AAECC 8, 71–83 (1997)

AAECC
Applicable Algebra in
Engineering, Communication
and Computing
© Springer-Verlag 1997

Dual Codes of Systematic Group Codes over Abelian Groups

A. A. Zain, B. Sundar Rajan

Department of Electrical Engineering, Indian Institute of Technology, Delhi, Hauz Khas, New Delhi 110016, India. email: bsrajan@ee.iitd.ernet.in

Received March 7, 1995; revised version April 3, 1996

Abstract. For systematic codes over finite fields the following result is well known: If $[I|P]$ is the generator matrix then the generator matrix of its dual code is $[-P^{tr}|I]$. The main result is a generalization of this for systematic group codes over finite abelian groups. It is shown that given the endomorphisms which characterize a group code over an abelian group, the endomorphisms which characterize its dual code are identified easily. The self-dual codes are also characterized. It is shown that there are self-dual and MDS group codes over elementary abelian groups which can not be obtained as linear codes over finite fields.

Keywords: Self-dual codes, Endomorphisms, Group codes, Dual codes.

I. Introduction

Study of codes over groups is motivated by the observation [7–9] that when more than two signals are used for transmission, a group structure, instead of the finite field structure traditionally assumed, for the alphabet is matched to the relevant distance measure. The Hamming distance properties of codes over groups have been studied in [5] and in [1] construction of group codes over abelian groups is given in terms of a 'parity check' matrix.

It is well known that binary linear codes are matched to binary signalling over an Additive White Gaussian Noise (AWGN) channel, in the sense that the squared Euclidean distance between two signal points in the signal space corresponding to two codewords is proportional to the Hamming distance between codewords. Similarly, linear codes over Z_M are matched to M-PSK modulation systems for an AWGN channel [11, 12]. The general problem of matching signal sets to linear codes over general algebraic structure of groups has been studied in [7–9]. Also, group codes constitute an important ingredient for the construction of Geometrically Uniform codes [4]. This motivates the study of codes over groups

Part of this correspondence was presented in 1994 International Symposium on Information Theory, Trondheim, Norway, June 1994 both abelian and nonabelian. In [1] construction of group codes over abelian groups that mimics the construction of algebraic codes over finite fields is considered and it is shown that the construction can be on the basis of a parity check matrix which provides the relevant information about the minimum Hamming distance of the code. The parity check symbols are seen as images of certain homomorphisms from G^k to G.

In this correspondence the dual code of a group code over an abelian group is characterized in terms of the endomorphisms of the abelian group. The study of dual codes is motivated by the fact that the weight distributions of the code and its dual are related for group codes over abelian groups [3]. It is shown that the endomorphisms of the dual code for a given code is related to the defining endomorphisms of the code, and in terms of appropriate matrix representations for the endomorphisms the relation is relatively simple. For the special case of codes over cyclic groups the characterization turns out to be straight forward, i.e., the endomorphisms defining the code and its dual are inverses in the group of endomorphisms. This special case actually corresponds to linear codes over residue class rings of integers. The necessary and sufficient conditions on the defining endomorphisms are obtained for the code to be self-dual.

In Sect. II the description of group codes in terms of endomorphisms is given. The characterization of dual codes is obtained in Sect. III. The special cases of group codes over cyclic groups and elementary abelian groups are discussed in Sect. IV. Section V deals with self-dual codes. Some concluding remarks and suggestions for further work are given in Section VI.

II. Group codes over abelian groups

Let G be a finite abelian group. The subgroups of G^n are called length n group codes. A group code isomorphic to G^k for some $k<n$, is called an information set supporting group code [1]. Information set supporting group codes are equivalent to systematic group codes. An instance of group codes that do not support an information set is where in none of the components all the elements of G appear. In this paper only information set supporting group codes are under consideration.

Definition 1. [1] A (n,k) systematic group code over an abelian group G is a subgroup of G^n with order $|G|^k$ described by $n-k$ homomorphisms ϕ_j, $j=1,2,\ldots,n-k$, of G^k onto G. Its codewords are $(x_1,\ldots,x_k,x_{k+1},\ldots,x_n)$, where

$$x_{k+j}=\phi_j(x_1,\ldots,x_k)=\bigoplus_{l=1}^{k}\phi_j(e,\ldots,e,x_l,e,\ldots,e) \tag{1}$$

with e and $\bigoplus$ denoting the identity element and the group operation of G, respectively.

