Hokkaido Mathematical Journal Vol. 25 (1996) p. 81–92

On contracted codes: an extension of Pless' theorem on codes

Tsuyoshi ATSUMI

(Received September 22, 1994; Revised April 3, 1995)

Abstract. Using Higman's algebra homomorphism, we prove an extension of Pless' theorem on self-orthogonal symmetry codes. Let C be a self-orthogonal code over F, where F is one of GF(2), GF(3), GF(4), or GF(p^a). Let τ be an automorphism of C. Then, under some additional conditions on τ, the code can be mapped onto a code of a smaller length that is still self-orthogonal.

Key words: contracted code, dual code, group, algebra homomorphism.

1. Introduction

Pless [10] proved the following interesting result on self-orthogonal symmetry codes:

Result 1 *Let C be a symmetry code over* GF(3) *and τ an automorphism of C. Under some additional conditions on τ, the code can be mapped onto a code of a smaller length which is still self-orthogonal.*

In this paper we shall extend Result 1 so that we can apply it to a wider class of orthogonal codes with automorphism groups. Our result will be given in Theorem 1 of Section 4.

Our proof of the main theorem in Section 5 is based on the fact that a contraction map given in [4] and [10] is nothing but Higman's algebra homomorphism (Section 2), which puts contraction of codes in a new perspective.

In Section 6 we study the contracted codes of the Golay code G_{24} and the extended binary quadratic residue code of length 48 as examples. Furthermore, we shall prove the useful lemma 5 which can be applied to decide the contracted code of a given code with a large automorphism group. (This lemma is interesting because it is related to Research Problem (16.4) of MacWilliams-Sloane's book [7].)

The method of attack is based on Higman's algebra homomorphism.

1991 Mathematics Subject Classification : 94B05.

2. Contraction of Matrices

Here we shall state Higman's result and a few lemmas on contraction of matrices. Let R be a commutative ring with identity and X, Y, Z all finite non-empty sets. Let $M_R(X,Y)$ be the totality of maps $A : X \times Y \mapsto R$. A is called an $X \times Y$ *matrix* over R. For $A \in M_R(X,Y)$ and $B \in M_R(Y,Z)$, define $AB \in M_R(Y,Z)$ by

$$AB(x,z) = \sum_{y \in Y} A(x,y)B(y,z) \quad (x \in X, z \in Z).$$

The *transpose* of a matrix A is denoted by A^t. If $\mathbf{P}$, $\mathbf{Q}$ are partitions of X, Y, respectively, then we say that $A \in M_R(X,Y)$ has *property* $(\mathbf{P}, \mathbf{Q})$ if for all $S \in \mathbf{P}, T \in \mathbf{Q}$,

$$\sum_{t \in T} A(s,t) \text{ is independent of } s \in S.$$

Assume that $A \in M_R(X,Y)$ has property $(\mathbf{P}, \mathbf{Q})$. Then for $S \in \mathbf{P}$, $T \in \mathbf{Q}$, we set $\delta(A)(S,T) = \sum_{t \in T} A(s,t)$ for some $s \in S$. Higman [5, p. 1] proved the following proposition.

Proposition 1 *If $A \in M_R(X,Y)$ has property $(\mathbf{P}, \mathbf{Q})$ and $B \in M_R(Y,Z)$ has property $(\mathbf{Q}, \mathbf{U})$, then $AB \in M_R\ (X,Z)$ has property $(\mathbf{P}, \mathbf{U})$ and $\delta(AB) = \delta(A)\delta(B)$.*

Proof. See Higman [5]. □

We call δ in Proposion 1, *Higman's algebra homomorphism.* Let $\mathbf{P} = \{S_1, \ldots, S_l\}$ be a partition of X or Y. We define an $\mathbf{P} \times \mathbf{P}$ matrix $D(\mathbf{P})$ as follows: Let $S_i, S_j \in \mathbf{P}$,

$$D(\mathbf{P})(S_i, S_j) = \begin{cases} |S_i| & \text{if } S_i = S_j \\ 0 & \text{otherwise.} \end{cases}$$

Then we have

Proposition 2 *Suppose that $\mathbf{P} = \{S_1, \ldots, S_l\}$ and $\mathbf{Q} = \{T_1, \ldots, T_m\}$ are partitions of X and Y, respectively. If A and A^t have property $(\mathbf{P}, \mathbf{Q})$ and property $(\mathbf{Q}, \mathbf{P})$, respectively, then*

$$D(\mathbf{Q})\delta(A^t) = \delta(A)^t D(\mathbf{P}).$$

Proof. See Atsumi [2]. □

The following lemma plays an important part in the calculations of the dimension of contracted codes.

