i \geq 1$, any integer l satisfying $1 \leq l \leq 2^i - 1$ can be uniquely expressed as the form*

$$l = 2^{i-1} + a_{i-2} \cdot 2^{i-2} + \cdots + a_1 \cdot 2 + a_0,$$

where $(1, a_{i-2}, a_{i-3}, \cdots, a_1, a_0)$ satisfies the condition

$$(*) \quad \text{there exists an integer } \alpha \geq 0 \text{ such that } \begin{cases} a_j = 1 \text{ or } -1 & \text{for } j \geq \alpha \\ a_j = 0 & \text{for } j < \alpha. \end{cases}$$

Proof. Note that we can express any number as the form

$$b_r \cdot 2^r + b_{r-1} \cdot 2^{r-1} + \cdots b_1 \cdot 2 + b_0,$$

where each coefficient is 0 or 1. If $b_j = 1$ and $b_{j+1} = 0$, then we can replace them by $b'_j = -1$ and $b'_{j+1} = 1$, since $2^j = 2^{j+1} - 2^j$. Repeating this process, we obtain the desired expression. The uniqueness can be easily proved.

In terms of Theorem 2.4, for fixed interger $i \geq 1$, there is an one to one correspondence between the natural numbers less than 2^i and set of i-tuples $(1, a_{i-2}, a_{i-3}, \cdots, a_1, a_0)$ satisfying the above condition $(*)$. So we identify this i-tuple with l or with the cyclic code with the generator polynomial $g(x) = (1+x)^l$.

THEOREM 2.5. *With the same notation above, we have*

(1) $d_r(1, 1, a_{i-3}, \cdots, a_1, a_0) = 2 \cdot d_r(1, a_{i-3}, \cdots, a_1, a_0)$ *for* $1 \leq r \leq n - l$.

(2) $\{d_r(1, -1, a_{i-3}, \cdots, a_1, a_0) \mid 1 \leq r \leq n - l\}$
$= \{1, 2, \cdots, 2^i\} \setminus \{2^i + 1 - d_r(1, 1, -a_{i-3}, \cdots, -a_1, -a_0) \mid 1 \leq r \leq l\}$.

Proof. (1) If $l = 2^{i-1} + 1 \cdot 2^{i-2} + a_{i-3} \cdot 2^{i-3} + \cdots + a_1 \cdot 2 + a_0$, then clearly $l > 2^{i-1}$. By Theorem 2.3.(1), we obtain the equality. (2) If $l = 2^{i-1} + (-1) \cdot 2^{i-2} + a_{i-3} \cdot 2^{i-3} + \cdots + a_1 \cdot 2 + a_0$, then the generator polynomial of the dual code is $l = 2^{i-1} + 1 \cdot 2^{i-2} - a_{i-3} \cdot 2^{i-3} - \cdots - a_1 \cdot 2 - a_0$. So we get the equation by Theorem 1.4.

Example 2.6. Let C be a binary cyclic code with length 2^i and $g(x) = (1+x)^l$ be the generator polynomial of C. Then, using Theorem 2.5 several times, we get the following:

(1) If $l = 2^{i-1} + 2^{i-2} + \cdots + 2 + 1$, then $d_1(C) = 2^i$.
(2) If $l = 2^{i-1} + 2^{i-2} + \cdots + 2^\alpha$ with $\alpha \geq 1$, then

$$d_r(C) = r \cdot 2^{i-\alpha} \text{ for } 1 \leq r \leq 2^\alpha.$$

(3) If $l = 2^{i-1} + 2^{i-2} + \cdots + 2^\alpha - 2^{\alpha-1} - 2^{\alpha-2} - \cdots - 2 - 1$ with $\alpha \geq 1$, then

$$d_r(C) = (r+1) \cdot 2^{i-\alpha-1} \text{ for } 1 \leq r \leq 2^{\alpha+1} - 1.$$

(4) If $l = 2^{i-1} + 2^{i-2} + \cdots + 2^\alpha - 2^{\alpha-1} - 2^{\alpha-2} - \cdots - 2^\beta$ with $\alpha > \beta \geq 1$, then

$$d_r(C) = (r + \lceil \frac{r}{2^{\alpha-\beta+1} - 1} \rceil) 2^{i-\alpha-1} \text{ for } 1 \leq r \leq 2^{\alpha+1} - 2^\beta,$$

where $\lceil t \rceil$ means the integer part of t.
(5) If $l = 2^{i-1} + 2^{i-2} + \cdots + 2^\alpha - 2^{\alpha-1} - 2^{\alpha-2} - \cdots - 2^\beta + 2^{\beta-1} + \cdots + 2 + 1$ with $\alpha > \beta \geq 1$, then

$$d_r(C) = \begin{cases} (r + \lceil \frac{r}{2^{\alpha-\beta} - 1} \rceil) 2^{i-\alpha-1} \text{ for } 1 \leq r \leq (2^{\beta+1} - 2)(2^{\alpha-\beta} - 1) \\ (r + 2^{\beta+1} - 1) 2^{i-\alpha-1} \text{ for } (2^{\beta+1} - 2)(2^{\alpha-\beta} - 1) + 1 \leq \\ \qquad\qquad r \leq 2^{\alpha+1} - 2^{\beta+1} + 1. \end{cases}$$

For a general integer $n \geq 1$, we have the theorem.

THEOREM 2.7. *Let $n = 2^i \cdot m$ with $i \geq 0$ and odd interger $m \geq 1$. Let C be a binary cyclic code with length n and $g(x) = (1+x)^l$ with $1 \leq l \leq 2^i - 1$ be the generator polynomial of C. Suppose that $\overline{C}$ be a binary cyclic code with*

length 2^i and $\overline{g}(x)$ be the generator polynomial of $\overline{C}$. Then $C^\perp = \gamma_m(C)$ and hence $d_r(C^\perp) = m \cdot d_r(\overline{C})$ for $1 \leq r \leq l$.

Proof. The check polynomial $h(x)$ of C is

$$\begin{aligned} h(x) &= (1+x)^{2^i - l} \cdot (1 + x + x^2 + \cdots + x^{m-1})^{2^i} \\ &= (1+x)^{2^i - l} \cdot (1 + x^{2^i} + x^{2 \cdot 2^i} + \cdots + x^{(m-1) 2^i} \\ &= (1+x)^{2^i - l} + (1+x)^{2^i - l} \cdot x^{2^i} + (1+x)^{2^i - l} \cdot x^{2 \cdot 2^i} \\ &\quad + \cdots + (1+x)^{2^i - l} \cdot x^{(m-1) 2^i}. \end{aligned}$$

Hence the generator polynomial of $C^{\perp}$ is $x^{\deg h(x)}h(1/x) = h(x)$. Comparing their generator matrices, we obtain the result.

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