In (1), the term $\phi_j(e,\ldots,e,x_l,e,\ldots,e)$ can be replaced by an endomorphism of G, say, $\psi_{l,j}$. With this notation the code is defined by the set of endomorphisms $\{\psi_{l,j}$, $l=1,2,\ldots,k$ and $j=1,2,\ldots,n-k\}$ and (1) can be rewritten as

$$x_{k+j}=\phi_j(x_1,\ldots,x_k)=\bigoplus_{l=1}^{k}\phi_j(e,\ldots,e,x_l,e,\ldots,e)=\bigoplus_{l=1}^{k}\psi_{l,j}(x_l). \tag{2}$$

The set of endomorphisms $\{\psi_{l,j}, l=1,2,\ldots,k; j=1,2,\ldots,n-k\}$ will be referred to as the defining endomorphisms of the code. The generator matrix Λ of the code can be written as $\Lambda=[I\,|\,\Psi]$, where

$$\Psi=\begin{bmatrix} \psi_{1,1} & \psi_{1,2} & \cdot & \cdot & \cdot & \psi_{1,n-k} \\ \psi_{2,1} & \psi_{2,2} & \cdot & \cdot & \cdot & \psi_{2,n-k} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \psi_{k,1} & \psi_{k,2} & \cdot & \cdot & \cdot & \psi_{k,n-k} \end{bmatrix}.$$

and $[x_1\,x_2\cdots x_n]=[x_1\,x_2\cdots x_k]\Lambda$. Ψ will be referred to as the *associated matrix* of the group code.

From the Normal Basis Theorem [6], any finite abelian group G can be written as the direct product of m cyclic groups given by $G\equiv C_{d_1}\otimes C_{d_2}\otimes\cdots\otimes C_{d_m}$, where C_d denotes a cyclic group of order d and $d_1|d_2|\cdots|d_m$. Let g_i denote the generator of C_{d_i}. Then an arbitrary element $x_\beta\in G$ can be written as

$$x_\beta=x_{\beta,1}g_1\oplus x_{\beta,2}g_2\oplus\cdots\oplus x_{\beta,m}g_m=\bigoplus_{h=1}^{m}x_{\beta,h}g_h,\, x_{\beta,i}\in Z_{d_i},\quad i=1,2,\ldots,m.$$

Any endomorphism of G can be uniquely specified by the images of the generators of the group under the endomorphism. Let ψ, an endomorphism of G, be defined by $\psi(g_i)=\bigoplus_{j=1}^{m}\alpha_{i,j}g_j$, $i=1,2,\ldots,m$. Then ψ can be specified by the *mxm* matrix

$$[\psi]=\begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \cdots & \alpha_{1,m} \\ \alpha_{2,1} & \alpha_{2,2} & \cdots & \alpha_{2,m} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \alpha_{m,1} & \alpha_{m,2} & \cdots & \alpha_{m,m} \end{bmatrix},\quad \alpha_{i,j}\in Z_{d_j},\tag{3}$$

and

$$\psi(x_\beta)=x_{\beta,1}\psi(g_1)\oplus x_{\beta,2}\psi(g_2)\oplus\cdots\oplus x_{\beta,m}\psi(g_m)=\bigoplus_{h=1}^{m}\left[\sum_{i=1}^{m}\{x_{\beta,i}\alpha_{i,h}\bmod d_h\}\right]g_h\tag{4}$$

The above expression gives the image of any element of G under any endomorphism of G. The matrix representation (3) can be rewritten as

$$\begin{bmatrix} a_{1,1} & \frac{d_2}{d_1}a_{1,2} & \frac{d_3}{d_1}a_{1,3} & \cdots & \frac{d_m}{d_1}a_{1,m} \\ a_{2,1} & a_{2,2} & \frac{d_3}{d_2}a_{2,3} & \cdots & \frac{d_m}{d_2}a_{2,m} \\ \cdot & \cdot & \cdot & \cdot & \\ \cdot & \cdot & \cdot & \cdot & \\ a_{m,1} & a_{m,2} & a_{m,3} & \cdots & a_{m,m} \end{bmatrix}\tag{5}$$

Table I. Matrix representations of all the endomorphisms of $C_2 \otimes C_4$

$\psi^{(1)} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$	$\psi^{(2)} = \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix}$	$\psi^{(3)} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$	$\psi^{(4)} = \begin{bmatrix} 0 & 0 \\ 0 & 3 \end{bmatrix}$	$\psi^{(5)} = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$	$\psi^{(6)} = \begin{bmatrix} 0 & 2 \\ 0 & 3 \end{bmatrix}$	$\psi^{(7)} = \begin{bmatrix} 0 & 0 \\ 1 & 2 \end{bmatrix}$	$\psi^{(8)} = \begin{bmatrix} 0 & 2 \\ 0 & 2 \end{bmatrix}$
$\psi^{(9)} = \begin{bmatrix} 0 & 0 \\ 1 & 3 \end{bmatrix}$	$\psi^{(10)} = \begin{bmatrix} 0 & 2 \\ 0 & 1 \end{bmatrix}$	$\psi^{(11)} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$	$\psi^{(12)} = \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}$	$\psi^{(13)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\psi^{(14)} = \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix}$	$\psi^{(15)} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$	$\psi^{(16)} = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$
$\psi^{(17)} = \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}$	$\psi^{(18)} = \begin{bmatrix} 1 & 2 \\ 0 & 2 \end{bmatrix}$	$\psi^{(19)} = \begin{bmatrix} 1 & 0 \\ 1 & 3 \end{bmatrix}$	$\psi^{(20)} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$	$\psi^{(21)} = \begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix}$	$\psi^{(22)} = \begin{bmatrix} 0 & 2 \\ 1 & 3 \end{bmatrix}$	$\psi^{(23)} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$	$\psi^{(24)} = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$
$\psi^{(25)} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$	$\psi^{(26)} = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix}$	$\psi^{(27)} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$	$\psi^{(28)} = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$	$\psi^{(29)} = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}$	$\psi^{(30)} = \begin{bmatrix} 0 & 2 \\ 1 & 2 \end{bmatrix}$	$\psi^{(31)} = \begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix}$	$\psi^{(32)} = \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}$

where

$$\alpha_{i,j} = \frac{d_j}{d_i} a_{i,j} \text{ if } j > i,$$
$$= a_{i,j} \text{ otherwise.}$$