Lemma 1 (Block) *Assume that R is a field. Suppose that* $\mathbf{P} = \{S_1, \ldots, S_l\}$ *and* $\mathbf{Q} = \{T_1, \ldots, T_m\}$ *are partitions of X and Y, respectively. If* $A \in M_R\,(X,Y)$ *has property* $(\mathbf{P},\mathbf{Q})$, *then* $\operatorname{rank} A - \operatorname{rank}\delta(A) \leq |Y| - m$.

Proof. See Hughes and Piper [6, p. 43]. □

3. Terminology

Let F be a finite field $\mathrm{GF}(p^a)$, where p is a prime. Let C be a k-dimensional subspace of F^n. Then C is called an (n,k) *code* over F. A vector in C is called a *codeword.* The *weight* of a vector of F^n is defined to be the number of its non-zero coordinates. The *minimum weight* $d(C)$ of a code C is the weight of the non-zero codeword of smallest weight.

Conjugation in $F = \mathrm{GF}(p^a)$ is defined by $x \mapsto \overline{x} = x^p$ for $x \in F$. For vectors $\mathbf{u}$, $\mathbf{v}$ of F^n, the usual *inner product* $(\mathbf{u},\mathbf{v})$ of $\mathbf{u}$ and $\mathbf{v}$ is defined by

$$(\mathbf{u},\mathbf{v}) = u_1\overline{v}_1 +, \ldots, + u_n\overline{v}_n, \tag{1}$$

where $\mathbf{u} = (u_1,\ldots,u_n)$ and $\mathbf{v} = (v_1,\ldots,v_n)$. The *dual code* of C, denoted by $C^\perp$, is the subspace of F^n consisting of all vectors $\mathbf{v} \in F^n$ with $(\mathbf{v},\mathbf{c}) = 0$ for all $\mathbf{c} \in C$. $C^\perp$ has dimension $n-k$. C is called *self-orthogonal* if $C \subseteq C^\perp$ and *self-dual* if $C = C^\perp$.

A *monomial transformation* on F^n is a linear map given by a monomial matrix, that is, a map of the form

$$\tau : (v_1,\ldots,v_n) \mapsto (\epsilon_1 v_{(1)\pi},\ldots,\epsilon_n v_{(n)\pi}),$$

where π is a permutation $\{1,\ldots,n\}$ and $\epsilon_1,\ldots,\epsilon_n$ are non-zero elements of F. Two codes C and C' in F^n is called *equivalent* if there exists a monomial transformation τ such that $C' = C\tau$. Let C be a code over F in F^n. The group $G(C)$ consisting of all monomial transformations which send C onto itself is called the *automorphism group* of the code C. For further information on coding theory, see MacWilliams-Sloane [7]. For codes with automorphism groups, see Yoshida [13] which contains several interesting problems.

4. Contracted codes

Let C be an (n,k) code and τ an element in $G(C)$. As in [3], we call $\tau \in G(C)$ *orderly* if the order of τ equals the order of its induced permutation π. *From now on we assume that $\tau \in G(C)$ is orderly and its induced permutation π is a product of disjoint r cycles of length m with no fixed points.* (Note that τ is order m, $n = mr$ and π is conjugate to τ in the monomial transformation group of F^n.) In order to define the contracted code of C with respect to $\tau \in G(C)$, we need a lot of notations. Let $\pi = \pi_1 \cdots \pi_r$ be a cycle decomposition of the permutation associated to the monomial automorphism τ of the code C , so that every π_i is a cycle of length m by the above assumption. For each cycle π_i, there is a unique non-zero vector $\mathbf{w}^i$ of F^n which has 1 at the smallest coordinate index of the given cycle and 0's elsewhere. Clearly

