Some results of the Zetterberg codes

Ochiai, Tetsuya / Hiramatsu, Toyokazu

(出版者 / Publisher)
法政大学工学部
(雑誌名 / Journal or Publication Title)
法政大学工学部研究集報 / 法政大学工学部研究集報
(巻 / Volume)
31
(開始ページ / Start Page)
19
(終了ページ / End Page)
26
(発行年 / Year)
1995-03
(URL)
https://doi.org/10.15002/00003822

Some results of the Zetterberg codes

Toyokazu Hiramatsu * and Tetsuya Ochiai **

Abstract

We deal with the several properties of the first Zetterberg code C_4 which is one of the best known double error-correcting codes. We first determine the complete weight hierarchy of C_4 and next treat an algebraic decoding algorithm for C_4. Finally certain relation between the weight distribution of C_4 and the traces of Hecke operators is remarked.

§1 Introduction

For an integer $s > 1$ let $n = 2^{2s} + 1$ and let α be a primitive n th root of unity in the field GF(2^n). The Zetterberg code C_{2s} is defined to be a binary cyclic code of length n generated by the minimal polynomial $g_{2s}(x)$ of α over GF(2). The code C_{2s} has dimension $n-4s$ and minimum distance 5. Therefore C_{2s} is a double error-correcting binary linear code.

From now on we consider the case $s = 2$. According to Berlekamp's algorithm, the factorization of the polynomial $x^{17} - 1$ over GF(2) into irreducible factors is given by the following

$$x^{17} - 1 = (x - 1)(x^8 + x^5 + x^4 + x^3 + 1)(x^8 + x^7 + x^6 + x^4 + x^2 + x + 1).$$

Then we can put

$$g_4(x) = x^8 + x^7 + x^6 + x^4 + x^2 + x + 1, \tag{1}$$

and the roots of $g_4(x)$

$$\{\alpha, \alpha\alpha^2, \cdots, \alpha^{2^7}\} \quad (\alpha^{2^8} = \alpha^{-1}) \tag{2}$$

*,** System and Control Engineering, College of Engineering, Hosei University.

form a normal basis of $GF(2^8)$ over $GF(2)$. It is easily checked that

$$G = \begin{pmatrix} 1\,1\,1\,0\,1\,0\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,1\,1\,0\,1\,0\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,1\,1\,1\,0\,1\,0\,1\,1\,1\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,1\,1\,1\,0\,1\,0\,1\,1\,1\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,1\,1\,1\,0\,1\,0\,1\,1\,1\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,1\,1\,1\,0\,1\,0\,1\,1\,1\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,1\,0\,1\,1\,1\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,1\,0\,1\,1\,1\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,1\,0\,1\,1\,1 \end{pmatrix} \tag{3}$$

is a generator matrix for the code C_4 with generator polynomial $g_4(x)$.

§2 The generalized Hamming weights of C_4

Let C be an (n, k) linear code and D be a subcode of C. The support size of D, denoted by $\chi(D)$, is defined as the number of positions where not all the codewords of D are zero. The r th generalized Hamming weight of C is then defined by

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

for $1 \le r \le k$. In particular, $d_1(C)$ is just the minimum distance of C. The weight hierarchy of C is defined to be the set of generalized Hamming weights $\{d_r(C) : 1 \le r \le k\}$. The following theorem is known as monotonicity of $d_r(C)$ ([5]) and we state it without proof :

Theoerm 1. For every linear (n, k) code C,

$$0 < d_1(C) < d_2(C) < \cdots < d_k(C) \le n.$$

In particular, $d_r(C) \le n - k + r$ for $1 \le r \le k$.

In the following we shall determine the weight hierarchy of the code C_4.

Theorem 2. The Zetterberg code C_4 has the following weight hierarchy :

$$\{d_r(C_4) : 1 \le r \le 9\} = \{5,8,10,11,13,14,15,16,17\}.$$

Proof. First let us recall that $d_1(C_4) = 5$. We can list up the all codewords of C_4 by (3) and then it is easy to construct all 2-dimensional subcodes of C_4. Thus we have $d_2(C_4) = 8$. After a computation similar to that in the above case $r = 2$, we have also $d_3(C_4) = 10$. By Theorem 1, $10 < d_4(C_4) \leq 12$ and we have $d_4(C_4) = 11$ by computations of 4-dimensional subcodes of C_4. Also we obtain $d_5(C_4) = 13$ by similar method. The remaining cases are trivial by Theorem 1.

§3 Algebraic decoding of C_4

In this section we shall give another proof of Lemma 2 in [1] by using $g_4(x)$ of (1).