It can be seen that $a_{i,j} \in Z_{\min\{d_i,d_j\}}$, the ring of integers modulo min $\{d_i, d_j\}$. The matrix representation in eq. (5) is called the canonical matrix representation of ψ [1].

The following definition of dual endomorphism will be used to characterize the dual code pairs in the next section.

Definition 2. Given an endomorphism ψ whose canonical matrix representation is (5), the endomorphism with the canonical matrix representation

$$\begin{bmatrix} b_{1,1} & \frac{d_2}{d_1} b_{1,2} & \frac{d_3}{d_1} b_{1,3} & \cdots & \frac{d_m}{d_1} b_{1,m} \\ b_{2,1} & b_{2,2} & \frac{d_3}{d_2} b_{2,3} & \cdots & \frac{d_m}{d_2} b_{2,m} \\ \cdot & \cdot & \cdot & \cdot & \\ \cdot & \cdot & \cdot & \cdot & \\ b_{m,1} & b_{m,2} & b_{m,3} & \cdots & b_{m,m} \end{bmatrix}, \quad b_{i,j} \in Z_{\min\{d_i,d_j\}},$$

is called the dual of ψ, denoted by ψ^d, where $b_{i,j} = -a_{j,i}$ in $Z_{\min\{d_i,d_j\}}$. If $\psi = \psi^d$, then it is called a self-dual endomorphism.

Example 1. Let $G = C_2 \otimes C_4$. There are 32 endomorphisms of G. Let these endomorphisms be denoted by $\psi^{(i)}$, $i = 1, 2, \ldots, 32$. The matrix representations of all these endomorphisms are listed in Table I. It is seen from Table I that the eight endomorphisms $\psi^{(i)}$, $i = 25, 26, \ldots, 32$ are self-dual endomorphisms. The rest have been listed as pairs is, $\psi^{(i)}$, $\psi^{(i+1)}$, $i = 1, 3, \ldots, 23$, where each pair is a dual pair corresponding to dual endomorphisms.

III. Dual Codes

The group of characters of G can be used to define the dual code of a group code over an abelian group as given in Definition 3. The group of canonical characters [15] is isomorphic to the group G, and hence the characters can be indexed by the elements of G in accordance with the isomorphism.

Definition 3. [3] Let C be a (n, k) group code over G. The dual code denoted by C^d is defined as

$$C^d = \left\{ \underline{y} = (y_1, y_2, \ldots, y_n) \in G^n / \langle \underline{y}, \underline{x} \rangle = \prod_{i=1}^{n} \eta_{x_i}(y_i) = e^*, \quad \forall\, \underline{x} = (x_1, \ldots, x_n) \in C \right\}$$

where η_g denotes the character of G corresponding to $g \in G$, and e^* is the identity element of the group of nth roots of unity (range for the characters) in an appropriate field.

Let $\lambda_h = \lambda_m^{\left(\frac{d_m}{d_h}\right)}$, where λ_m is any primitive d_m-th root of unity, $h = 1, 2, \ldots, m$, in an appropriate field and the characters be defined by $\eta_{x_i}(g_h) = \lambda_h^{x_{i,h}}$ for $h = 1, 2, \ldots, m$. Then,

$$\eta_{x_i}(x_\beta) = \prod_{h=1}^{m} \lambda_h^{x_{i,h} x_{\beta,h}}, \quad \text{for } x_\beta = \bigoplus_{h=1}^{m} x_{\beta,h} g_h \in G. \tag{6}$$

For later use, we need the following:

$$\eta_{x_i}(\psi(x_\beta)) = \prod_{h=1}^{m} \lambda_h^{\sum_{l=1}^{m} \{x_{\beta,l}\alpha_{l,h} \operatorname{mod}(d_h)\} x_{i,h}} \tag{7}$$

$$= \prod_{h=1}^{m} \lambda_h^{\sum_{l=1}^{m} \{x_{\beta,l}\alpha_{l,h}\} x_{i,h}}$$

$$= \lambda_m^{\sum_{h=1}^{m} \left(\frac{d_m}{d_h}\right)\left[\sum_{l=1}^{m} \{x_{\beta,l}\alpha_{l,h}\} x_{i,h}\right]}$$