$$\mathbf{w}^1, \mathbf{w}^1\tau, \dots, \mathbf{w}^1\tau^{m-1}, \mathbf{w}^2, \mathbf{w}^2\tau, \dots, \mathbf{w}^r, \mathbf{w}^r\tau, \dots, \mathbf{w}^r\tau^{m-1} \tag{2}$$

form a basis of F^n. For each vector $\mathbf{v} \in F^n$, we denote by $\tilde{\mathbf{v}}$ the coordinate vector of $\mathbf{v}$ with respect to the above basis (2). For vectors $\mathbf{u}$, $\mathbf{v}$ of F^n, another inner product $(\mathbf{u}, \mathbf{v})_\tau$ is defined by

$$(\mathbf{u}, \mathbf{v})_\tau = \sum_{i=1}^{r} \sum_{j=0}^{m-1} x_{ij}\bar{y}_{ij}, \tag{3}$$

where $\mathbf{u} = \sum_{i=1}^{r} \sum_{j=0}^{m-1} x_{ij}\mathbf{w}^i\tau^j$ and $\mathbf{v} = \sum_{i=1}^{r} \sum_{j=0}^{m-1} y_{ij}\mathbf{w}^i\tau^j$. As in [10], we define a linear transformation σ on F^n by

$$\mathbf{u}\sigma = \mathbf{u} + \mathbf{u}\tau + \cdots + \mathbf{u}\tau^{m-1} \quad \text{for } \mathbf{u} \in F^n,$$

and set

$$F^n\sigma = \{\mathbf{u}\sigma | \mathbf{u} \in F^n\} \text{ and } C\sigma = \{\mathbf{u}\sigma | \mathbf{u} \in C\}.$$

For $i = 1, \dots, r$, set

$$\mathbf{v}^i = \mathbf{w}^i + \mathbf{w}^i\tau + \cdots + \mathbf{w}^i\tau^{m-1}.$$

Then $\mathbf{v}^1, \dots, \mathbf{v}^r$ form a basis of vector subspace $F^n\sigma$. Every element $\mathbf{w}$ of $F^n\sigma$ is of the form

$$\mathbf{w} = \sum_{i=1}^{r} x_i\mathbf{v}^i \quad \text{for some } x_i \in F.$$

The linear transformation φ defined by $(\mathbf{w})\varphi = (x_1, \ldots, x_r)$ for $\mathbf{w} \in F^n\sigma$, is an isomorphism from $F^n\sigma$ onto F^r (compare with the definition of φ in Section 3 in [10]).

Now we define contracted code $\tilde{C}_\tau$ of code C with automorphism τ to be the subspace

$$\tilde{C}_\tau = \{(x_1, \ldots, x_r) | \mathbf{w} = \sum_{i=1}^{r} x_i \mathbf{v}^i \quad \text{for all } \mathbf{w} \in C\sigma\}.$$

Note that $\tilde{C}_\tau = (C\sigma)\varphi = (C)\sigma\varphi$, the image of C under $\sigma\varphi$.

Clearly $\tilde{C}_\tau$ is an subspace of F^r, which is endowed with the usual inner product,

$$(\mathbf{u}, \mathbf{v}) = u_1\overline{v}_1 + \cdots + u_r\overline{v}_r, \tag{4}$$

where $\mathbf{u} = (u_1, \ldots, u_r)$ and $\mathbf{v} = (v_1, \ldots, v_r)$. Our main purpose in this paper is to prove the following

Theorem 1 *If C is self-orthogonal with respect to the inner product* (1) *and for $\tau \in G(C)$, its induced permutation π has r cycles of equal length m and no fixed points, then $\tilde{C}_\tau$ is also self-orthogonal with respect to the inner product* (4) *under one of the following conditions.* (a) *F is* GF(2), (b) *F is* GF(3), (c) *F is* GF(4), (d) *F is* GF(p^a) *and τ is a permutation, i.e., $\tau = \pi$.*

Remark. This theorem implies that the linear transformation $\sigma\varphi$ preserves the property of self-orthogonality.

