can be applied to higher rate and multiple-error correcting cyclic codes.

Since the derivation of these results involves only the error position, the results are applicable to cyclic codes over GF(2^m).

The permutation decoding concept in the error-trapping technique for decoding cyclic codes can be studied further by considering the following.

1) Generalize the improvements on the lower bounds *n* for high steps of the group *(T, U)* permutations, so that the capability of error-trapping technique can be extended to higher rate codes.
2) In addition to the group *(T, U)* permutations, there are other sets of permutations for which certain cyclic codes are invariant. At the present time, little theoretical progress has been made on this problem. If several different sets of permutations are used together, better lower bounds on *n* may be achieved compared to just using one set of permutations.

REFERENCES

[1] S. Lin and D. J. Costello, *Error-Control Coding; Fundamentals and Applications.* Englewood, NJ: Prentice-Hall, 1983.
[2] M. E. Mitchell, "Coding and decoding operation research," G.E. Advanced Electron. Final Rep. Contract AF 19(604)-6183, Air Force Cambridge Research Labs., Cambridge, MA, 1961.
[3] ———, "Error-trap decoding of cyclic codes," G.E. Rep. 62MCD3, General Electric Military Communications Dept., Oklahoma City, OK, Dec. 1962.
[4] L. Rudolph, "Easily implemented error-correction encoding-decoding," G.E. Rep. 62MCD2, General Electric Corporation, Oklahoma City, OK, Dec. 1962.
[5] T. Kasami, "A decoding procedure for multiple-error-correction cyclic codes," *IEEE Trans. Inform. Theory,* vol. IT-10, pp. 134-139, Apr. 1964.
[6] E. Prange, "The use of information sets in decoding cyclic codes," *IEEE Trans. Inform. Theory,* vol. IT-8, pp. 85-89, Sept. 1962.
[7] F. J. MacWilliams, "Permutation decoding of systematic codes," *Bell Syst. Tech. J.,* vol. 43, pt.I, pp. 485-505, Jan. 1964.
[8] E. J. Weldon, Jr., "A comparison of an interleaved Golay code and a three-dimensional product code," Final Rep., USNELC Contract N0095368M5345, Aug. 1968.
[9] A. Benyamin-Seeyar, S. S. Shiva, and V. K. Bhargava, "Capability of the error-trapping technique in decoding cyclic codes," *IEEE Trans. Inform. Theory,* vol. IT-32, pp. 166-180, Mar. 1986.
[10] S. G. S. Shiva, A. Benyamin-Seeyar, and V. K. Bhargava, "On the permutation-decodability of triple-error-correcting codes," presented at *Proc. 21 st Ann. Allerton Conf. Commun., Contr., Comput.,* Univ. of Illinois, Oct. 1983.
[11] M. Jia, A. Benyamin-Seeyar, and T. Le-Ngoc, "Exact lower bounds on the code length of three-step permutation-decodable cyclic codes," Int. Tech. Rep. DCRL-91-3, Concordia Univ., Jan. 1991.

Transform Domain Characterization of Abelian Codes

B. Sundar Rajan, *Member, IEEE,* and M. U. Siddiqi

Abstract—**Abelian codes constitute a class of codes that includes cyclic codes as a special case. It is shown that the general class of abelian codes can be characterized in the transform domain using discrete Fourier transform (DFT) over finite fields with appropriate mixed radix number system as the indexing scheme for DFT coefficients. A simple transform domain description for dual codes of abelian codes is also obtained. Using this description the idempotent generator of the dual of a given abelian code can be easily obtained. Finally, it is shown that in the case of cyclic codes which can be considered as abelian codes also, one can work in smaller extension fields compared to the extension fields if they were considered as cyclic codes only.**

Index Terms—**Abelian codes; mixed-radix number system; dual codes; transform domain.**

Manuscript received July 31, 1991.

B. S. Rajan is with the Electrical Engineering Department, Indian Institute of Technology, Delhi, New Delhi-110016, India.

M. U. Siddiqi is with the Electrical Engineering Department, Indian Institute of Technology, Kanpur-208016, India.

IEEE Log Number 9201541.

