Science and Technology, 8 (2003) 145-151

On Group Codes Over Elementary Abelian Groups

Adnan A. Zain

Department of Electronics and Communications Engineering, Faculty of Engineering, University of Aden, P.O.Box 7409, Almansoora City, Aden Governorate, Republic of Yemen, Email: aazain@gmx.de.

حول أنظمة التشفير المزمرة بواسطة زمر(Abel) الابتدائية

عدنان عبدالله زين

خلاصة : تقدم الورقة تعريفا لكل من مصفوفة التوليد و مصفوفة فحص التكافؤ لأنظمة التشفير المزمرة بواسطة الزمر الابتدائية من نوع (Abel) , وهذه المصفوفات عناصرها تنتمي إلى الحلقات المتبلورة للزمرة. باستخدام ذلك تم, في هذا البحث, تطوير النظرية التي تعطي العلاقة بين مصفوفة التوليد و مصفوفة فحص التكافؤ لأنظمة التشفير الخطية بواسطة الحقول المتناهية إلى نظرية جديدة لأنظمة التشفير المزمرة بواسطة الزمر الابتدائية من نوع (Abel). يعرض البحث شفرات جديدة تمتلك خواص جيدة مثل: أعلى قيمة للمسافة (Hamming) وقابلية الانفصال, ذاتية الازدواجية, والخاصية الحلقية.

ABSTRACT: For group codes over elementary Abelian groups we present definitions of the generator and the parity check matrices, which are matrices over the ring of endomorphism of the group. We also lift the theorem that relates the parity check and the generator matrices of linear codes over finite fields to group codes over elementary Abelian groups. Some new codes that are MDS, self-dual, and cyclic over the Abelian group with four elements are given.

KEYWORDS: Codes Over Groups, Elementary Abelian Groups, Endomorphism Rings.

1. Introduction

A group code C of length n over an Abelian group A is a subgroup of A^n, the n-fold direct product of A. The rate $k(C)$ is defined by $k(C) = \log_{|A|}|C|$, where $|X|$ stands for cardinality. A group code C of length n with rate k and minimum Hamming distance d_H is called a $[n,k,d_H]$ code. A linear code C over a field F is also a group code over the additive group of F. It has been shown by Forney and Trott (1993) that many of the important structural properties of codes over F are associated with the additive and not the multiplicative group properties of F. For an information set supporting group codes (Forney, 1992) i.e. for group codes that are equivalent to systematic group codes over Abelian groups, the notion of generator and check matrices was introduced in Biglieri and Elia (1993). In this paper, following Biglieri and Elia (1993), we present the formal definitions of a generator and parity check matrices over the endomorphism ring of the elementary Abelian groups. Based on this we generalize the well known theorem that relates the generator and parity check matrices of linear codes over fields to group codes over elementary Abelian groups. Some new codes, MDS, Self-Dual, and Cyclic over the Abelian group with four elements, which cannot be obtained as linear codes over fields, are presented.

The paper is organized as follows. Section 2 contains the mathematical preliminaries. In section 3 the main theorem of the paper is proved. Table 2 contains the generator matrices and the listing of the code words of the new codes.

2. Preliminaries

An elementary abelian group, denoted by A_{p^m}, of order $q = p^m$, where p is a prime, is isomorphic to the direct sum of m cyclic groups, C_p, of order p, written as $A_{p^m} \equiv C_p \oplus \ldots \oplus C_p$ $(m-\text{times})$. Let g_i be a generator for the i^{th} cyclic group. An arbitrary element $x_\beta \in A_{p^m}$ can be written as

$$x_\beta = \bigoplus_{h=1}^{m} x_{\beta,h} g_h, \quad x_{\beta,i} \in Z_p, \quad i = 1,2,\ldots,m. \tag{1}$$

Let $\psi : A_{p^m} \to A_{p^m}$ be an endomorphism of the group A_{p^m} defined by the following

$$\psi(g_i) = \bigoplus_{j=1}^{m} \alpha_{i,j} g_j \text{ , } \alpha_{i,j} \in Z_p \text{ , } i = 1,2,\ldots,m. \tag{2}$$

