SQU Journal For Science, 14 (2009) 53-59

Transform Domain Characterization of Dual Group Codes of Cyclic Group Codes over Elementary Abelian Groups

Adnan Abdulla Zain

Department of Electronics and Communications Engineering, Faculty of Engineering, University of Aden, Yemen. Email: adnan_zain2003@yahoo.com.

الوصف في المجال المتحول للشفرات المزدوجة للشفرات الدورية على الزمر من نوع (آبل)

عدنان عبدالله زين

خلاصة: استخدمت مجموعة رموز الزمر من نوع (آبل) في تعريف الازدواجية بين المجموعات الجزئية للمجموعة ، والتي تم تعميمها لتعريف الازدواجية بين الشفرات على الزمر. في هذا البحث تم تطوير الوصف في المجال المتحول للشفرات الدورية ذات طول ($n = p^m - 1$) على هذه الزمر واستنتاج الوصف لشفراتها المزدوجة.

ABSTRACT: The group of characters of an elementary Abelian group Z_p^m has been used to define duality between its subgroups, which in turn is extended to duality between group codes. The transform domain description of the dual codes of cyclic group codes of length $n = p^m - 1$ over Z_p^m has been developed in this paper. Several example codes and their duals have been presented also.

KEYWORDS: group codes, cyclic codes, dual codes, Abelian groups.

1. Introduction

The transform domain description of cyclic linear codes over $GF(p^m)$ using discrete Fourier transform (DFT) defined over an extension field $GF(p^m)^r$ is well known (Blahut, 1997). The transform domain description of cyclic group codes over an elementary Abelian group $Z_p^m = Z_p \oplus Z_p \oplus .... \oplus Z_p$ (m-times), using discrete Fourier transform (DFT) defined over an extension group $(Z_p^m)^r = Z_p^m \oplus Z_p^m \oplus \ldots \oplus Z_p^m$ (r-times) has been developed by Zain and Rajan (1997) ; this class of codes are subgroups of the Cartesian product group $(Z_p^m)^n = Z_p^m \oplus Z_p^m \oplus .... \oplus Z_p^m$ (n- times), which amounts to relaxing the condition of linearity,

hence yielding a larger class of codes that contains the class of linear codes. The important class of Reed-Solomon codes over $GF(p^m)$ where the length of the code n is equal to $p^m - 1$ has been generalized to Reed-Solomon group codes over the elementary Abelian group Z_p^m, which is the additive group of $GF(p^m)$ (Zain and Rajan, 1995). The dual codes of systematic group codes over finite Abelian groups have been characterized (Zain and Rajan, 1997) in terms of the endomorphism of the Abelian group that defines the group code.

In this paper, using the structural properties of the dual codes of cyclic group codes of length $n = p^m - 1$ over Z_p^m, their characterization in the transform domain is presented. Several example codes and their duals are presented also. The paper is organized as follows. Section 2 presents the mathematical preliminaries that are relevant to the development of the main results. In section 3 the main theorem that characterizes the codes and their duals in the transform domain is proved. Illustration of the applicability of the main theorem with examples codes and their duals is presented in section 4. Conclusions and suggestions for further work are given in section 5.

2. Mathematical preliminaries

The minimum mathematical background that is necessary for the development of the main result of the paper is presented in the following two subsections.

2.1 Group characters, inner product and dual subgroups

A character of a group G is a homomorphism of G into the group of units of the field of complex numbers C^* or group of units of any appropriate field in which there exist an $m-th$ root of unity, where m is the exponent of G. Let $\hat{G}$ be the set of characters of G.

Result (1)(Hungerford, 1989):

$$\hat{G} \cong G \tag{1}$$

Under the above isomorphism, the elements of $\hat{G}$ can be indexed with the elements of G as follows:

$$\eta : G \to \hat{G}$$
$$x \to \eta_x \in \hat{G}, \quad \forall x \in G \tag{2}$$

Let H be a subgroup of G .

Definition (1) (Hungerford, 1989):

The subgroup H^d of G is said to be the dual of the subgroup H if

$$\eta_H(H^d) = e \tag{3}$$

where e is the identity element in the group of units.