I. INTRODUCTION

In the area of error-control codes, a cyclic code is described as an ideal of the group algebra of an appropriate cyclic group [1], [2]. A class of codes, called abelian codes, that includes cyclic codes as a subclass has been studied by several authors [3]-[7]. Berman [3], [4] has shown that under certain conditions the general class of abelian codes has better error correcting capabilities than the class of cyclic codes. Cyclic codes over finite fields have been studied in the transform domain [8], [9] using discrete Fourier transform (DFT) over finite fields. In this correspondence, we extend the transform approach developed for cyclic codes to the general class of abelian codes. The key idea is using an appropriate mixed-radix number system for indexing the DFT coefficients and codeword components. A transform domain characterization for abelian dual code pair is also obtained. Some of the cyclic codes can be considered as abelian codes also. For such codes it is shown that one can work in smaller extension fields compared to the extension fields if they were considered only as cyclic codes.

The content of this correspondence is arranged as follows: In Section II, using appropriate mixed-radix number system, abelian codes and DFT's suitable for the transform domain study of these codes are described. Properties of these DFT's that are useful for our study are proved. Transform domain characterization of abelian codes is obtained in Section III. In Section IV, dual codes of abelian codes and their idempotent generators are described in the transform domain. In Section V, through examples, it is illustrated how, for cyclic codes that are also abelian, one is able to work in smaller extension fields.

II. DFT FOR ABELIAN CODES

Let $G = \{g_o, g\backslash, g2, \text{"}, g_n\text{--}\wedge$ be an abelian group of order n and let $G¥(q)$ denote the finite field with q elements. The group algebra of G over GF(<?), denoted by FG, is the set

$$FG = \left\{ \sum_{g \in G} a_g g / a_g \in \mathrm{GF}(q) \right\}$$

with addition and multiplication operations respectively defined by

$$\mathop{\mathbf{E}}_{\text{geC}} a_g g + \mathop{\mathbf{E}}_{geG} b_g g = \mathop{\mathbf{E}}_{geG} (\text{«}_g + b_g)\S \qquad (.1)$$

and

$$\left(\sum_{g \in G} a_g g \right) \left(\sum_{h \in G} b_h h \right) = \sum_{k \in G} c_k k, \qquad (2)$$

where

$$^{c}k = \mathop{\mathbf{E}}_{gh = k} (a_g b_h).$$

There is an obvious one-to-one correspondence between the set of n-tuples over $GF(q)$ and FG. The subsets of the set of n-tuples over GF(g) that correspond to ideals of FG are defined as abelian codes [3], [5], [7]. It can be seen that when G is a

cyclic group, (2) represents cyclic convolution and ideals of *FG* are cyclic codes. For general abelian groups (2) represents a generalized convolution determined by the structure of the abelian group and accordingly abelian codes are linear codes with the property that the set of codewords are closed under this generalized convolution.

The key idea to the transform domain characterization of abelian codes is the use of mixed-radix number system [10] for indexing DFT coefficients that is explained as follows. Let $m_0, m_1, \cdots, m_{r-1}$ be the specified positive integers called mixed radixes and let n be the product of the mixed radixes i.e., $n = m_0 m_1 \cdots m_{r-1}$. Then any integer i; $0 \le i \le (n-1)$ can be expressed as

$$i = i_{r-1}(m_0 m_1 \cdots m_{r-2}) + i_{r-2}(m_0 m_1 \cdots m_{r-3}) + \cdots + i_2(m_0 m_1) + i_1 m_0 + i_0,$$

where $0 \le i_k < m_k$, $k = 0, 1, \cdots, (r-1)$. The integer i is represented by $\langle i_{r-1}, i_{r-2}, \cdots, i_0\rangle$ and called mixed-radix representation. In the mixed-radix number system, addition and subtraction, denoted respectively by $\oplus$ and $\ominus$, are defined as follows. For $i = \langle i_{r-1}, i_{r-2}, \cdots, i_0\rangle$ and $j = \langle j_{r-1}, j_{r-2}, \cdots, j_0\rangle$, mixed-radix addition is defined as