Then ψ can be specified by the following $m \times m$ matrix over $Z_p \equiv GF(p)$

$$[\psi] = \begin{bmatrix} \alpha_{1,1} \ \alpha_{1,2} \ldots \alpha_{1,m} \\ \alpha_{2,1} \ \alpha_{2,2} \ldots \alpha_{2,m} \\ \vdots \quad \vdots \quad \vdots \\ \alpha_{m,1} \ \alpha_{m,2} \ldots \alpha_{m,m} \end{bmatrix} \tag{3}$$

The action of ψ on any element $x_\beta \in A_{p^m}$, is given by the following expression

$$\psi(x_\beta) = x_{\beta,1}\psi(g_1) \oplus \ldots \oplus x_{\beta,m}\psi(g_m) = \bigoplus_{h=1}^{m}[\sum_{i=1}^{m}\{x_{\beta,i}\alpha_{i,h} \text{ mod } p\}]g_h \tag{4}$$

The endomorphism ring of A_{p^m} denoted by $End(A_{p^m})$ is isomorphic to the matrix ring $M_m(Z_p)$ consisting of $m \times m$ matrices over a finite field with p elements denoted by $GF(p)$ (McDonald, 1974).

Example 1: Consider the group $A_{2^2} \equiv C_2 \oplus C_2$. $End(A_{2^2}) \equiv M_2(Z_2)$.

$$M_2(Z_2) = \left\{ \begin{bmatrix} 0\,0 \\ 0\,0 \end{bmatrix}, \begin{bmatrix} 1\,0 \\ 0\,0 \end{bmatrix}, \begin{bmatrix} 0\,1 \\ 0\,0 \end{bmatrix}, \begin{bmatrix} 0\,0 \\ 1\,0 \end{bmatrix}, \begin{bmatrix} 0\,0 \\ 0\,1 \end{bmatrix}, \begin{bmatrix} 1\,1 \\ 0\,0 \end{bmatrix}, \begin{bmatrix} 1\,0 \\ 1\,0 \end{bmatrix}, \begin{bmatrix} 1\,0 \\ 0\,1 \end{bmatrix}, \begin{bmatrix} 0\,1 \\ 1\,0 \end{bmatrix}, \begin{bmatrix} 0\,1 \\ 0\,1 \end{bmatrix}, \begin{bmatrix} 0\,0 \\ 1\,1 \end{bmatrix}, \begin{bmatrix} 1\,1 \\ 1\,0 \end{bmatrix}, \begin{bmatrix} 1\,1 \\ 0\,1 \end{bmatrix}, \begin{bmatrix} 0\,1 \\ 1\,1 \end{bmatrix}, \begin{bmatrix} 1\,0 \\ 1\,1 \end{bmatrix}, \begin{bmatrix} 1\,1 \\ 1\,1 \end{bmatrix} \right\}$$

$$GL_2(Z_2) = \left\{ \begin{bmatrix} 10 \\ 01 \end{bmatrix}, \begin{bmatrix} 01 \\ 10 \end{bmatrix}, \begin{bmatrix} 11 \\ 10 \end{bmatrix}, \begin{bmatrix} 01 \\ 11 \end{bmatrix}, \begin{bmatrix} 10 \\ 11 \end{bmatrix}, \begin{bmatrix} 11 \\ 01 \end{bmatrix} \right\}$$

$$F_{2^2} = \left\{ \begin{bmatrix} 00 \\ 00 \end{bmatrix}, \begin{bmatrix} 10 \\ 01 \end{bmatrix}, \begin{bmatrix} 01 \\ 11 \end{bmatrix}, \begin{bmatrix} 11 \\ 10 \end{bmatrix} \right\} \equiv GF(2^2)$$

The set $M_2(Z_2)$, the set of endomorphisms, contains as a proper subset the set $GL_2(Z_2)$, the set of automorphisms, which contains a proper subset of the set F_{2^2} that is isomorphic to the finite field with four elements, $GF(4)$. The action of every endomorphism on the group elements is shown in Table 1, where the first column contains the elements of the group against which are the images under the action of the underlying endomorphism.