For contracted codes, see Conway and Pless [3] and Pless [10].

5. Proof of Theorem

Now we start to prove our theorem. From now on suppose that F will denote one of GF(2), GF(3), GF(4), or GF(p^a) in Theorem 1. We shall divide our proof of the theorem into several lemmas. Let us set

$$C_\tau = \{\tilde{\mathbf{v}} | \text{for all } \mathbf{v} \in C\}.$$

(Here recall that $\tilde{\mathbf{v}}$ denotes the coordinate vector of $\mathbf{v}$ with respect to the basis (2).) Then we have the following.

Lemma 2 (a) *C_τ is self-orthogonal with respect to the inner product* (3). (b) *Permutation π sends C_τ onto itself.*

Proof. When F is GF(2), GF(3) or GF(4), $(\mathbf{u},\mathbf{v}) = (\mathbf{u},\mathbf{v})_\tau$. Also, when F is GF(p^a) and τ is a permutation, $(\mathbf{u},\mathbf{v}) = (\mathbf{u},\mathbf{v})_\tau$. These equations imply part (a). We next prove part (b). Let $\mathbf{u} = \sum_{i=1}^{r}\sum_{j=0}^{m-1} x_{ij}\mathbf{w}^i\tau^j$ be a codeword. Clearly $\mathbf{u}\tau = \sum_{i=1}^{r}\sum_{j=0}^{m-1} x_{ij}\mathbf{w}^i\tau^{j+1}$. Since τ is of order m, we have $\tilde{\mathbf{u}}\pi^{-1} = \widetilde{\mathbf{u}\tau}$. This equation proves part (b). □

If $F = $ GF(4), then the lemma above is Theorem 2 of Conway and Pless [4].

Lemma 3 *Let* $\mathbf{u} = \sum_1^r x_i\mathbf{v}^i \in C\sigma$. *That is,* $(x_1,\ldots,x_r) \in \tilde{C}_\tau$. *Then, there exists* $\mathbf{u}' \in C$ *such that* $\mathbf{u} = \mathbf{u}' + \mathbf{u}'\tau + \cdots + \mathbf{u}'\tau^{m-1}$. *Let* $\tilde{\mathbf{u}}' = (x_{11},\ldots,x_{1m},x_{21},\ldots,x_{r1},\ldots,x_{rm})$ *be the coordinate vector of* $\mathbf{u}'$ *with respect to the basis* (2). *Then the following hold:*
(a) *For* $i = 1,\ldots,r$, $x_i = x_{i1} + \cdots + x_{im}$.
(b) $\tilde{\mathbf{u}} = \tilde{\mathbf{u}}' + \tilde{\mathbf{u}}'\pi^{-1} + \cdots + \tilde{\mathbf{u}}'(\pi^{-1})^{m-1}$.

Proof. Clear. □

Let R be a principal ideal domain such that (a) F is a homomorphic image of R and (b) the quotient field K of R has characteristic 0. (For existence proof for such a principal ideal domain R, see Theorem 13.13 in [8, p. 81] and Theorem 13.27 in [8, p. 91].) So let *: $R \mapsto F$ be the ring homomorphism and the kernel of * $\wp$. $\Lambda(C)$ in R^n is defined by taking as its elements all $\mathbf{u} = (u_1,\ldots,u_n) \in R^n$ such that $u_i \in R$ and $\mathbf{u}^* = (u_1^*,\ldots,u_n^*) \in C_\tau$, where $u_i^* \in F$.