$$i \oplus j = \langle a_{r-1}, a_{r-2}, \cdots, a_0\rangle,$$

where

$$a_k = (i_k + j_k) \bmod m_k, \qquad k = 0, 1, \cdots, r-1,$$

and mixed-radix subtraction is defined as

$$i \ominus j = \langle b_{r-1}, b_{r-2}, \cdots, b_0\rangle$$

where

$$b_k = (i_k - j_k) \bmod m_k, \qquad k = 0, 1, \cdots, r-1.$$

Any finite abelian group can be expressed as a direct product of its cyclic subgroups [11]. Let G be the direct product of r cyclic subgroups, denoted by $C_0, C_1, \cdots, C_{r-1}$, of orders $m_0, m_1, \cdots, m_{r-1}$ respectively. Then any element $g \in G$ can be expressed as

where g_k is a generator of C_k, $k = 0, 1, \cdots, r-1$. The element $g \in G$ is denoted by $g_{\langle i_{r-1}, \cdots, i_0\rangle}$ or simply by g_i. It is easily seen that the group operation can now be given in terms of mixed-radix number system with mixed-radixes $m_0, m_1, \cdots, m_{r-1}$ as

$$g_i g_j = g_{i \oplus j}.$$

With this representation of group elements and group operation, the generalized convolution, given by (2), of two elements of FG, $\sum_{i=0}^{n-1} a_i g_i$ and $\sum_{i=0}^{n-1} b_i g_i$, is given by $\sum_{i=0}^{n-1} c_i g_i$ where

$$c_k = \sum_{i=0}^{n-1} a_{k \ominus i} b_i, \qquad k = 0, 1, \cdots, n-1.$$

The DFT over G with mixed-radix number system as indexing scheme, suitable for length n abelian codes over GF(q), is obtained as follows. The exponent of an abelian group is the maximum of the orders of its elements. Let e be the exponent of G. Choose the least integer m such that e divides $(q^m - 1)$. In $GF(q^m)$, let $\alpha_{m_0}, \alpha_{m_1}, \cdots, \alpha_{m_{r-1}}$ denote elements of order respectively $m_0, m_1, \cdots, m_{r-1}$. The DFT is defined as follows

Definition 1: Let $a = (a_0, a_1, \cdots, a_{n-1})$ be an n-tuple over GF(q), where q is a power of a prime p and n and p are relatively prime. The DFT of a, which is an n-tuple over GF(q^m), denoted by $A = (A_0, A_1, \cdots, A_{n-1})$, is given by

$$A_j = \sum_{i_{r-1}=0}^{m_{r-1}-1} \cdots \sum_{i_0=0}^{m_0-1} (\alpha_{m_0})^{i_0 j_0} \cdots (\alpha_{m_{r-1}})^{i_{r-1} j_{r-1}} a_i, \qquad 0 \le j \le n-1,$$

where $i = \langle i_{r-1}, i_{r-2}, \cdots, i_0\rangle$ and $j = \langle j_{r-1}, j_{r-2}, \cdots, j_0\rangle$ are the mixed-radix representations of i and j with mixed-radixes $m_0, m_1, \cdots, m_{r-1}$.

The DFT previously defined has the following properties.

1) Convolution Property: If a, b, and c are n-tuples over $GF(q)$ such that $c_i = \sum_{k=0}^{n-1} a_{i \ominus k} b_k$, $i = 0, 1, \cdots, n-1$, then their DFT coefficients satisfy the relation $C_j = A_j B_j$, $j = 0, 1, \cdots, n-1$.