Table 1. List of $End(A_{2^2}) \equiv M_2(Z_2)$ and Their actions on the group elements.

	$\begin{bmatrix}00\\00\end{bmatrix}$	$\begin{bmatrix}10\\00\end{bmatrix}$	$\begin{bmatrix}01\\00\end{bmatrix}$	$\begin{bmatrix}00\\10\end{bmatrix}$	$\begin{bmatrix}00\\01\end{bmatrix}$	$\begin{bmatrix}11\\00\end{bmatrix}$	$\begin{bmatrix}10\\10\end{bmatrix}$	$\begin{bmatrix}10\\01\end{bmatrix}$	$\begin{bmatrix}01\\10\end{bmatrix}$	$\begin{bmatrix}01\\01\end{bmatrix}$	$\begin{bmatrix}00\\11\end{bmatrix}$	$\begin{bmatrix}01\\11\end{bmatrix}$	$\begin{bmatrix}10\\11\end{bmatrix}$	$\begin{bmatrix}11\\01\end{bmatrix}$	$\begin{bmatrix}11\\10\end{bmatrix}$	$\begin{bmatrix}11\\11\end{bmatrix}$
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
10	00	10	01	00	00	11	10	10	01	01	00	01	10	11	11	11
01	00	00	00	10	01	00	10	01	10	01	11	11	11	01	10	11
11	00	10	01	10	01	11	00	11	11	00	11	10	01	10	01	00

3. (n,k) Group Codes

A block of k message symbols $u = u_1 u_2 \ldots u_k$, where $u_i \in A_{p^m}$,$i = 1,2,\ldots,k$, will be encoded into a codeword $x = x_1 x_2 \ldots x_n$, $x_j \in A_{p^m}$, where $n \geq k$, and these code words form a code. The first part of the codeword consists of the message itself: $x_1 = u_1, x_2 = u_2, \ldots, x_k = u_k$, followed by $n-k$ check symbols $x_{k+1}, \ldots, x_n$.

Following the definition of systematic group codes presented by Biglieri and Elia (1993), the check symbols can be obtained as

$$x_{k+l} = \bigoplus_{i=1}^{k} \psi_{il}(x_i), \quad l = 1,2,\ldots,(n-k). \tag{5}$$

In matrix notation the above can be written as

$$x = u\Psi \tag{6}$$

where Ψ is the *generator matrix* of the code given by

$$\Psi = \begin{bmatrix} \psi_I \ \psi_0 \cdots \psi_0 \,|\, \psi_{11} \ \psi_{12} \cdots \psi_{1s} \\ \psi_0 \ \psi_I \cdots \psi_0 \,|\, \psi_{21} \ \psi_{22} \cdots \psi_{2s} \\ \vdots \quad \vdots \qquad \vdots \ |\, \vdots \quad \vdots \qquad \vdots \\ \psi_0 \ \psi_0 \cdots \psi_I \,|\, \psi_{k1} \ \psi_{k2} \cdots \psi_{ks} \end{bmatrix} \tag{7}$$

and ψ_I is the identity endomorphism that maps every element in the group onto itself while ψ_0 is the zero endomorphism that maps every element on to the identity element of the group e.
The $(n-k) \times n$ *parity check* matrix H for the code can be obtained as follows

$$\mathrm{H}\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \mathrm{H}x^{tr} = \begin{bmatrix} e \\ e \\ \vdots \\ e \end{bmatrix} \tag{8}$$

$$\mathrm{H} = \begin{bmatrix} \psi_{11} \ \psi_{21} \cdots \psi_{k1} \,|\, \psi_{inv} \ \psi_0 \cdots \psi_0 \\ \psi_{12} \ \psi_{22} \cdots \psi_{k2} \ \ \psi_0 \ \psi_{inv} \cdots \psi_0 \\ \vdots \quad \vdots \quad \ldots \vdots \ \ |\, \vdots \quad \vdots \quad \ldots \ \vdots \\ \psi_{1s} \ \psi_{2s} \cdots \psi_{ks} \,|\, \psi_0 \ \psi_0 \ \cdots \psi_{inv} \end{bmatrix} \tag{9}$$

where ψ_{inv} is the endomorphism that maps every element on to its inverse. (This parity check matrix is different from the parity check matrix in Biglieri and Elia (1993)).