To prove our theorem, we need the following simple notation. For $x \in R$, we set $\overline{x} = x^p$, where p is the characteristic of F. (Note that $\overline{x}^* = \overline{x^*}$ in F, where $\overline{x^*}$ is the conjugate of x^* in F (see Section 3).) For $A \in M_R(X,Y)$, we define $\overline{A} \in M_R(X,Y)$ by

$$\overline{A}(x,y) = \overline{A(x,y)} \quad (x \in X, y \in Y).$$

Now we shall finish the proof. Let $\{\mathbf{u}_1,\ldots,\mathbf{u}_l\}$ is a basis of $C\sigma$. Then by Lemma 3 for $i = 1,\ldots,l$, there exists $\mathbf{u}_i' \in C$ such that $\tilde{\mathbf{u}}_i = \tilde{\mathbf{u}}_i' + \tilde{\mathbf{u}}_i'\pi^{-1} + \cdots + \tilde{\mathbf{u}}_i'(\pi^{-1})^{m-1}$. For $i = 1,\ldots,l$, let $\mathbf{w}_i \in \Lambda(C)$ such that $\mathbf{w}_i^* = \tilde{\mathbf{u}}_i'$. The vectors,$\mathbf{w}_1, \mathbf{w}_1\pi^{-1},\ldots,$ $\mathbf{w}_1(\pi^{-1})^{m-1}$, $\mathbf{w}_2, \mathbf{w}_2\pi^{-1},\ldots,$ $\mathbf{w}_l, \mathbf{w}_l\pi^{-1}$, $\ldots, \mathbf{w}_l(\pi^{-1})^{m-1}$ form an $lm \times n$ matrix A (with rows labeled $1,\ldots m, m+1,\ldots,2m,\ldots,(l-1)m+1,\ldots,lm$). Let us set $S_i = \{(i-1)m+1,\ldots,im\}$, $T_j =$ the set of the coordinate indices in π_j, where π_j is a cycle of π.

Let $\mathbf{P} = \{S_1, \ldots, S_l\}$, $\mathbf{Q} = \{T_1, \ldots, T_r\}$. Then we see that $\overline{A}$ and $\overline{A}^t$ have property **(P, Q)** and property **(Q, P)**, respectively. By Proposition 2

$$D(\mathbf{Q})\delta(\overline{A}^t) = \delta(\overline{A})^t D(\mathbf{P}),$$

where $D(\mathbf{Q}) = mI_r$, $D(\mathbf{P}) = mI_l$. Hence,

$$\delta(\overline{A}^t) = \delta(\overline{A})^t. \tag{5}$$

By Proposition 1 we have

$$\begin{aligned} \delta(A\overline{A}^t) &= \delta(A)\delta(\overline{A}^t) \\ &= \delta(A)\delta(\overline{A})^t, \quad \text{by (5).} \end{aligned} \tag{6}$$

It follows from Lemma 2 that every (i, j) component of matrix $A\overline{A}^t$ is in $\wp$, the kernel of *. So is that of matrix $\delta(A\overline{A}^t)$. So this fact and Equation (6) show that

$$\{\delta(A)\delta(\overline{A})^t\}^* = 0 \quad \text{(zero matrix).} \tag{7}$$

Lemma 4 *The rows of matrix $\delta(A)^*$ generate $\tilde{C}_T$ and $\tilde{C}_T$ is self-orthogonal.*

Proof. Lemma 3(a) implies that the rows of $\delta(A^*)(= \delta(A)^*)$ generates $\tilde{C}_T$. This completes the first statement.

$$\begin{aligned} \{\delta(\overline{A})^t\}^* &= \{\delta(\overline{A})^*\}^t \\ &= \delta(\overline{A^*})^t \\ &= \overline{\delta(A^*)}^t \\ &= \overline{\delta(A)^*}^t, \end{aligned}$$

where the third equation holds since δ and $^-$ commute with one another. By this equation and (7), we have

$$\delta(A)^*\overline{\delta(A)^*}^t = 0 \quad \text{(zero matrix),}$$

which shows that $\tilde{C}_T$ is self-orthogonal. $\square$

This lemma completes a proof of our theorem.

6. Examples

To determine the contracted codes of codes given below in Examples 1 and 2, we need the following lemma (cf. Research Problem (16.4) [7, p. 498]).

