数理解析研究所講究録
1109 巻 1999 年 12-21

On designs in codes over $\mathbf{Z}_4$

田辺顕一朗 (Kenichiro Tanabe) tanabe@math.kyushu-u.ac.jp
九州大学大学院数理学研究科
Graduate School of Mathematics
Kyushu University 33
Fukuoka 812-8581, Japan

1 Introduction

The Assmus–Mattson theorem is a method to find designs in linear codes over a finite field. The theorem can find 5-designs in the extended binary Golay code, the extended ternary Golay code, and so on. The theorem is shown by using combinatorial method and MacWilliams identity in [1] (or see [6]).

Let us consider $\mathbf{Z}_4$-codes in this note. It is shown that the lifted Golay code over $\mathbf{Z}_4$ contains 5-designs in [5], [8], and [9]. Hence it is a natural problem to find an analogue of the Assmus–Mattson theorem for $\mathbf{Z}_4$-codes and to show those facts by the theorem.

Recently, Bachoc [2] gave a new proof of the Assmus–Mattson theorem for linear binary codes. She introduced the harmonic weight enumerators for a binary linear code and showed a MacWilliams type identity for the weight enumerators. The Assmus–Mattson theorem for linear binary codes is shown by using this identity and the characterization of designs in terms of the harmonic spaces by Delsarte.

In this note we modify her method and apply it to $\mathbf{Z}_4$-codes. In section 2, we introduce $\mathbf{Z}_4$-codes and designs. In section 3, we give an identity in Theorem 2. But it is not quite MacWilliams type. We have an analogue of the Assmus–Mattson theorem for $\mathbf{Z}_4$-codes by using this identity in Theorem 3. In section 4, we apply this theorem to the lifted Golay code over $\mathbf{Z}_4$ and show that this code contains 5-designs on some Lee compositions with help of computer.

2 Notations and Preliminary

Throughout this note, we use the following notations:

n, t, k : positive integers such that $t, k \leq n$,
$\mathbf{Z}_4$ $:= \mathbf{Z}/4\mathbf{Z}$,
V $:= \mathbf{Z}_4^n$,
C : a $\mathbf{Z}_4$-code,
X : The set of all subset of $\{1, 2, \ldots, n\}$,
X_i : The set of all subset of $\{1, 2, \ldots, n\}$ of cardinality i $(i = 0, \ldots, n)$,
$\mathbf{R}X$, $\mathbf{R}X_i$,$\mathbf{R}V$: The free real vector spaces spanned by respectively the elements of X, X_i, and V.

For $u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \in V$,

$$
\begin{aligned}
s_0(u) &:= \{i \in \{1, \ldots, n\} \mid u_i = 0\},\\
s_1(u) &:= \{i \in \{1, \ldots, n\} \mid u_i = 1 \text{ or } 3\},\\
s_2(u) &:= \{i \in \{1, \ldots, n\} \mid u_i = 2\},\\
\mathrm{supp}(u) &:= \{i \in \{1, \ldots, n\} \mid u_i \neq 0\},\\
(n_0(u), n_1(u), n_2(u)) &:= (\#s_0(u), \#s_1(u), \#s_2(u));\\
&\quad \text{The Lee composition of } u,\\
wt(u) &:= \#\mathrm{supp}(u);\ \text{The Hamming weight of } u,\\
V_{ij} &:= \{u \in V \mid n_1(u) = i \text{ and } n_2(u) = j\},\\
V_i &:= \{u \in V \mid wt(u) = i\},\\
u * s_i(v) &:= \#(\mathrm{supp}(u) \cap s_i(v)),\ (i = 1, 2),\\
uv &:= \sum_{i=1}^{n} u_i v_i.
\end{aligned}
$$

Definition 1 By a $\mathbf{Z}_4$-code of length n we shall mean an additive subgroup of V. For a $\mathbf{Z}_4$-code C, define $C^{\perp} := \{u \in V \mid uv = 0, \text{ for any } v \in C\}$ and the symmetrized weight enumerator of C:

$$\sum_{u \in C} x_0^{n_0(u)} x_1^{n_1(u)} x_2^{n_2(u)}.$$

A $\mathbf{Z}_4$-code C is said to be self-dual if $C = C^{\perp}$. We call an element of $\{(n_0(u), n_1(u), n_2(u)) \mid u \in C\}$ a Lee composition of C and an element of $\{wt(u) \mid u \in C\}$ a Hamming weight of C.