Lemma 1. For $\underline{x}, \underline{y} \in G^n$ where

$$\underline{x} = \left(x_1, x_2, \ldots, x_k, \bigoplus_{i=1}^{k} \psi_{i,k+1}(x_i), \bigoplus_{i=1}^{k} \psi_{i,k+2}(x_i), \ldots, \bigoplus_{i=1}^{k} \psi_{i,n}(x_i)\right)$$

and

$$\underline{y} = \left(\bigoplus_{i=1}^{n-k} \psi^*_{i,1}(y_{k+i}), \bigoplus_{i=1}^{n-k} \psi^*_{i,2}(y_{k+i}), \ldots, \bigoplus_{i=1}^{n-k} \psi^*_{i,k}(y_{k+i}), y_{k+1}, y_{k+2}, \ldots, y_n\right),$$

the inner product $\langle \underline{y}, \underline{x} \rangle$ is given by

$$\langle \underline{y}, \underline{x} \rangle = \left\{\prod_{i=1}^{k} \eta_{x_i}\left(\bigoplus_{j=1}^{k} \psi^*_{j,i}(y_{k+j})\right)\right\}\left\{\prod_{i=k+1}^{n} \eta_{y_i}\left(\bigoplus_{j=1}^{k} \psi_{j,i}(x_j)\right)\right\}.$$

Proof.

$$\langle \underline{y}, \underline{x} \rangle = \prod_{i=1}^{n} \eta_{x_i}(y_i)$$

$$= \left\{\prod_{i=1}^{k} \eta_{x_i}(y_i)\right\}\left\{\prod_{i=k+1}^{n} \eta_{y_i}(x_i)\right\}. \qquad \text{since } \eta_{x_i}(y_i) = \eta_{y_i}(x_i)$$

$$= \left\{\eta_{x_1}\left(\bigoplus_{j=1}^{n-k} \psi^*_{j,1}(y_{k+j})\right)\eta_{x_2}\left(\bigoplus_{j=1}^{n-k} \psi^*_{j,2}(y_{k+j})\right)\cdots\eta_{x_k}\left(\bigoplus_{j=1}^{n-k} \psi^*_{j,k}(y_{k+j})\right)\right\}$$

$$\left\{\eta_{y_{k+1}}\left(\bigoplus_{j=1}^{k} \psi_{j,k+1}(x_j)\right)\eta_{y_{k+2}}\left(\bigoplus_{j=1}^{k} \psi_{j,k+2}(x_j)\right)\cdots\eta_{y_n}\left(\bigoplus_{j=1}^{k} \psi_{j,n}(x_j)\right)\right\}$$

$$= \left\{\prod_{i=1}^{k} \eta_{x_i}\left(\bigoplus_{j=1}^{k} \psi^*_{j,i}(y_{k+j})\right)\right\}\left\{\prod_{i=k+1}^{n} \eta_{y_i}\left(\bigoplus_{j=1}^{k} \psi_{j,i}(x_j)\right)\right\}.$$

Q.E.D.

Theorem 1. Let C be an (n,k) systematic group code over G, defined by the endomorphisms $\psi_{i,j}$ $i=1,2,\ldots,k$, $j=1,2,\ldots,n-k$, with codewords $(x_1,\ldots,x_n)$ given by $x_{k+j}=\bigoplus_{i=1}^{k}\psi_{i,k+j}(x_i)$, $j=1,2,\ldots,n-k$. Then the dual code C^d is an $(n,n-k)$ systematic group code over G with codewords $(y_1,\ldots,y_n)$ given by $y_i=\bigoplus_{j=1}^{n-k}\psi^*_{j,i}(y_{k+j})$ $i=1,2,\ldots,k$, where

$$\psi^*_{i,j}=\psi^d_{j,i}. \tag{8}$$

In terms of generator matrices, if $[I\,|\,\Psi]$ is the generator matrix of C, then its dual has the generator matrix $[(\Psi^d)^{tr}|I]$, where $[\Psi^d]$ is the matrix obtained by replacing each entry of $[\Psi]$ by its dual.

Proof. The proof consists of verifying Definition 3 for the pair of codes given in the statement of the theorem by using Definition 2 of matrix representations of dual endomorphisms. This is carried out as follows:

Let the matrices representing the endomorphisms $\psi_{i,j}$ and $\psi^*_{i,j}$ respectively be $\alpha_{i,j}=[\alpha_{i,j}(l,h)]$, $l,h=1,2,\ldots,m$ and $\alpha^*_{i,j}=[\alpha^*_{i,j}(l,h)]$, $l,h=1,2,\ldots,m$ for $i=1,2,\ldots,n-k$ and $j=1,2,\ldots,k$. Let

$$\underline{x}=\left(x_1,x_2,\ldots,x_k,\bigoplus_{i=1}^{k}\psi_{i,k+1}(x_i),\bigoplus_{i=1}^{k}\psi_{i,k+2}(x_i),\ldots,\bigoplus_{i=1}^{k}\psi_{i,n}(x_i)\right)\in C,$$

and

$$\underline{y}=\left(\bigoplus_{i=1}^{n-k}\psi^*_{i,1}(y_{k+i}),\bigoplus_{i=1}^{n-k}\psi^*_{i,2}(y_{k+i}),\ldots,\bigoplus_{i=1}^{n-k}\psi^*_{i,k}(y_{k+i}),y_{k+1},y_{k+2},\ldots,y_n\right).$$