Lemma 5 *Let C be an (n, k) code over F, having a permutation, π_0 $(= \tau_0)$ in $G(C)$ such that the cycle structure of π_0 is*

$$(1, \ldots, m)(m+1, \ldots, 2m), \ldots, ((r-1)m+1, \ldots, rm). \tag{8}$$

Let G' be a generator matrix for C. Let G be obtained from G' by arranging the columns of G' in the order $1, \ldots, m, m+1, \ldots, 2m, \ldots, (r-1)m+1, \ldots, rm$ given in (8). Suppose $G = [L|R]$, where L is an $k \times lm$ matrix of rank *lm, R is a $k \times (r-l)m$ matrix. Then, the dimension of $\tilde{C}_{\tau_0}$ is greater than or equal to l.*

Proof. We let the vectors in the basis $G = [L|R]$ be denoted by $\mathbf{e}_i$. The vectors, $\mathbf{e}_1, \mathbf{e}_1\pi_0^{-1}, \ldots, \mathbf{e}_1(\pi_0^{-1})^{m-1}, \mathbf{e}_2, \mathbf{e}_2\pi_0^{-1}, \ldots, \mathbf{e}_k, \mathbf{e}_k\pi_0^{-1}, \ldots, \mathbf{e}_k(\pi_0^{-1})^{m-1}$ form an $km \times n$ matrix $A = [L'|R']$ (with rows labeled $1, \ldots, m, m+1, \ldots, 2m, \ldots, (k-1)m+1, \ldots, km$), where L' is a $km \times lm$ matrix, R' is a $km \times (r-l)m$ matrix. Let us set $S_i = \{(i-1)m+1, \ldots, im\}$, $T_j = \{(j-1)m+1, \ldots, jm\}$. Let us set $\mathbf{P} = \{S_1, \ldots, S_k\}$, $\mathbf{Q}' = \{T_1, \ldots, T_l\}$, $\mathbf{Q}'' = \{T_{l+1}, \ldots, T_r\}$. We see that A and L' have property $(\mathbf{P}, \mathbf{Q}' \cup \mathbf{Q}'')$ and property $(\mathbf{P}, \mathbf{Q}')$, respectively. Clearly

$$rank\, \delta(A) \geq rank\, \delta(L'). \tag{9}$$

By Lemma 1,

$$rank\, L' - rank\, \delta(L') \leq lm - l. \tag{10}$$

Since $rank\, L' = rank\, L = lm$, by (10) we have

$$rank\, \delta(L') \geq l.$$

From this inequality and (9),

$$rank\, \delta(A) \geq l. \tag{11}$$

Since the $\mathbf{e}_i + \mathbf{e}_i\pi_0^{-1} + \cdots + \mathbf{e}_i(\pi_0^{-1})^{m-1}$'s generate $C\sigma_0$, it follows from Lemma 3 (a) that the rows of $\delta(A)$ generate $\tilde{C}_{\tau_0}$. So this and (11) prove our lemma. □

Example 1. We take for C the (24, 12) Golay code over GF(2). Note that when $F = \mathrm{GF}(2)$, for every $\tau \in G(C)$ τ equals π, the induced permutation of τ. We shall use the following results (a) and (b) from [7, p. 498]. (a) A double circulant generator matrix G for this code is given by

$$G = [I_{12}|A],$$

where I is the identity matrix of order 12, and

$$A = \begin{pmatrix} 1&1&0&1&1&1&1&0&1&0&0&0\\ 0&1&1&0&1&1&1&1&0&1&0&0\\ 0&0&1&1&0&1&1&1&1&0&1&0\\ 0&0&0&1&1&0&1&1&1&1&0&1\\ 1&0&0&0&1&1&0&1&1&1&1&0\\ 0&1&0&0&0&1&1&0&1&1&1&1\\ 1&0&1&0&0&0&1&1&0&1&1&1\\ 1&1&0&1&0&0&0&1&1&0&1&1\\ 1&1&1&0&1&0&0&0&1&1&0&1\\ 1&1&1&1&0&1&0&0&0&1&1&0\\ 0&1&1&1&1&0&1&0&0&0&1&1\\ 1&0&1&1&1&1&0&1&0&0&0&1 \end{pmatrix}$$

and the columns of G are labeled 21, 7, 16, 12, 19, 22, 0, ∞, 14, 15, 18, 2, 20, 17, 4, 6, 1, 5, 3, 11, 9, 13, 8, 10. (b) Permutation $\pi =$ (21, 7, 16, 12, 19, 22, 0, ∞, 14, 15, 18, 2) (20, 17, 4, 6, 1, 5, 3, 11, 9, 13, 8, 10) is an automorphism of C.