An element of $\mathbf{R}X_k$ is denoted by

$$f = \sum_{a \in X_k} f(a)a$$

We denote an element of $\mathbf{R}V$ similarly. For $f = \sum_{z \in X_k} f(z)z \in \mathbf{R}X_k$, define

$$\tilde{f} := \sum_{u \in X} \Big(\sum_{\substack{z \in X_k \\ z \subset u}} f(z) \Big) u \in \mathbf{R}X,$$

$$\Big(\text{resp. } \tilde{f} := \sum_{u \in V} \Big(\sum_{\substack{z \in V_k \\ \mathrm{supp}(z) \subset \mathrm{supp}(u)}} f(\mathrm{supp}(z)) \Big) u \in \mathbf{R}V \Big).$$

$$f^{(i,j)} := \sum_{v \in V} \Big(\sum_{\substack{u \in V_k \\ u * s_1(v) = i \\ u * s_2(v) = j}} f(\mathrm{supp}(u)) \Big) v \in \mathbf{R}V.$$

for non-negative integers i and j. Note that $\sum_{i=0}^{k} f^{(k-i,i)}(v) = \tilde{f}(v)$ and $f^{(i,j)} = 0$ if $i + j > k$ by the definition. It is shown that $\tilde{f}(u) = 0$, if $wt(u) < k$ or $wt(u) > n - k$ in [2]. The *differentiation* γ is the operator defined by linearity from

$$\gamma(z) = \sum_{y \in X_{k-1},\ y \subset z} y$$

for all $z \in X_k$ and for all $k = 0, 1, \ldots, n$, and Harm_k is the kernel of γ:

$$\mathrm{Harm}_k = \mathrm{Ker}(\gamma|_{\mathbf{R}X_k}), \qquad k = 0, 1, \ldots, n.$$

We introduce the definition of designs and the characterization of designs in terms of the harmonic spaces.

Definition 2 Let i be an integer with $t \leq i$ and λ be a positive integer. Let $\mathcal{B} \subset X_i$. We say $\mathcal{B}$ is a t-(n, i, λ) design (or t-design simply) if $\#\{U \in \mathcal{B} \mid T \subset U\} = \lambda$ for all $T \in X_t$.

Theorem 1 [7] *Let i be an integer with $t \leq i$ and $\mathcal{B} \subset X_i$. $\mathcal{B}$ is a t-design if and only if $\sum_{b \in \mathcal{B}} \tilde{f}(b) = 0$, for any $f \in \mathrm{Harm}_k$ and for any k $(1 \leq k \leq t)$.*

3 An identity and the main theorem

The following identity is essential in Theorem 3.

Theorem 2 ([11] Theorem 2) *Let C be a $\mathbf{Z}_4$-code and $f \in \mathrm{Harm}_k$. Then*

$$\sum_{u\in C^\perp} \tilde{f}(u)(x_0+2x_1+x_2)^{n-n_1(u)-n_2(u)-k}(x_0-x_2)^{n_1(u)}(x_0-2x_1+x_2)^{n_2(u)}$$
$$= \frac{(-1)^k 4^{n-k}}{|C|}\sum_{v\in C}\sum_{m=0}^{k} f^{(m,k-m)}(v)x_0^{n-n_1(v)-n_2(v)-k}x_1^{n_1(v)-m}x_2^{n_2(v)-k+m}$$
$$\times(x_0-x_1)^m(x_0-x_2)^{k-m}.$$

Corollary 1 ([11] Corollary 1) *Let C be a $\mathbf{Z}_4$-code and $f \in \mathrm{Harm}_k$. Then*

$$\sum_{u\in C^\perp} \tilde{f}(u)(x_0+3x_1)^{n-wt(u)-k}(x_0-x_1)^{wt(u)-k}$$
$$= \frac{(-1)^k 4^{n-k}}{|C|}\sum_{v\in C} \tilde{f}(v)x_0^{n-wt(v)-k}x_1^{wt(v)-k}.$$

Remark. This corollary is an analogue result of Theorem 2.1 in [2] for $\mathbf{Z}_4$-codes.

For a $\mathbf{Z}_4$-code C we denote by $\Gamma(C)$ the set of all Lee compositions (n_0, n_1, n_2) of C satisfying one of the following conditions:

1. $n_1 = 0$.
2. $n_1 > 0$ and there is no pair of Lee compositions of C $((a_0, a_1, a_2), (b_0, b_1, b_2))$ such that
   (1) $a_1 = b_1 = 0$, $a_2 > 0$, $b_2 > 0$, and $a_2 + b_2 = n_1$, or
   (2) $a_1 = b_1 = 2(n_1 - a_2 - b_2)$ and $n_2 \geq n_1 - a_2 - b_2 > 0$.
3. $n_1 > 0$ and there is no pair of Lee compositions of C of type (1) and there are pairs of Lee compositions of C of type (2) in 2. For any Lee composition of C of type (2) in 2, $(n - n_2 - a_2 - b_2, n_1, n_2 - n_1 + a_2 + b_2)$ is not a Lee composition of C.