Then,

$$\langle\underline{y},\underline{x}\rangle=\prod_{i=1}^{n}\eta_{x_i}(y_i)=\left\{\prod_{i=1}^{k}\eta_{x_i}\left(\bigoplus_{j=1}^{n-k}\psi^*_{j,i}(y_{k+j})\right)\right\}\left\{\prod_{i=k+1}^{n}\eta_{y_i}\left(\bigoplus_{j=1}^{k}\psi_{j,i}(x_j)\right)\right\} \tag{9}$$

(using symmetry of characters w.r.t. both the arguments and lemma 1). Using (7),

$$\eta_{x_i}\left(\bigoplus_{j=1}^{n-k}\psi^*_{j,i}(y_{k+j})\right)=\lambda_m^{\sum_{j=1}^{n-k}\sum_{h=1}^{m}\left(\frac{d_m}{d_h}\right)\left[\sum_{l=1}^{m}\{y_{k+j,l}\alpha^*_{j,i}(l,h)\}x_{i,h}\right]}. \tag{10}$$

Using (10), the first term in (9) becomes

$$\lambda_m^{\sum_{i=1}^{k}\sum_{j=1}^{n-k}\sum_{h=1}^{m}\left(\frac{d_m}{d_h}\right)\left[\sum_{l=1}^{m}\{y_{k+j,l}\alpha^*_{j,i}(l,h)\}x_{i,h}\right]}=\lambda_m^{\sum_{i=1}^{k}\sum_{j=1}^{n-k}\sum_{h=1}^{m}\sum_{l=1}^{m}\left\{\left(\frac{d_m}{d_h}\right)y_{k+j,l}\alpha^*_{j,i}(l,h)x_{i,h}\right\}} \tag{11}$$

Similarly, the second term in (9) becomes

$$\lambda_m^{\sum_{i=k+1}^{n}\sum_{j=1}^{k}\sum_{h=1}^{m}\sum_{l=1}^{m}\left\{\left(\frac{d_m}{d_h}\right)x_{j,l}\alpha_{j,i}(l,h)y_{i,h}\right\}} \tag{12}$$

Substituting (11) and (12), with suitable substitutions for summation variables, in (9) gives

$$\langle \underline{y}, \underline{x} \rangle = \lambda_m^{\sum_{i=1}^{k} \sum_{j=1}^{n-k} \sum_{h=1}^{m} \sum_{l=1}^{m} \left\{ \left(\frac{d_m}{d_h}\right) y_{k+j,l} [\alpha^*_{j,i}(l,h) + \alpha_{j,i}(h,l)] x_{i,h} \right\}} = e^*,$$

since the term inside the square bracket is always zero, which follows from (8) and the definition of dual endomorphisms.

We have shown that there are $|G|^{n-k}$ codewords in C^d. It remains to show that C^d has only these $|G|^{n-k}$ codewords. It is shown in [3, Theorem 1] that C^d has $|G|^{n-k}$ codewords. *Q.E.D.*

Theorem 1 generalizes the result available for linear codes over finite fields: If $[I|P]$ is the generator matrix then the generator matrix of its dual code is $[-P^{tr}|I]$. Note that the minus sign appearing in the generator matrix of the dual code in the finite field case is due to the codes being a special case. A similar statement is possible for the special case of group codes over cyclic groups. A similar statement in not possible for elementary abelian group codes in general though this class includes linear codes over finite fields as a proper subclass. We discuss these special cases in the next section.

Example 2. Let $G = C_2 \otimes C_4$, and L_1 be the (3, 1) code defined by $\psi_{11} = \psi^{(23)}$ and $\psi_{21} = \psi^{(22)}$ (refer to Table I) and given by

$$\psi_{11} = \psi^{(23)} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \quad \text{and} \quad \psi_{21} = \psi^{(22)} = \begin{bmatrix} 0 & 2 \\ 1 & 3 \end{bmatrix}.$$

Then,

$$\psi^*_{11} = \psi^d_{11} = \psi^{(24)} = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \quad \text{and} \quad \psi^*_{12} = \psi^d_{21} = \psi^{(21)} = \begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix}.$$

The generator matrix of L_1 is

$$\begin{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} & \begin{bmatrix} 0 & 2 \\ 1 & 3 \end{bmatrix} \end{bmatrix},$$

and the generator matrix of L_1^d is

$$\begin{bmatrix} \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} & \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \\ \begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix} & \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} & \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{bmatrix}$$

The code L_1^d is the (3, 2) code given by $(\psi^*_{11}(y_1)\psi^*_{12}(y_2), y_1, y_2)$ $\forall\, y_1, y_2 \in G$, and the codewords of L_1 are given by $(x, \psi_{11}(x), \psi_{21}(x))$, $\forall\, x \in G$. The complete listing of all the codewords of L_1 and L_1^d is given in Table II. The following notation has been used in the listing. $C_2 = \{0, 1\}$; $C_4 = \{0, 1, 2, 3\}$ and $G = \{00, 10, 01, 11, 02, 12, 03, 13\}$. Each element, say ab, is represented by $a + 2b$.