Let $C(x)$ be a codeword in C_4, $r(x)$ be the received word and $e(x) = r(x) - C(x)$ the error pattern. We consider the syndromes

$$S_i = e(\alpha^i),\ i = 2^j,\ 0 \leq j \leq 7.$$

It is obvious that

$$S_{2^j} = S_1^{2^j}, 0 \leq j \leq 7.$$

In particular we put

$$S_{-1} = S_1^{2^4}$$

and set $\gamma = S_1 S_{-1}$ which is an element in $GF(2^4)$.

Now we define the trace of $\tau \in GF(2^{2s})$ over $GF(2)$ by

$$\mathrm{tr}GF(2^{2s})/GF(2)(\tau) = \tau + \tau^2 + \tau^{2^2} + \cdots + \tau^{2^{2s-1}}$$

Then we have the following theorem which is Lemma 2 ($s = 2$) in [1].

Theorem 3. $\mathrm{tr}GF(2^4)/GF(2)(\gamma^{-1}) = 1$ if and only if two errors have occurred in the transmission.

Proof. The first half. Suppose that two errors with locators α^{j_1} and α^{j_2} have occurred for $0 \leq j_2 \leq j_1 \leq 2^4$. Since

$S_1 = \alpha^{i_1} + \alpha^{i_2}$, $S_{-1} = \alpha^{-i_1} + \alpha^{-i_2}$,

we have

$$\gamma = \alpha^{i_1 - i_2} + \alpha^{-(i_1 - i_2)}.$$

Now we can assume that γ was chosen in such a way that

$$\gamma = \alpha^2 + \alpha^{-2} = \alpha^2 + \alpha^{2^5}.$$

Since $\alpha, \alpha^2, \alpha^{2^2}, \cdots, \alpha^{2^7}$ is a normal basis of $GF(2^8)$ over $GF(2)$, the elements

$$\beta = \alpha + \alpha^{2^4}, \beta^2 = \alpha^2 + \alpha^{2^5}, \beta^{2^2} = \alpha^{2^2} + \alpha^{2^6}, \beta^{2^3} = \alpha^{2^3} + \alpha^{2^7}$$

belong to $GF(2^4)$ and form a normal basis of $GF(2^4)$ over $GF(2)$. Then the minimal polynomial $f_2(x)$ of β over $GF(2)$ is given by the following

$$f_2(x) = x^4 + x^3 + x^2 + x + 1.$$

Therefore $\beta^5 = 1$ and thus

$$\gamma^{-1} = \beta^3 = \beta^{2^3}.$$

Let $\tau \in GF(2^4)$ and

$$\tau = \sum_{i=0}^{3} a_i \beta^{2^i}, \ a_i \in GF(2).$$

Then we have

$$\mathrm{trGF}(2^4)/\mathrm{GF}(2)(\tau) = \sum_{i=0}^{3} a_i.$$

Therefore

$$\mathrm{trGF}(2^4)/\mathrm{GF}(2)(\gamma^{-1}) = 1.$$

The latter half. Let τ be an element of $GF(2^8)$ such that $\mathrm{trGF}(2^8)/\mathrm{GF}(2)(\tau) = 0$.

Then the quadratic equation

$$x^2 + x + \tau = 0$$

has two roots in $GF(2^8)$ given by

$$x = \sum_{i=0}^{7} x_i \alpha^{2^i},$$

where

$$\tau = \sum_{i=0}^{7} b_i \alpha^{2^i};$$
$$x_0 = \delta,\ x_1 = \delta + b_1, \cdots,\ x_7 = \delta + b_1 + \cdots + b_7$$

with $\delta = 0$ or 1 ([3], p.278, Theorem 15).

Since $\gamma^{-1} \in GF(2^4)$ then $trGF(2^8)/GF(2)(\gamma^{-1}) = 0$ and the following equation

$$(x^{1/2})^2 + x^{1/2} + \gamma^{-1} = 0$$

has two roots, say $\delta_1^{1/2}$ and $\delta_2^{1/2}$. Therefore the locators

$$\alpha^{h_1} = S_1 \delta_1^{1/2},\ \alpha^{h_2} = S_1 \delta_2^{1/2}$$

correspond to the syndrome S_1.　Q.E.D.

Based on the above, an algebraic decoding algorithm for C_4 is the following ([1]):

1) Calculate $S_1 = r(\alpha)$ and go to 2).
2) If $S_1 = 0$, then no error has occurred. Otherwise, go to 3).
3) Calculate $\gamma = S_1^n$ and if $\gamma = 1$ there is a single error with locator S_1. Otherwise, go to 4).
4) Calculate γ^{-1} and $tr(\gamma^{-1})$. If $tr(\gamma^{-1}) = 1$ go to 5). Otherwise, three errors have occurred and decoding is failure.
5) Solve the equation

$$x^2 + x + \gamma^{-2} = 0 \qquad (4)$$

and correct two errors on positions

$$\alpha^{(1)} = S_1 \delta_1^{1/2},\ \alpha^{(2)} = S_1 \delta_2^{1/2},$$

where δ_1 and δ_2 are two roots of (4) in $GF(2^8)$.