Proof: Taking the inverse DFT of $(C_0, C_1, \cdots, C_{n-1})$ and using $C_j = A_j B_j$, we get

$$c_i = \frac{1}{(n \bmod p)} \sum_{j=0}^{n-1} (\alpha_{m_0})^{-i_0 j_0} \cdots (\alpha_{m_{r-1}})^{-i_{r-1} j_{r-1}} \cdot \left\{ A_j \sum_{k=0}^{n-1} (\alpha_{m_0})^{k_0 j_0} \cdots (\alpha_{m_{r-1}})^{k_{r-1} j_{r-1}} b_k \right\}$$

$$= \frac{1}{(n \bmod p)} \sum_{k=0}^{n-1} b_k \cdot \left\{ \sum_{j=0}^{n-1} A_j (\alpha_{m_0})^{-(i_0 - k_0) j_0} \cdots (\alpha_{m_{r-1}})^{-(i_{r-1} - k_{r-1}) j_{r-1}} \right\}$$

$$= \frac{1}{(n \bmod p)} \sum_{k=0}^{n-1} b_k \{(n \bmod p) a_{i \ominus k}\}$$

$$= \sum_{k=0}^{n-1} a_{i \ominus k} b_k. \qquad \circ$$

This property shows that under the DFT the generalized convolution given by (2) is mapped onto pointwise multiplication in the transform domain.

2) Conjugate Symmetry Property: For an n-tuple $c = (c_0, c_1, \cdots, c_{n-1})$ over GF(q) the DFT coefficients in the transform vector $(C_0, C_1, \cdots, C_{n-1})$ are related by

$$C^q_{\langle j_{r-1}, \cdots, j_0\rangle} = C_{\langle (q j_{r-1})_{m_{r-1}}, \cdots, (q j_0)_{m_0}\rangle}$$

where $(qj_k)_{m_k}$ denotes $(qj_k) \bmod m_k$. For simplicity, we denote $\langle (qj_{r-1})_{m_{r-1}}, \cdots, (qj_1)_{m_1}, (qj_0)_{m_0}\rangle$ by $q(j)$. With this notation we have

$$C_j^q = C_{\langle j \rangle}.$$

Proof:

$$C_j^q = \left\{ \sum_{i_{r-1}=0}^{m_{r-1}-1} \cdots \sum_{i_0=0}^{m_0-1} (\alpha_{m_0})^{i_0 j_0} \cdots (\alpha_{m_{r-1}})^{i_{r-1} j_{r-1}} c_i \right\}^q$$

$$= \sum_{i_{r-1}=0}^{m_{r-1}-1} \cdots \sum_{i_0=0}^{m_0-1} \{(\alpha_{m_0})^{i_0 j_0} \cdots (\alpha_{m_{r-1}})^{i_{r-1} j_{r-1}} c_i\}^q.$$

Since the relation $(a + b)^q = a^q + b^q$ holds for any a and b in a field of q elements, we have

$$= \sum_{i_{r-1}=0}^{m_{r-1}-1} \cdots \sum_{i_0=0}^{m_0-1} \cdots = C_{\langle (qj_0)_{m_0}, (qj_1)_{m_1}, \cdots, (qj_{r-1})_{m_{r-1}}\rangle}$$

This property identifies those n-tuples over the extension field which are images, under DFT, of n-tuples over $GF(q)$.

3) Reversal Preserving Property: Let $c = (c_o, c_1, \cdots, c_{n-1})$ and $d = (d_0, d_1, \cdots, d_{n-1})$ be two n-tuples over $GF(q)$, and let $C = (C_0, C_1, \cdots, C_{n-1})$ and $D = (Z)_o, D_l, \cdots, D_{n-1})$ be their transform vectors. If $d_i = c_{nei}$- for all $i = 0, 1, \cdots, n-1$, then $D_t = C_{nei}$ for all $i = 0, l, \cdots, n-1$.

Proof: For any / e {0,1,---, n — 1}, we have

$$D_j = \sum_{i=0}^{n-1} (\alpha_{m_0})^{i_0 j_0} \cdots (\alpha_{m_{r-1}})^{i_{r-1} j_{r-1}} d_i$$

$$= \sum_{i=0}^{n-1} (a \quad V^{o;o} -- ra \quad V^{r-i;-1} c$$

$$= \sum_{k=0}^{n-1} \alpha^{(m_0 - k_0) j_0} \cdots \alpha^{(m_{r-1} - k_{r-1}) j_{r-1}} c$$

$$= \sum_{k=0}^{n-1} \alpha_{m_0}^{k_0(m_0 - j_0)} \cdots \alpha_{m_{r-1}}^{k_{r-1}(m_{r-1} - j_{r-1})} c_k$$

$$= C_{Bey}. \qquad \blacksquare$$

This property is useful in characterizing the dual abelian codes in the transform domain.