Table II. Codewords of L_1 over $C_2 \otimes C_4$ and its dual code

Codewords of L_1	Codewords of L_1^d							
000	000	401	302	703	404	005	706	307
154	510	111	612	213	114	515	216	617
237	720	321	022	423	324	725	426	027
363	230	631	532	133	634	235	136	537
444	440	041	742	343	044	445	346	747
510	150	551	252	653	554	155	656	257
673	360	761	462	063	764	365	066	467
727	670	271	172	573	274	675	576	177

IV. Special cases

1. Codes over cyclic groups

When G is cyclic of order M, say, $\{1 = g^0, g, g^2, \ldots, g^{M-1}\}$, the set of endomorphisms of G form a cyclic group isomorphic to G. Explicitly, the endomorphisms are given by

$$\psi^{(i)}(g) = g^i, \quad i = 0, 1, \ldots, M-1.$$

The matrix (1×1) representations of these endomorphisms are nothing but elements of $Z_M = \{0, 1, \ldots, M-1\}$. Therefore the dual endomorphism of an endomorphism is its additive inverse in Z_M. So, in this case, $[I \mid \Psi]$ is the generator matrix of a group code then the generator matrix of its dual code is $[-\Psi^{tr} \mid I]$: a straight forward generalization of the finite field case. This is illustrated in Example 3 for codes over C_6.

Example 3. Let $G = C_6 = \{0, 1, 2, 3, 4, 5\}$ with addition modulo 6 as the group operation. There are six endomorphisms of G, described by their images of the generator as $0, 1, 2, 3, 4$, and 5. The (4, 2) codes are described by four endomorphisms. There are $6^4 = 1296$ codes each described by four endomorphisms. The code defined by the endomorphisms which map the generator to $1, 2, 3$ and 4 respectively, i.e.,

$$\psi_{11} = \psi^{(1)}; \psi_{12} = \psi^{(2)}; \psi_{21} = \psi^{(3)}; \quad \text{and} \quad \psi_{22} = \psi^{(4)}$$

referred as L_2, has dual code defined by the endomorphisms which map the generator respectively to $5, 3, 4$ and 2, i.e.,

$$\psi_{11}^* = \psi^{(5)}; \psi_{12}^* = \psi^{(3)}; \psi_{21}^* = \psi^{(4)}; \quad \text{and} \quad \psi_{22}^* = \psi^{(2)}.$$

The generator matrices of L_2 and L_2^d are respectively

$$\begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 3 & 4 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 5 & 3 & 1 & 0 \\ 4 & 2 & 0 & 1 \end{bmatrix}.$$

Since every group code over a cyclic group with M elements can be seen as a linear code over Z_M, the residue class ring of integers modulo M, this special case actually deals with linear codes over Z_M. For the class of linear cyclic codes over Z_M,

Table III. Codewords of a (4, 2, 3) MDS group code over C_2^2 corresponding to Example 4

(00 00 00 00)	(10 00 11 11)	(01 00 01 01)	(11 00 10 10)
(00 10 11 01)	(10 10 00 10)	(01 10 10 00)	(11 10 01 11)
(00 01 01 10)	(10 01 10 01)	(01 01 00 11)	(11 01 11 00)
(00 11 10 11)	(10 11 01 00)	(01 11 11 10)	(11 11 00 01)

the dual code pairs and self-dual codes have been discussed in [14] using the discrete Fourier transform over Galois rings.

2. *Codes over elementary abelian groups*

An important special case is the class of group codes over elementary abelian groups $G \equiv C_p^m = C_p \otimes C_p \otimes \cdots \otimes C_p$ (direct product of m cyclic groups of order p each). These being the additive groups of finite fields include as a proper subclass the linear codes over finite fields $GF(p^m)$. The endomorphism ring of C_p^m is a matrix ring consisting mxm matrices over $GF(p)$. The structure of this matrix ring is well studied [13]. Moreover, it is easily seen that the matrices in (3) and (5) are identical, since in this case $d_1 = d_2 = \cdots d_m = p$. Group codes over C_p^m play an important role when Maximum Distance Separable (MDS) codes are considered [5]. There are MDS group codes over C_p^m which cannot be obtained as conventional linear codes over $GF(p^m)$. This is exemplified by Example 4 discussed below.

Example 4. Consider the (4, 2) code over $C_2^2 = \{00, 10, 01, 11\}$, defined by the generator matrix

$$\begin{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} & \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \\ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} & \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \end{bmatrix}$$

The codewords of this code are given in Table III, from which it is easy to check that it is a MDS code. The generator matrix of the dual code of this code is, by Theorem 1,

$$\begin{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \\ \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} & \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} & \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{bmatrix}.$$

V. Self-Dual Codes

Self-dual codes and certain types of lattice sphere packings are closely related [2]. A new construction of the Nordstrom-Robinson code as the union of the binary images of two isomorphic linear (4, 2, 3) codes over $GF(4)$ has been reported recently [16]. The (4, 2, 3) code used in this construction is both self-dual and MDS which is a unique code over $GF(4)$. We show that for the same parameters several self-dual group codes over C_2^2 exist which are also MDS.