Definition (2) (Hungerford, 1989):

A subgroup H of G is said to be self dual if

$$H^d = H \, . \tag{4}$$

An inner product on G is defined next.
The indexing of the characters of G with the elements of G can be done such that the mapping:

$$G \times G \to C^*$$

given by

$$< x, y >= \eta_x(y), \quad x, y \in G \tag{5}$$

is symmetric in both arguments. This mapping will be called an inner product on G (Delsarte 1972).

Result (2)(Hungerford, 1989):

$$\left|H\right|\left|H^d\right| = \left|G\right|. \tag{6}$$

where $|.|$ stands for the cardinality of the set.

2.2 Elementary Abelian Discrete Fourier Transform (EADFT)

Let Z_p^m denote the elementary Abelian group, $Aut(Z_p^m)$ the group of automophrisms of Z_p^m, and n denote the length of the code where n and p are relatively prime.

Definition (3) (Zain and Rajan, 1995): The transform vector of

$$\vec{a} = (a_0, a_1, \ldots, a_{n-1}), \quad a_i \in Z_p^m, \ i = 0,1,\ldots,n-1,$$

denoted by $\vec{A} = (A_0, A_1, \ldots, A_{n-1}), \quad A_j \in Z_p^m, \ j = 0,1,\ldots,n-1,$ is defined by

$$A_j = \bigoplus_{i=0}^{n-1} \alpha^{ij}(a_i) \tag{7}$$

where $\alpha(a_i)$ denotes the image of a_i under the action of the automorphism $\alpha \in Aut(Z_p^m)$ whose order is n.
The EADFT transform defined above is invertible (Zain and Rajan, 1995), and its inverse is given below:

$$a_i = \Lambda_n^{-1}\left(\bigoplus_{j=0}^{n-1} \alpha^{-ij}(A_j)\right), i = 0,1,\ldots,n-1 \tag{8}$$

where Λ_n^{-1} is the inverse of an automorphism of Z_p^m defined by:

$$\Lambda_n(x) = x \oplus \cdots \oplus x(\text{n times}) \ \ \forall x \in Z_p^m \tag{9}$$

The following definition is important to the characterization of the class of codes that are cyclic.
Definition (4) (Zain and Rajan, 1997): (Invariant Subgroups): Let G be a group and H be a subgroup of $Aut(G)$. A subgroup of G which is invariant under the action of H on G is called a H -invariant subgroup of G.
Definition (5)(Zain and Rajan, 1997):(Conjugacy Classes): The p^m -conjugacy class containing $j, \ 0 \le j \le p^m - 1$ is the set

$$C_{p,n}(j) \equiv \{j, jp^m, j(p^m)^2, \ldots, j(p^m)^{e_j - 1}\}$$

where $j(p^m)^{e_j} = j \ \text{modulo}\,(p^m)$, and e_j is the exponent.

2.3 Transform Domain Characterization of Cyclic Group Codes

The transform domain characterization of the class of codes that are group codes (not necessarily linear codes), cyclic and of length $n = p^m - 1$ over the elementary Abelian group Z_p^m presented in (Zain and Rajan 1995), identifies two cases as shown below:

- Case 1, In this class of cyclic group codes, all the transform components are free.
- Case 2, In this class of cyclic group codes, the transform components that are in the same conjugacy class are related.

In this paper, we consider case 1 which is the class of codes of length n that is equal to $p^m - 1$, in which the transform components that lie in the same conjugacy class are all either free or zeros.

3. Main theorem

The following theorem gives the transform domain characterization of the dual codes of the cyclic codes, whose transform components that lie in one conjugacy class are all either free or assigned zeros, (those codes covered by case 1).

Theorem (1):

If C is a cyclic group code of length $n = p^m - 1$ over Z_p^m whose transform vectors are all free and take values from the following S_j -invariant subgroups of Z_p^m, $S_{j1}, S_{j2}, \ldots, S_{jn}$ for the components $j_1, j_2, \ldots, j_n$, respectively, then the transform vectors of the dual code C^d take values from the following S_j -invariant subgroups, $S_{j1}^d, S_{j2}^d, \ldots, S_{jn}^d$ respectively for the components $(n - j_1), (n - j_2), \ldots, (n - j_n)$.