III. TRANSFORM DOMAIN CHARACTERIZATION

From the conjugate symmetry property, it is seen that the DFT coefficients in the set $\{C_{(j)}, C_{qU)}, \cdots, C_{qS} - i_{(j)}\}$, where $q^s(j) = (j)$, are related. This set is called the conjugacy class containing ;; denoted by I}, and s is called the exponent of the conjugacy class F;. The conjugacy classes form a partition of the set {0, l,2,--,(n - 1)}. The sum of the exponents of all the conjugacy classes is equal to n. Among the set of all n-tuples over GF(<jr^m) only those which satisfy the conjugate symmetry property, denoted by ft, constitute the image of all n-tuples over GF(<?) under DFT.

Theorem 1: The set ft of images of all n-tuples over GFd?) under DFT, is isomorphic to the direct sum of Galois fields given by

$$\text{ft} = \bigoplus_{k=l}^{t} GF(q^{s*}),$$

where t is the number of conjugacy classes and s_k, $k = 1,2,\cdots, t$, are the exponents of the conjugacy classes.

Proof: Let $(C_o, C_1, \cdots, C_{n-1})$ e ft. From the conjugacy relation we have $Cfl = C_o$. This means C_o must belong to the subfield of GF(<7^m) which is isomorphic to GF(g). In fact GF(<7^m) contains a unique subfield GF(^r^e) for every e that divides m. Now consider any other component C_i, where i e {1,2,---, n — 1}. Let the exponent of the conjugacy class F, be e,. From the conjugate symmetry property we have $Cf = C$,. This means C, must belong to the subfield of GF(g^m) that is isomorphic to GF(^^{e}0. In other words, it is necesary for all the components in the conjugacy class F; to take values only from the subfield GF(^^{e}0 to satisfy the conjugate symmetry property. Since the value at one component of a conjugacy class uniquely determines the values at other components of the conjugacy class and the set of all conjugacy classes form a partition of {0,1,--, n — 1} and since both addition and multiplication are pointwise in ft, we have

$$\Omega = \bigoplus_{i=1}^{t} GF(q^{e_i}),$$

where t is the number of conjugacy classes with exponents e_i, $i = 1, 2, \cdots, t$. $\blacksquare$

From Theorem 1, it follows that the set ft constitutes a semisimple ring under pointwise addition and pointwise multiplication. The DFT defines an isomorphism between FG considered as a ring and ft. This means there is a one-to-one correspondence between ideals of FG (that is abelian codes) and ideals of ft. Since multiplication in ft is pointwise and there are only trivial ideals in GF(g^m), every ideal of ft consists of those n-tuples that have zeros in some conjugacy classes and nonzeros in other conjugacy classes. Hence, we have the following transform domain characterization of abelian codes.

Definition 2: An abelian code of length n over GF(g) consists of the inverse DFT vectors of the set of n-tuples over GF(^^{m}) that satisfy the conjugate symmetry property and have zeros in specified DFT components.

Hence, an abelian code that has nonzeros in u conjugacy classes and zeros in other conjugacy classes in the transform domain can be given by

$$\bigoplus_{k=1}^{u} GF(q^{e_k}),$$

where e_k, $k = 1,2,\cdots,w$, are the exponents of the conjugacy classes in which nonzero values are taken. The number of codewords in this abelian code can be found as follows. A DFT component in the conjugacy class with exponent e_k can take any one of q^{et} elements GF(^^{e}*)- Since the value at one component of a conjugacy class does not put any constraint on the values of components of the other conjugacy classes, the total number of codewords is

$$\prod_{i=1}^{u}$$

Hence, the dimension of this abelian code is equal to the sum of the exponents $e_x + e_2 + \cdots e_u$.