Now we are in a position to generalize the well-known result that relates the generator matrix and the parity check matrix for a (n,k) linear code over finite fields.

Theorem 1*:* For (n,k) codes over an elementary Abelian group A_{p^m} the generator matrix Ψ and the parity check matrix H are related by $\Psi \circ H^{tr} = H \circ \Psi^{tr} = [O_{k\times s}]$, where $[O_{k\times s}]$ is the matrix with all entries equal to ψ_0 i.e. the zero endomorphism, and $\circ$ denotes a composition of endomorphisms.

Proof: From equation (8) that defines H, we have

$$\mathrm{H}\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \mathrm{H}x^{tr} = \begin{bmatrix} e \\ e \\ \vdots \\ e \end{bmatrix} = [e]_{s\times 1}$$

Use equation (6) to substitute for x^{tr} in the above to obtain

$$H \circ \Psi^{tr} u^{tr} = [e]_{s\times 1}$$

Using (7) and (9) in the above matrix equation, we obtain

$$\begin{bmatrix} \psi_{11}\ \psi_{21} \cdots \psi_{k1} \,|\, \psi_{inv}\ \psi_0 \cdots \psi_0 \\ \psi_{12}\ \psi_{22} \cdots \psi_{k2}\ \ \psi_0\ \psi_{inv} \cdots \psi_0 \\ \vdots \quad \vdots \quad \ldots \vdots \quad | \vdots \quad \vdots \quad \ldots \vdots \\ \psi_{1s}\ \psi_{2s} \cdots \psi_{ks} \,|\, \psi_0\ \psi_0 \ \cdots \psi_{inv} \end{bmatrix} \circ \begin{bmatrix} \psi_I\ \psi_0 \cdots \psi_0 \\ \psi_0\ \psi_I \cdots \psi_0 \\ \vdots \quad \vdots \ \ldots \vdots \\ \psi_0\ \psi_0 \cdots \psi_I \\ ------ \\ \psi_{11}\ \psi_{21} \cdots \psi_{k1} \\ \psi_{12}\ \psi_{22} \cdots \psi_{k2} \\ \vdots \quad \vdots \quad \ldots \quad \vdots \\ \psi_{1s}\ \psi_{2s} \cdots \psi_{ks} \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_k \end{bmatrix} = \begin{bmatrix} e \\ e \\ \vdots \\ e \end{bmatrix}$$

$$\begin{bmatrix} \psi_{11}\ \ \psi_{21}\ \ \cdots \psi_{k1} \,|\, \psi_{inv}\ \ \psi_0\ \ \cdots \psi_0 \\ \psi_{12}\ \ \psi_{22}\ \ \cdots \psi_{k2}\ \ \ \psi_0\ \ \psi_{inv}\ \ \cdots \psi_0 \\ \vdots \quad \vdots \quad \ldots \vdots \quad | \vdots \quad \vdots \quad \ldots \quad \vdots \\ \psi_{1s}\ \ \psi_{2s}\ \ \cdots \psi_{ks} \,|\, \psi_0\ \ \psi_0\ \ \ \cdots \psi_{inv} \end{bmatrix} \circ \begin{bmatrix} \psi_I(u_1) \\ \psi_I(u_2) \\ \vdots \\ \psi_I(u_k) \\ \bigoplus_{i=1}^{k} \psi_{i1}(u_i) \\ \vdots \\ \bigoplus_{i=1}^{k} \psi_{is}(u_i) \end{bmatrix} = \begin{bmatrix} e \\ e \\ \vdots \\ e \end{bmatrix}$$