Let $(n_0, n_1, n_2) \in \Gamma(C)$. By the definition of $\Gamma(C)$, two codewords of C with the Lee composition (n_0, n_1, n_2), which have the same support must be scalar multiples of each other. This is the reason of the introduction of $\Gamma(C)$. We can use Theorem 1 in Theorem 3 by this property of $\Gamma(C)$.

For non-negative integers i, j, a, b, and l, define

$$P_l^{(n-2k)}(i-k) := \sum_{m=0}^{l} \binom{i-k}{m} \binom{n-k-i}{l-m} 3^{l-m}(-1)^m$$

; the Krawtchouk polynomials,

$$Q^k(i,j\ ;\ a,b) := \sum_{r,s,t\geq 0} \binom{n-k-i-j}{n-k-i-j-a-b+r+s+t,\ a-s,\ b-r-t} \times \binom{i}{r} \binom{j}{j-s-t,\ s,\ t,} (-1)^{r+s},$$

where

$$\binom{i}{i-j_1-j_2, j_1, j_2} := \frac{i!}{(i-j_1-j_2)!j_1!j_2!}.$$

$P_l^{(n-2k)}(i-k)$ is the coefficient of $x_0^{n-2k-l}x_1^l$ in $(x_0+3x_1)^{n-k-i}(x_0-x_1)^{i-k}$ and $Q^k(i,j\ ;\ a,b)2^a$ is the coefficient of $x_0^{n-k-a-b}x_1^a x_2^b$ in $(x_0+2x_1+x_2)^{n-i-j-k}(x_0-x_2)^i(x_0-2x_1+x_2)^j$.

Now we state the main theorem.

Theorem 3 *Let C be a $\mathbf{Z}_4$-code. For $1 \leq k \leq t$, define*

$$\Lambda_1(k) := \left\{ (a,b) \in \{1,\ldots,n\}^2 \;\middle|\; \begin{array}{l} 0 \leq a+b \leq n-k \text{ and} \\ a > n_1(v) \text{ or } b > n_2(v) \text{ for any } v \in C^\perp \end{array} \right\},$$

$$\Lambda_2(k) := \left\{ c \in \{0,\ldots,n-2k\} \;\middle|\; c+k \text{ is not a Hamming weight of } C^\perp \right\},$$

$$\Lambda_3(k) := \left\{ (n_1(u), n_2(u)) \;\middle|\; u \in C \text{ and } k \leq wt(u) \leq n-k \right\}.$$

Define matrix:

$$M_1(k) := \left(Q^k(i,j\ ;\ a,b)\right)_{(a,b),\ (i,j)} \in \mathrm{Mat}_{\Lambda_1(k)\times\Lambda_3(k)}(\mathbf{R}),$$

$$M_2(k) := \left(P_c^{(n-2k)}(i+j-k)\right)_{c,\ (i,j)} \in \mathrm{Mat}_{\Lambda_2(k)\times\Lambda_3(k)}(\mathbf{R}),$$

$$M(k) := \begin{bmatrix} M_1(k) \\ M_2(k) \end{bmatrix}.$$

Suppose that the rank of $M(k)$ is equal to its column length ($= \#\Lambda_3(k)$) for any k ($1 \leq k \leq t$). Then, the support of the codewords with Lee composition $(n_0, n_1, n_2) \in \Gamma(C)$ with $t \leq n_1 + n_2 \leq n-t$ forms a t-design.