Proof:

Let $\vec{A} = (A_0, A_1, \ldots, A_{n-1})$ be the transform vector of the code vector $\vec{a} = (a_0, a_1, \ldots, a_{n-1}) \in C$.

By definition of the EADFT and its inverse, we have

$$a_i = \Lambda_n^{-1}\left(\bigoplus_{j=0}^{n-1} \alpha^{-ij}(A_j) \right), i = 0,1,\ldots,n-1$$

Given that the transform vectors take values from $S_{j1}, S_{j2}, \ldots, S_{jn}$ invariant subgroups for the components $j_1, j_2, \ldots, j_n$ respectively, we have

$$a_i = S_{j1} \oplus S_{j2} \oplus \ldots \oplus S_{jn}, \quad i = 0,1,\ldots,n-1. \tag{10}$$

Now, let $\vec{b} = (b_0, b_1, \ldots, b_{n-1}) \in C^d$ and $\vec{B} = (B_0, B_1, \ldots, B_{n-1})$ be its transform vector, so we have

$$b_i = \Lambda_n^{-1}\left(\bigoplus_{j=0}^{n-1} \alpha^{-ij}(B_j) \right), i = 0,1,\ldots,n-1 \tag{11}$$

Since the components of the transform vector $(n - j_1), (n - j_2), \ldots, (n - j_n)$ take values from the $S_{j1}^d, S_{j2}^d, \ldots, S_{jn}^d$ invariant subgroups, we have

$$b_i = S_{j1}^d \oplus S_{j2}^d \oplus \ldots \oplus S_{jn}^d, \quad i = 0,1,\ldots,n-1. \tag{12}$$

Next we compute the inner product $< \vec{a}, \vec{b} >$:

$$< \vec{a}, \vec{b} >= \prod_{i=0}^{n-1} \eta_{a_i}(b_i) = \prod_{i=0}^{n-1} \{\eta_{S_{j1}}(S_{j1}^d) * \eta_{S_{j2}}(S_{j2}^d) * \ldots * \eta_{S_{jn}}(S_{jn}^d)\} = \prod_{i=0}^{n-1} e = e$$

where $*$ stands for the operation in the group of units.

Now, we want to show that $\left|C\right\|C^d\left| = \right|G|^n$.

since $|C| = |S_{j1}\|S_{j2}|\ldots|S_{jn}|$,

and $|C^d| = |S_{j1}^d\|S_{j2}^d|\ldots|S_{jn}^d|$,

we have

$$|C\|C^d| = |S_{j1}\|S_{j1}^d|\ldots|S_{jn}\|S_{jn}^d| = |G|\ldots|G| = |G|^n$$

This completes the proof.

4. Illustrations of the theorem

The usefulness of the main theorem is best demonstrated with the following two numerical examples, where a length 3 cyclic group code over the elementary Abelian group with four elements is characterized in the transform domain, then by using the theorem, its dual is also characterized and obtained.

Example (1):

Let $G \cong Z_2 \oplus Z_2 = \{<00>, <10>, <01>, <11>\}$.

Then we define $\hat{G} = \{\eta_{<00>}, \eta_{<10>}, \eta_{<01>}, \eta_{<11>}\}$ according to the following inner product mapping $G \times G \to C^*$ given by $< x, y >= \eta_x(y), \quad x, y \in G$ where $C^* \cong Z_2 = \{0,1\}$ since 2 is the exponent of G. The detailed mapping is given in Table 1:

Table 1. Characters mappings

	<00>	<10>	<01>	<11>
$\eta_{<00>}$	0	0	0	0
$\eta_{<10>}$	0	1	0	1
$\eta_{<01>}$	0	0	1	1
$\eta_{<11>}$	0	1	1	0

Table 2 gives all possible dual subgroups of $G \cong Z_2 \oplus Z_2$.

Table 2. Subgroups and their Duals.