$$\begin{bmatrix} \{\bigoplus_{l=1}^{k}\psi_{l1}(u_l)\} \oplus \{\psi_{inv}(\bigoplus_{i=1}^{k}\psi_{i1}(u_i))\} \\ \vdots \\ \{\bigoplus_{l=1}^{k}\psi_{ls}(u_l)\} \oplus \{\psi_{inv}(\bigoplus_{i=1}^{k}\psi_{is}(u_i))\} \end{bmatrix} = \begin{bmatrix} e \\ e \\ \vdots \\ e \end{bmatrix}$$

$$\begin{bmatrix} v_1 \oplus \psi_{inv}(v_1) \\ \vdots \\ v_s \oplus \psi_{inv}(v_s) \end{bmatrix} = \begin{bmatrix} e \\ \vdots \\ e \end{bmatrix}$$

which yields

$$\begin{bmatrix} \psi_{11}\ \psi_{21} \cdots \psi_{k1} \mid \psi_{inv}\ \psi_0 \cdots \psi_0 \\ \psi_{12}\ \psi_{22} \cdots \psi_{k2}\ \ \psi_0\ \psi_{inv} \cdots \psi_0 \\ \vdots\ \ \vdots\ \ \ldots \vdots\ \mid \vdots\ \ \vdots\ \ \ldots\ \vdots \\ \psi_{1s}\ \psi_{2s} \cdots \psi_{ks} \mid \psi_0\ \psi_0\ \cdots \psi_{inv} \end{bmatrix} \circ \begin{bmatrix} \psi_I\ \psi_0 \cdots \psi_0 \\ \psi_0\ \psi_I \cdots \psi_0 \\ \vdots\ \ \vdots\ \ldots \vdots \\ \psi_0\ \psi_0 \cdots \psi_I \\ ------ \\ \psi_{11}\ \psi_{21} \cdots \psi_{k1} \\ \psi_{12}\ \psi_{22} \cdots \psi_{k2} \\ \vdots\ \ \vdots\ \ \ldots\ \ \vdots \\ \psi_{1s}\ \psi_{2s} \cdots \psi_{ks} \end{bmatrix} = \begin{bmatrix} \psi_0 \cdots \psi_0 \\ \vdots\ \ldots\ \vdots \\ \psi_0 \cdots \psi_0 \end{bmatrix}$$

That is $H \circ \Psi^{tr} = [O_{k\times s}]$.
In a similar way it can be proved that $\Psi \circ H^{tr} = [O_{k\times s}]$, hence the result.

The class of codes over A_{p^m} obtained using Ψ contains as a proper subclass the linear codes over $GF(p^m)$. This can be illustrated using the following example.
Example 2: (n,k) codes over A_{2^2} and (n,k) codes over $GF(4)$.
The matrix Ψ with entries $\psi_{ij} \in End(A_{2^2}) \equiv M_2(Z_2)$ generates (n,k) codes over A_{2^2} denoted by the set P.
The matrix Ψ with entries $\psi_{ij} \in GL_2(Z_2) \subset End(A_{2^2})$ generates (n,k) codes over A_{2^2} denoted by the set P'.
The matrix Ψ with entries $\psi_{ij} \in F_{2^2} \subset GL_2(Z_2) \subset End(A_{2^2})$ generates (n,k) codes over A_{2^2} denoted by the set P''. This set coincides with (n,k) codes over $GF(4)$.

Clearly the following inclusion property holds, $\mathrm{P} \supset \mathrm{P}' \supset \mathrm{P}''$: Based on example 2 we present, in Table 2, three new (4,2,3) group codes and their binary images, where the codes belong to the set P', and they do not belong to the set P''; that means that they cannot be obtained as linear codes over $GF(4)$. We also observe that these codes are self-dual, MDS and two of them are also cyclic.