Proof: For k $(1 \le k \le t)$ and $f \in \mathrm{Harm}_k$, define

$$A_{ij} := \sum_{\substack{u \in C \\ n_1(u)=i \\ n_2(u)=j}} \tilde{f}(u), \quad B_{ij} := \sum_{\substack{v \in C^\perp \\ n_1(v)=i \\ n_2(v)=j}} \tilde{f}(v),$$

$$B_{ij}^{(k-m,m)} := \sum_{\substack{v \in C^\perp \\ n_1(v)=i \\ n_2(v)=j}} f^{(k-m,m)}(v).$$

By Theorem 1 and the remark after the definition of $\Gamma(C)$, it is sufficient to show that $A_{ij} = 0$ for any $(i,j) \in \Lambda_3(k)$. By Theorem 2 and its corollary we have two kinds of equations:

$$\begin{aligned} &\sum_{i,j \ge 0} A_{ij}(x_0 + 2x_1 + x_2)^{n-k-i-j}(x_0 - x_2)^i(x_0 - 2x_1 + x_2)^j \\ &= \frac{(-1)^k 4^{n-k}}{|C^\perp|} \sum_{i,j \ge 0} \sum_{m=0}^{k} B_{ij}^{(m,k-m)} x_0^{n-k-i-j} x_1^{i-m} x_2^{j-k+m} \\ &\quad \times (x_0 - x_1)^m (x_0 - x_2)^{k-m}, \end{aligned}$$

$$\begin{aligned} &\sum_{l=k}^{n-k} \sum_{i=0}^{l} A_{i,l-i}(x_0 + 3x_1)^{n-k-l}(x_0 - x_1)^{l-k} \\ &= \frac{(-1)^k 4^{n-k}}{|C^\perp|} \sum_{j=k}^{n-k} \sum_{i=0}^{j} B_{i,j-i} x_0^{n-k-j} x_1^{j-k}. \end{aligned}$$

Comparing the coefficients, we have

$$\begin{aligned} &\sum_{i,j \ge 0} A_{ij} Q^k(i,j;\ a,b) 2^a \\ &= \frac{(-1)^{a+b} 4^{n-k}}{|C^\perp|} \sum_{i,j \ge 0} \sum_{m=0}^{k} B_{ij}^{(m,k-m)} \binom{m}{i-a} \binom{k-m}{j-b} (-1)^{i+j}, \end{aligned}$$

for any (a,b) $(0 \le a+b \le n-k)$, and

$$\sum_{l=k}^{n-k} \sum_{i=0}^{l} A_{i,l-i} P_m^{(n-2k)}(l-k) = \frac{(-1)^k 4^{n-k}}{|C^\perp|} \sum_{i=0}^{m+k} B_{i,m+k-i},$$

for any m $(0 \leq m \leq n-2k)$.

By the definitions of $\Lambda_1(k)$ and $\Lambda_2(k)$,

$$\begin{aligned} \sum_{i,j \geq 0} A_{ij} Q^k(i,j;\ a,b) &= 0, \text{ for any } (a,b) \in \Lambda_1(k), \\ \sum_{l=k}^{n-k} \sum_{i=0}^{l} A_{i,l-i} P_c^{(n-2k)}(l-k) &= 0, \text{ for any } c \in \Lambda_2(k). \end{aligned}$$

Hence we have

$$M(k) \begin{bmatrix} \vdots \\ A_{ij} \\ \vdots \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

We have that $A_{ij} = 0$ for any $(i,j) \in \Lambda_3(k)$ because of the assumption of the rank of $M(k)$ $(1 \leq k \leq t)$. □

4 An Application to the Lifted Golay Code

The lifted Golay code G_{24} over $\mathbf{Z}_4$ is defined in [4]. G_{24} is constructed from the cyclic code with generator polynomial $x^{11} + 2x^{10} + 3x^9 + 3x^7 + 3x^6 + 3x^5 + 2x^4 + x + 3$ by appending 3 to the last coordinate of the generator vectors. G_{24} is a self-dual code over $\mathbf{Z}_4$.

It is shown that G_{24} contains some 5-designs by using computer in [8] and [9] at first. Let C' be a $\mathbf{Z}_4$-code with the same symmetrized weight enumerator as G_{24}. Recently, it is shown that the support of the codewords with any given Lee composition of C' forms a 5-design possibly with repeated blocks in [5].

We apply Theorem 3 to G_{24} (or C'). The symmetrized weight enumerator of G_{24} is given in [3]. We show it in Table 1. The last column in Table 1 gives the value λ in t-$(24,k,\lambda)$ design and "$*$"means that the Lee composition $(n_0,n_1,n_2) \notin \Gamma(G_{24})$ there.