As given in Definition 1, an (n,k) group code over G is defined by $n-k$ homomorphisms $\phi_l, l=1,2,\ldots,n-k$, from G^k onto G. For self-dual codes $n-k=k$ and it is convenient to define the homomorphism Φ from G^k to G^k corresponding to ϕ_l, $l=1,2,\ldots,k$, as follows:

$$\Phi(x_1,x_2,\ldots,x_k)=(\phi_1(x_1,x_2,\ldots,x_k),\phi_2(x_1,x_2,\ldots,x_k),\ldots,\phi_k(x_1,x_2,\ldots,x_k))$$

where $x_i \in G$, $i=1,2,\ldots,k$. In terms of Φ the codewords of an $(2k,k)$ code can be written as

$$(\underline{x},\Phi(\underline{x})) \text{ where } \underline{x}=(x_1,x_2,\ldots,x_k),\ \Phi(\underline{x})=(x_{k+1},x_{k+2},\ldots,x_{2k})\in G^k.$$

It is easy to see that the homomorphism Φ is represented by the associated matrix Ψ.

Theorem 2. Let C be a $(2k,k)$ group code over G defined by $\Phi: G^k \to G^k$ or the associated matrix Ψ. Then C is self-dual iff $\Psi(\Psi^d)^{tr}=I$, the identity map.

Proof. Let $\underline{a}=(\underline{x},\Phi(\underline{x}))\in C$, $\underline{x}\in G^k$, and C^d denote its dual code. From Theorem 1, any codeword in C^d is of the form $\underline{b}=(\Phi^d(\underline{y}),\underline{y})$ where $\underline{y}\in G^k$.

Suppose C is self-dual. Then, the set of first k symbols of all the codewords and the set of last k symbols of all the codewords both form information sets. In other words Φ is an automorphism of G^k. Any codeword $\underline{a}=(\underline{x},\Phi(\underline{x}))\in C$ can also be written as $\underline{a}=(\Phi^d(\Phi(\underline{x})),\Phi(\underline{x}))$. Therefore $\Phi^d\Phi(\underline{x})=\underline{x}$ and similarly starting from $\underline{b}$ one gets $\Phi\Phi^d(\underline{x})=\underline{x}$.

Conversely, let $\Phi\Phi^d(\underline{x})=\Phi^d\Phi(\underline{x})=\underline{x}, \forall\, \underline{x}\in G^k$. For $\underline{a}=(\underline{x},\Phi(\underline{x}))\in C$, any $2k$ tuple which is orthogonal to $\underline{a}$ is of the form $(\Phi^d(\underline{z}),\underline{z})$, where $\underline{z}\in G^k$, from Theorem 1. Since $\Phi\Phi^d(\underline{x})=\Phi^d\Phi(\underline{x})=\underline{x}, \forall\, \underline{x}\in G^k$, Φ is a invertible mapping and let $z=\Phi(\underline{x})$. Then

$$(\Phi^d(\underline{z}),\underline{z})=(\Phi^d(\Phi(\underline{x})),\Phi(\underline{x}))=(\underline{x},\Phi(\underline{x})).$$

Therefore $(\underline{x},\Phi(\underline{x}))$ is in C^d also. By similar argument it follows that any vector in C^d is also in C. So, in terms of Φ, the condition for self-duality is $\Phi\Phi^d=I$, which, in terms of the associated matrix is same as $\Psi(\Psi^d)^{tr}=I$. *Q.E.D.*

Example 5. Consider the case of $(4,2)$ codes over $G=C_2^2=\{00, 01, 10, 11\}$. Each code is defined by four endomorphisms of G. Each endomorphism is represented by a 2x2 matrix over Z_2. Consider the code defined by the following matrices.

$$\psi_{11}=\begin{bmatrix}1&1\\0&1\end{bmatrix};\quad \psi_{12}=\begin{bmatrix}0&1\\1&1\end{bmatrix};\quad \psi_{21}=\begin{bmatrix}1&1\\1&0\end{bmatrix};\quad \psi_{22}=\begin{bmatrix}1&0\\1&1\end{bmatrix}.$$

We have

$$\Psi=\begin{bmatrix}\begin{bmatrix}1&1\\0&1\end{bmatrix}&\begin{bmatrix}0&1\\1&1\end{bmatrix}\\ \begin{bmatrix}1&1\\1&0\end{bmatrix}&\begin{bmatrix}1&0\\1&1\end{bmatrix}\end{bmatrix}$$