Subgroup (H)	Dual subgroup (H^d)
{<00>}	{<00>, <10>, <01>, <11>}
{<00>, <10>}	{<00>, <01>}
{<00>, <01>}	{<00>, <10>}
{<00>, <11>}	{<00>, <11>}
{<00>, <10>, <01>, <11>}	{<00>}

Note that the subgroup {<00>, <11>} is self-dual.

Example (2): Length 3 code over $G \cong Z_2 \oplus Z_2$ and its dual.

The transform vectors for the code are listed in the first column where the characterization for the conjugacy classes is as follows:

$$A_0 = \{<00>, <10>\},\ A_1 = \{<00>\},\ A_2 = \{<00>, <10>, <01>, <11>\}.$$

According to the theorem the dual code should have the following characterization for the conjugacy classes:

$B_0 = \{<00>, <01>\}$, which is the dual subgroup of $\{<00>, <10>\}$

$B_1 = \{<00>, <10>, <10>, <11>\}$, which is the dual subgroup of $\{<00>\}$

$B_2 = \{<00>\}$, which is the dual subgroup of $\{<00>, <10>, <10>, <11>\}$

The detailed listing of the code vectors and the transform vectors of the code and its dual is presented in Table 3.

Table 3. Code vectors and their transforms.

Transform Vector	Code Vector	Transform Vector	Dual Code Vector
A_0 A_1 A_2	a_0 a_1 a_2	B_0 B_1 B_2	b_0 b_1 b_2
<00> <00> <00>	<00> <00> <00>	<00> <00> <00>	<00> <00> <00>
<00> <00> <10>	<00> <11> <01>	<00> <10> <00>	<00> <11> <10>
<00> <00> <01>	<01> <00> <11>	<00> <01> <00>	<01> <01> <01>
<00> <00> <11>	<01> <11> <10>	<00> <11> <00>	<01> <10> <11>
<10> <00> <00>	<10> <01> <11>	<01> <00> <00>	<10> <00> <11>
<10> <00> <10>	<10> <10> <10>	<01> <10> <00>	<10> <11> <01>
<10> <00> <01>	<11> <01> <00>	<01> <01> <00>	<11> <01> <10>
<10> <00> <11>	<11> <10> <01>	<01> <11> <00>	<11> <10> <00>

5. Conclusions

The structural properties of the dual codes of cyclic group codes of length $n = p^m - 1$ over the elementary Abelian group Z_p^m have been used to present and prove a theorem that gives the characterization, in the transform domain, of the dual codes in terms of the dual subgroups of the group Z_p^m. As an example a length 3 cyclic group codes over Z_2^2 is characterized in the transform domain, then its dual code is obtained.

Further work can be done to generalize the main result to other classes of cyclic group codes whose transform characterization contains components that are related (Zain and Rajan, 1997), and to quasi-cyclic codes (Dey and Rajan, 2003).

5. References

BLAHUT, R.E. 1997. *Theory and Practice of Error Control Codes*, Addison-Wesely.

DELSARTE, P. 1972. Bounds for unrestricted codes by linear programming. *Philips Research Dev. J.*, **27:** 272-289.

DEY, B.K. Rajan B. S. 2003. DFT Domain Characterization of Quasi-Cyclic Codes", *Applicable Algebra in Engineering, Communication and Computing*, Springer-Verlag, **13(1):** 453-474.

HUNGERFORD, T.W. 1989. *Algebra*, Springer-Verlag.

ZAIN, A.A. and RAJAN, B.S. 1997. M-PSK BCM Using Cyclic Codes over Elementary Abelian Groups. *Proceedings of ISIT*, Ulm, Germany, June 29-July 4 1997, p.410.

ZAIN, A.A. and RAJAN, B.S. 1995. Reed-Solomon Group Codes. *Proceedings of ISIT*, British Columbia, Canada, 17-22 September 1995, p.495.

ZAIN, A.A. and RAJAN, B.S. 1997. Dual Codes of Systematic Group Codes over Abelian Groups. *Applicable Algebra in Engineering, Communication and Computing*, Springer-Verlag, **8**(**1):** 71-83.

Received 24 April 2008
Accepted 24 May 2009