Table 1: Symmetrized weight enumerator of G_{24} [3]

Hamming weight	Lee composition		Number of words	λ
	n_1	n_2		
0	0	0	1	$\times$
8	0	8	759	1
10	8	2	12144	36
12	8	4	170016	1584
	0	12	2576	48
13	12	1	61824	936
14	8	6	765072	*
15	12	3	1133440	40040
16	16	0	24288	*
	8	8	1214400	*
	0	16	759	78
17	12	5	4080384	*
18	16	2	680064	*
	8	10	765072	*
19	12	7	4080384	*
20	16	4	1700160	$\times$
	8	12	170016	$\times$
21	12	9	1133440	$\times$
22	16	6	680064	$\times$
	8	14	12144	$\times$
23	12	11	61824	$\times$
24	24	0	4096	$\times$
	16	8	24288	$\times$
	0	24	1	$\times$

We can see $\Gamma(G_{24}), \Lambda_1(k), \Lambda_2(k)$, and $\Lambda_3(k)$ in Theorem 3 from this table. For example,

$$\Gamma(G_{24}) = \left\{ \begin{array}{l} (16,0,8),(14,8,2),(12,8,4),(12,0,12), \\ (11,12,1),(9,12,3),(8,0,16) \end{array} \right\},$$

$$\Lambda_1(5) = \left\{ \begin{array}{l} (1,15),(1,16),(1,17),(1,18),(2,15), \\ (2,16),(2,17),(3,15),(3,16),(4,15), \\ (17,1),(17,2),(18,1) \end{array} \right\},$$

$$\Lambda_2(5) = \{0,1,2,4,6\},$$

$$\Lambda_3(5) = \left\{ \begin{array}{l} (0,8),(8,2),(8,4),(0,12),(12,1), \\ (8,6),(12,3),(16,0),(8,8),(0,16), \\ (12,5),(16,2),(8,10),(12,7) \end{array} \right\}.$$

The ranks of $M(k)$ in Theorem 3 are computed by using computer.

Table 2

k	$\#\Lambda_1(k)$	$\#\Lambda_2(k)$	$\#\Lambda_1(k)+\#\Lambda_2(k)$	$\#\Lambda_3(k)$	rank$M(k)$
1	66	9	75	20	20
2	47	8	55	19	19
3	32	7	39	17	17
4	21	6	27	16	16
5	13	5	18	14	14
6	7	4	11	13	11

Hence G_{24} (or a $\mathbf{Z}_4$-code with the same symmetrized weight enumerator as G_{24}) contains 5-designs on Lee compositions:

$$(16,0,8),(14,8,2),(12,8,4),(12,0,12),(11,12,1),(9,12,3),(8,0,16).$$

Remark. It was shown that the support of the codewords with any given Lee composition of the lifted quadratic residue code of length 32 over $\mathbf{Z}_4$ forms a 3-design possibly with repeated blocks in [5]. The symmetrized weight enumerator of the code is given in [10]. Similarly we can show those facts for some Lee compositions.

References

[1] E. F. Assmus, Jr. and H. F. Mattson, Jr., "New 5-designs, " *J. Combin. Theory*, vol. 6, pp. 122–151, 1969.

[2] C. Bachoc, "On harmonic weight enumerators of binary codes," preprint.

[3] A. Bonnecaze, P. Solé, C. Bachoc, and B. Mourrain, "Type II codes over $\mathbf{Z}_4$," *IEEE Trans. Inform. Theory*, vol. 43, pp. 969–976, 1997.

[4] A. Bonnecaze, A. R. Calderbank, and P. Solé, "Quaternary quadratic residue codes and unimodular lattices," *IEEE Trans. Inform. Theory*, vol. 41, pp. 366–377, 1995.

[5] A. Bonnecaze, E. Rains, and P. Solé, "3-colored 5-designs and $\mathbf{Z}_4$-codes," preprint.

[6] P. J. Cameron and J. H. Van Lint, *Graphs, Codes and Designs*, London Mathematical Society Lecture Note Series, vol. 43, Cambridge Univ. Press, Cambridge, 1980.

[7] P. Delsarte, "Hahn polynomials, discrete harmonics, and t-designs," *SIAM J. Appl. Math.*, vol. 34, pp.157–166, 1978.

[8] T. A. Gulliver and M. Harada, "Extremal double circulant Type II codes over $\mathbf{Z}_4$ and 5-$(24, 10, 36)$ designs, " *Discrete Math.*, vol. 194, pp. 129–137, 1999.

[9] M. Harada, "New 5-designs constructed from the lifted Golay code over $\mathbf{Z}_4$," *J. Combin. Des.*, vol. 6, pp. 225–229, 1998.

[10] V. Pless and Z. Qian, "Cyclic Codes and Quadratic Residue Codes over Z_4," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1594–1600, 1996.

[11] K. Tanabe, "An Assmus–Mattson theorem for $\mathbf{Z}_4$-codes," preprint, http://www.math.kyushu-u.ac.jp/~tanabe/.