Here in order to define the basis (2) we introduce the following convention: $\infty < 0 < 1 < \cdots < 22$. Let us set $\tau = \pi^6$. Then, τ satisfies the assumptions of Theorem 1. So

$$\tilde{C}_\tau \quad \text{is self-orthogonal.} \tag{12}$$

We apply Lemma 5 with $\pi_0 = \tau$ and $G' = G$. Then we have

$$\dim \tilde{C}_\tau \geq 6. \tag{13}$$

Hence by (12) and (13) we have that

$$\tilde{C}_\tau \text{ is self-dual.}$$

Note that $\tilde{C}_\tau$ has no codewords of weight 2. For if $\tilde{C}_\tau$ has a codeword of weight 2, then the code C has a codeword of weight 4, which contradicts the fact that the minimum weight of the Golay code is 8. We see that $\tilde{C}_\tau$ is equivalent to B_{12} as described in [9].

Example 2. We take for C the (48, 24) extended quadratic residue code over GF(2). Let N denote the set of nonresidues modulo 47. Let

$$\begin{aligned} g(x) &= (1+x)(1+x+x^2+x^3+x^5+x^6+x^7+x^9 \\ &\qquad +x^{10}+x^{12}+x^{13}+x^{14}+x^{18}+x^{19}+x^{23}). \end{aligned}$$

Then

$$g(x)\left(1+\sum_{n\in N} x^n\right) \equiv g(x) \mod (x^{47}-1).$$

By this equation and Theorem 1 in [7, p. 217],

$$< g(x) > \subseteq < 1+\sum_{n\in N} x^n > .$$

Since both $< g(x) >$ and $< 1+\sum_{n\in N} x^n >$ are of 23 dimensions, we must have

$$< g(x) > = < 1+\sum_{n\in N} x^n > .$$

From this equation and a generator matrix (28) in [7, p. 490] it follows that a generator matrix $\hat{G}$ for C is given by

$$\hat{G} = \left(\begin{array}{ccccc|c} & & & & & 0 \\ & & \bar{G} & & & \vdots \\ & & & & & 0 \\ \hline 1 & 1 & \ldots & 1 & 1 & 1 \end{array}\right),$$

where $\bar{G}$ is a generator matrix for the cyclic code $< g(x) >$ of length 47 and the columns of $\hat{G}$ are labeled 0, 1, ..., 46, ∞. Theorem 10 in [7, p 492] states that the automorphism group of the code C contains $PSL_2(47)$. So, this code has a permutation τ of order 2 in $G(C)$, which is given by

$$\tau : y \mapsto -1/y,$$

where $y \in \{0, 1, \ldots, 46, \infty\}$. The cycle structure of τ is

$$(0,\infty)(1,46)(2,23)(3,31)(4,35)(5,28)(6,39)(7,20)(8,41)(9,26)$$

$$(10,14)(11,17)(12,43)(13,18)(15,25)(16,44)(19,42)(21,38)$$
$$(22,32)(24,45)(27,40)(29,34)(30,36)(33,37)$$

In order to define the basis (2) we make the following convention: $\infty < 0 < 1 < \cdots < 46$. Clearly τ satisfies the conditions of Theorem 1. So,

$$\tilde{C}_\tau \text{ is self-orthogonal.} \tag{14}$$

We start to calculate the dimension of $\tilde{C}_\tau$. We see that the columns of $\hat{G}$ whose labels are in 12 cycles of τ, $(0, \infty)$, $(1, 46)$, $(3, 31)$, $(4, 35)$, $(5, 28)$, $(6, 39)$, $(8, 41)$, $(24, 45)$, $(27, 40)$, $(29, 34)$, $(30, 36)$, $(33, 37)$, are independent. We apply Lemma 5 with $\pi_0 = \tau$, and $G' = G$. Then we have

$$\dim \tilde{C}_\tau \geq 12. \tag{15}$$

Hence by (14) and(15) we have that

$$\tilde{C}_\tau \text{ is self-dual.} \tag{16}$$

In order to determine $\tilde{C}_\tau$ we need the following easy

Lemma 6 *$\tilde{C}_\tau$ has no codewords of weight 4, but codewords of weight 6.*