Remark. The weight distribution of C_4

Let C be a linear code of length n and A_i be the number of codewords of weight i. Then the sequence $\{A_0, A_1, \cdots, A_n\}$ is called the weight distribution of C. In the following we study some relation between the weight distribution of the Zetterberg code C_4 and the traces of Hecke operators acting on spaces of cusp forms ([4]).

For any integer $N \geq 1$, put

$$\Gamma_1(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(Z) : a \equiv d \equiv 1,\ c \equiv 0 \mod N\}.$$

Let k be a positive integer and $S_k(\Gamma_1(N))$ be the linear space of cusp forms of weight k on the group $\Gamma_1(N)$. For

$$f(z) = \sum_{m=1}^{\infty} a_m e^{2\pi\sqrt{-1}mz} \in S_k(\Gamma_1(N)),$$

we set

$$T(n) \cdot f(z) = \sum_{m=1}^{\infty} \left(\sum_{d \mid m,n} d^{k-1} a_{mn/d^2}\right) e^{2\pi\sqrt{-1}mz}$$

and is called the n th Hecke operator on $S_k(\Gamma_1(N))$. Then we have the following trace formula of Hecke operators:

Theorem A. The trace of the Hecke opeator $T(2^4)$ acting on the space of cusp forms $S_k(\Gamma_1(4))$ is given by

$$Tr(T(2^4)) = \begin{cases} 0 & (k = 2) \\ -1 - \sum_t Q_{k-2}(t, 2^4) H(t^2 - 2^6) & (k > 2), \end{cases}$$

where the sum over t is taken over $\{t \in Z : t^2 < 2^6$ and $t \equiv 1 \mod 4\}$, $H(t^2 - 2^6)$ denotes the Kronecker class number of $t^2 - 2^6$ and

$$Q_{k-2}(t, 2^4) = \frac{\rho^{k-1} - \overline{\rho}^{k-1}}{\rho - \overline{\rho}};$$

here ρ and $\overline{\rho}$ denote the zeros of $x^2 - tx + 2^4 = 0$.

We denote by μ_{17} the cyclic group generated by α. Then the dual C_4' of the code C_4 is given by

$$C_4' = \{(\mathrm{trGF}(2^8)/\mathrm{GF}(2)(ax))_{x\in\mu_{17}} : a \in \mathrm{GF}(2^8)\}.$$

Then the weight distribution of C_4' is as follows :

Theorem B. The non-zero weights of the code C_4' are

$$w_t = \frac{1}{2}(17 - t),\ t^2 < 2^6 \text{ and } t \equiv 1 \mod 4 \ ;$$

and w_t has frequency $17H(t^2 - 2^6)$.

It is essential for its proof that if N(t) denotes the number of classes of GF(q) - isomorphisms of elliptic curves over GF(q) such that the number of points over GF(q) is equal to $q + 1 - t$, then

$$N(t) = H(t^2 - 4q).$$

This formula is basically due to Honda and Schoof.

Finally the weight distribution of the Zetterberg code C_4 itself is obtained by applying the MacWilliams theorem ([2], p.39).

Theorem C. The number A_i of codewords of weight i in the Zetterberg code C_4 is given by

$$2^8 A_i = \binom{17}{i} - 17\sum_{\substack{j=0 \\ i\equiv j \bmod 2}}^{i} V_{i,j}(2^4)(1 + \tau_{j+2}(2^4)),$$

where the polynomials $V_{i,j}(2^4)$ are defined by

$$V_{0,0} = 1,\ V_{i,1} = 1,$$
$$(i+1)\,V_{i+1,j+1} = 2^4 V_{i,j+2} + V_{i,j} - (18-i)\,V_{i-1,j+1},$$
$$(0 \le j \le i,\ i \equiv j \bmod 2)$$

and $\tau_k(2^4)$ denotes the trace of the Hecke operator $T(2^4)$ on the space $S_k(\Gamma_1(4))(k \ge 3)$. For convenience we let $\tau_2(2^4) = -2^4$.

References

[1] S. M. Dodunekov and J. E. M. Nilsson, Algebraic decoding of the Zetterberg codes, IEEE Trans. Inform. Theory 38 (1992) 1570－1573.

[2] J. H. van Lint, Introduction to Coding Theory, 2nd Ed. (Springer－Verlag, Berlin Heidelberg, 1992).

[3] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes (North－Holland, Amsterdam. 1977).

[4] R. Schoof and M. van der Vlugt, Hecke operators and the weight distributions of certain codes, J. Comb. Theory, Ser. A 57 (1991) 163－186.

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