Table 2: New (4,2,3) group codes over $A_{2^2} \equiv C_2 \oplus C_2 \equiv \{00,10,01,11\} \equiv \{0,1,2,3\}$

Generator Matrix	Code	Binary Image	Remarks
$\begin{bmatrix} \begin{pmatrix}10\\01\end{pmatrix} & \begin{pmatrix}00\\00\end{pmatrix} & \begin{pmatrix}11\\01\end{pmatrix} & \begin{pmatrix}01\\11\end{pmatrix} \\ \begin{pmatrix}00\\00\end{pmatrix} & \begin{pmatrix}10\\01\end{pmatrix} & \begin{pmatrix}11\\10\end{pmatrix} & \begin{pmatrix}10\\11\end{pmatrix} \end{bmatrix}$	0000 0123 0232 0311 1013 1130 1221 1302 2031 2112 2203 2320 3022 3101 3210 3333	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	MDS SELF-DUAL
$\begin{bmatrix} \begin{pmatrix}10\\01\end{pmatrix} & \begin{pmatrix}00\\00\end{pmatrix} & \begin{pmatrix}01\\11\end{pmatrix} & \begin{pmatrix}11\\01\end{pmatrix} \\ \begin{pmatrix}00\\00\end{pmatrix} & \begin{pmatrix}10\\01\end{pmatrix} & \begin{pmatrix}10\\11\end{pmatrix} & \begin{pmatrix}11\\10\end{pmatrix} \end{bmatrix}$	0000 0113 0231 0322 1023 1130 1212 1301 2032 2121 2203 2310 3011 3102 3220 3333	00 00 00 00 00 10 10 11 00 01 11 10 00 11 01 01 10 00 01 11 10 10 11 00 10 01 10 01 10 11 00 10 01 00 11 01 01 10 01 10 01 01 00 11 01 11 10 00 11 00 10 10 11 10 00 01 11 01 01 00 11 11 11 11	MDS SELF-DUAL CYCLIC
$\begin{bmatrix} \begin{pmatrix}10\\01\end{pmatrix} & \begin{pmatrix}00\\00\end{pmatrix} & \begin{pmatrix}11\\10\end{pmatrix} & \begin{pmatrix}10\\11\end{pmatrix} \\ \begin{pmatrix}00\\00\end{pmatrix} & \begin{pmatrix}10\\01\end{pmatrix} & \begin{pmatrix}11\\01\end{pmatrix} & \begin{pmatrix}01\\11\end{pmatrix} \end{bmatrix}$	0000 0132 0223 0311 1031 1103 1212 1320 2013 2121 2230 2302 3022 3110 3201 3333	00 00 00 00 00 10 11 01 00 01 01 11 00 11 10 10 10 00 11 10 10 10 00 11 10 01 10 01 10 11 01 00 01 00 10 11 01 10 01 10 01 01 11 00 01 11 00 01 11 00 01 01 11 10 10 00 11 01 00 10 11 11 11 11	MDS SELF-DUAL CYCLIC

4. Conclusion

In this paper, the formal definitions of a generator and parity check matrices over the endomorphism ring of the elementary Abelian groups have been presented. The well-known theorem that relates the generator and parity check matrices of linear codes over fields were generalized to group codes over elementary Abelian groups. New codes, MDS, Self-Dual, and Cyclic over the Abelian group with four elements, which cannot be obtained as linear codes over fields, were also given. The algebraic framework motivates us to a further study of the class of group codes that are cyclic over elementary Abelian groups especially over A_{2^2} to cover the recently developed codes in Ran and Snyders (2000).

References

BIGLIERI, E. and ELIA, M. 1993 Construction of linear block codes over groups. IEEE International Symposium on Information Theory, San Antonio, Texas.

FORNEY, G.D. 1992 On the Hamming distance properties of group codes. *IEEE Trans. Inform. Theory*, **IT-38:** 1797-1801.

FORNEY, G.D. JR. and TROTT, M.D.1993 The dynamics of group codes: state space, trellis diagram, and the canonical encoders. *IEEE Trans. Inform. Theory*, **IT-39:** 1491-1513.

McDONALD, B.R. 1974. *Finite rings with identity*. Marcel Dekker, New York, 1974.

RAN, M. and SNYDERS, J. 2000. On cyclic reversible self-dual additive codes with odd length over Z_{2^2}. *IEEE Trans. Inform. Theory*, **IT-46:** 1056-1059.

Received 5 February 2002
Accepted 3 September 2003