Table IV. Associated matrices of (4, 2) self-dual, MDS codes over C_2^2

$\psi^{(1)} = \begin{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \\ \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} & \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \end{bmatrix}$	$\psi^{(2)} = \begin{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \\ \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \end{bmatrix}$	$\psi^{(3)} = \begin{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \\ \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} & \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \end{bmatrix}$
$\psi^{(4)} = \begin{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \\ \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} & \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \end{bmatrix}$	$\psi^{(5)} = \begin{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \\ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \end{bmatrix}$	$\psi^{(6)} = \begin{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} & \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \\ \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \end{bmatrix}$

It is easy to check that $\Psi(\Psi^d)^{tr} = I$. The codewords of this self-dual code are

{(00 00 00 00), (00 10 01 11), (00 01 11 01), (00 11 10 10), (10 00 10 11), (10 10 11 00), (10 01 01 10), (10 11 00 01), (01 00 11 10), (01 10 10 01), (01 01 00 11), (01 11 01 00), (11 00 01 01), (11 10 00 10), (11 01 10 00), (11 11 11 11)}

Note that the code of Example 5 is MDS also. Moreover, the binary image of the code of Example 5 is equivalent to the extended (8, 4, 4) Hamming code.

Using the well known result [10] on the number of linear self-dual codes over finite fields, there are only five (4, 2) self-dual linear codes over $GF(4)$, and among them there is only one which is MDS. By computer search it was seen that there are 34 self-dual (4, 2) codes over C_2^2, among which 6 are MDS. The associated matrices of the self-dual codes which are MDS also are listed in Table IV. Note that $\psi^{(1)}$ and $\psi^{(2)}$ are permutation equivalent, i.e., by permuting the last two columns of codewords one changes to other. Similarly, the pair $\psi^{(4)}$ and $\psi^{(6)}$ are permutation equivalent. So, upto permutation equivalence there are 4 MDS self-dual (4, 2, 3) codes over C_2^2. The code given by $\Psi^{(4)}$, in this table corresponds to the unique self-dual MDS code over $GF(4)$.

VI. Discussion

The class of self-dual codes and dual code pairs of group codes over finite abelian groups have been characterized. This characterization subsumes as special cases the class of linear codes over residue class integer rings and the conventional linear codes over finite fields. It is hoped that the techniques of this correspondence will suggest ways for algebraic characterization of dual codes over nonabelian groups. It will be of greater interest to explore whether the duality of codes over groups gives rise to a relation between Euclidean distance properties of dual code pairs when appropriately matched signal sets are considered.

Acknowledgements. The authors gratefully acknowledge Prof. E. Biglieri for sending his preprints and thank the referees for their suggestions which helped to improve the clarity of the paper and pointing out a crucial omission in the proof of Theorem 1.

References

1. Biglieri E., Elia M.: Construction of linear block codes over groups. IEEE International Symposium on Information Theory, San Antonio, Texas, 1993
2. Conway J. H., Sloane N. J. A.: Sphere Packings, Lattices and Groups. Springer Berlin, Heidelberg New York 1988
3. Delsarte P.: Bounds for unrestricted codes by linear programming. Philips Research Dev. J., **27**, 272–289 (1972)
4. Forney G. D.: Geometrically Uniform Codes. IEEE Transactions on Information Theory, Vol. IT-37, **5**, 1241–1260 (1991)
5. Forney G. D. Jr.: On the Hamming distance property of group codes. IEEE Trans. Information Theory, Vol.IT-38, **6**, 1797–1801 (1992)
6. Hall M., Jr.: The Theory of Groups. MacMillan 1964
7. Loeliger H. A., Mittelholzer T.: Linear codes over groups and new Slepian-type signal sets. Proc. 1991 IEEE International Symposium on Information Theory, Budapest, Hungary, June 24–28 (1991)
8. Loeliger H. A.: On Euclidean Space Group Codes, Ph.D. Dissertation, Swiss Federal Institute of Technology, Zurich, Switzerland (1992)
9. Loeliger H. A.: Signal sets matched to groups. IEEE Trans. Information Theory, Vol.IT-37, **6**, 1675–1682 (1991)
10. MacWilliams F. J., Sloane N. J. A.: The Theory of Error Correcting Codes, North-Holland (1977)
11. Massey J. L., Mittelholzer T.: Systematicity and rotational invariance of convolutional codes over rings, Proc. 2nd Int. Workshop on Algebraic and Combinatorial Coding Theory, Leningrad Russia, Sept. 16–22 (1990)
12. Massey J. L., Mittelholzer T., Riedel T., Vollenweider M.: Ring Convolutional codes for Phase Modulation, Int. Symp. Inform. Theory, San Diego, CA, Jan. 14–19 (1990).
13. McDonald B. R.: Finite rings with identity, Marcel Dekker, New York (1974)
14. Sundar Rajan B., Siddiqi M. U.: Transform domain characterization of cyclic codes over Z_m. AAECC 5(5), 261–275 (1994)
15. Van der Warden: Modern Algebra II, Fredrick Ungar, New York
16. Vardy A.: The Nordstrom-Robinson Code: Representation over $GF(4)$ and Efficient Decoding. IEEE Trans. IT, 48(5) 1686–1693 (1994)