Proof. If $\tilde{C}_\tau$ has a codeword of weight 4, then C has a codeword of weight 8, which contradicts the fact that the minimum weight of the code C is 12 (see [7, p. 483]). Let $\mathbf{v}$ be the third row of $\hat{G}$. Since an 1×48 matrix $\mathbf{v} + \mathbf{v}\tau$ has property $(\{1\}, \mathbf{Q})$, where $\mathbf{Q}$ is the set of the orbits of τ on $\{\infty, 0, 1, \ldots, 46\}$. So by using Proposition 1 $\delta(\mathbf{v} + \mathbf{v}\tau)$ is a codeword of weight 6 in $\tilde{C}_\tau$. □

This lemma and (16) prove that $\tilde{C}_\tau$ is equivalent to Z_{24}, which is described in [11].

Remark. We see that the symmetry codes are good ones from a viewpoint of Lemma 5. The Mathematica [12] was used to compute various properties of the code in Example 2.

7. Concluding Remarks

We found that by modifying Pless' method (see the proof of Theorem 4 [10]) over a suitable principal ideal domain we can give a straightforward proof to the theorem. If we define contracted code for the code with an "orderly" automorphism group, then all results of this paper hold when

τ is replaced with an "orderly" automorphism group G which induces a semiregular permutation group on $\{1, \ldots, n\}$.

Acknowledgments I would like to thank the referee for his many suggestions that have helped to improve the paper.

References

[1] Assmus E.F. Jr. and Mattson H.F. Jr., *Contractions of self-orthogonal codes.* Discrete Math. **3** (1972), 21–32.

[2] Atsumi T., *An elementary proof of Yoshida's inequality for block designs which admit automorphism groups.* J. Math. Soc. Japan, **41** (1989), 301–310.

[3] Conway J.H. and Pless V., *On primes dividing the group order of a doubly-even* (72, 36, 16) *code and the group order of a quaternary* (24, 12, 10) *code.* Discrete Math. **38** (1982), 143–156.

[4] Conway J.H. and Pless V., *Monomials of orders* 7 *and* 11 *cannot be in the group of a* (24, 12, 10) *self-dual quaternary code.* IEEE Trans. Inform. Theory **29** (1983), 137–140.

[5] Higman D.G., *Combinatorial considerations about permutation groups.* Mathematical Institute, Oxford, 1972.

[6] Hughes D.R. and Piper F.C., *Design theory.* Cambridge University Press, Cambridge, 1985.

[7] MacWilliams F.J. and Sloane N.J.A., *The theory of error-correcting codes.* North-Holland, Amsterdam, 1977.

[8] Nagao H. and Tsushima Y., *Representations of Finite Groups.* Academic Press, New York, 1989.

[9] Pless V., *A classification of self-orthogonal codes over* GF(2). Discrete Math. **3** (1972). 209–246.

[10] Pless V., *Symmetry codes and their invariant subcodes.* J. Combin. Theory, Series A, **18** (1975), 116–125.

[11] Pless V. and Sloane N.J.A., *On the classification and enumeration of self-dual codes.* J. Combin. Theory, Series A, **18** (1975), 313–335.

[12] Wolfram S., *Mathematica.* Second Ed., Addison-Wesley, Reading MA, 1991.

[13] Yoshida T., *MacWilliams identity for linear codes with group action.* Kumamoto J. Math. **6** (1993), 29–45.

Department of Mathematics
Faculty of Science
Kagoshima University
Kagoshima 890, Japan
E-mail: atsumi@sci.kagoshima-u.ac.jp