IV. DUAL CODES

Two n-tuples over GF(<?), $a = (a_o, a_1, \cdots, a_{n-i})$ and $b = (b_o, b_1, \cdots, b_{n-i})$, are said to be orthogonal if E^oa,^,-= 0. Given a linear code L, the set of n-tuples that are orthogonal to all the codewords of L is a linear code called the dual code of L. In the following theorem, dual codes of abelian codes are characterized in the transform domain.

Theorem 2: For an abelian code 4> that takes zeros in the conjugacy classes $T_{ki}, T_{k2}, \cdots, T_{kii}$, where $k_x, k_2, \cdots, k_u$ e {0,1,---, (n - 1)}, the dual code $\$^d$ takes zero in all DFT components except those of the conjugacy classes $T_{neki}, T_{neki}, \cdots,$ F$_{neAv}$

Proof: Let $a = (a_o$»^{a}i>""»^{fl}«-i) ^{G} *• L^^{1} $^\$$* denote the abelian code with nonzeros in the conjugacy classes F^, F^,---, r$_v$ Also let $h = (h_o, h_i, \cdots, h_{n-i})$ e **. From $A_l H_i = 0$, $i = 0, 1, \cdots, n-1$, where $A = (A_Q, A_r, \cdots, A_{n-x})$ and $H = (H_Q, H_u, \cdots, H_{n-i})$ are the transform vectrors of a and h, respectively, it follows that

$$\left(\sum_{i=0}^{n-1} \quad \right)\left(\sum_{j=0}^{n-1} h_j S_i\right) = 0,$$

TABLE I
TRANSFORM VECTORS OF IDEMPOTENT GENERATORS OF ALL ABELIAN CODES OF LENGTH 9

Code */	Transform Vector of the Idempotent Generator of $<t>_I$								
	^<00>	^<01>	^<02>	A_{0}»>	$^{A}(U)$	$^{A}(12)$	-4<20>	^<21>	^<22>
* i.	0	1	1	0	1	1	0	1	1
* 2.	0	0	0	1	1	1	1	1	1
$ 3.	0	1	1	1	0	0	1	0	0
* 4.	0	1	1	1	0	1	1	1	0
* 5	0	0	0	1	1	0	1	0	1
* 6.	0	1	1	0	1	0	0	0	1
* 7.	0	0	0	0	0	1	0	1	0
Φ_8	0	1	1	1	1	0	1	0	1
* 9.	0	0	0	1	0	1	1	1	0
*10	0	1	1	0	0	1	0	1	0
Φ_{11}	0	0	0	0	1	0	0	0	1
*12	0	0	0	0	1	1	0	1	1
<D_{13}	0	1	1	0	0	0	0	0	0
*14	0	0	0	1	0	0	1	0	0
Φ_{15}	0	1	1	1	1	1	1	1	1
Φ_1	1	0	0	1	0	0	1	0	0
Φ_2	1	1	1	0	0	0	0	0	0
O-j	1	0	0	0	1	1	0	1	1
^ d	1	0	0	0	1	0	0	0	1
O_5	1	1	1	0	0	1	0	1	0
Φ_6	1	0	0	1	0	1	1	1	0
Φ_7	1	1	1	1	1	0	1	0	1
Φ_8	1	0	0	0	0	1	0	1	0
<I_{9}	1	1	1	0	1	0	0	0	1
*.o	1	0	0	1	1	0	1	0	1
(Φ_{11}	1	1	1	1	0	1	1	1	0
<^12	1	1	1	1	0	0	1	0	0
Φ_{13}	1	0	0	1	1	1	1	1	1
<&14	1	1	1	0	1	1	0	1	1
Φ_{15}	1	0	0	0	0	0	0	0	0

where g_i, $i = 0, 1, \cdots, n-1$, are the elements of the abelian group under consideration. In particular, the coefficient of the identity element, g_0, is equal to zero, i.e.,

$$\sum_{i=0} "ih_{nei} = o.$$

For a given element h in <£*, define $b = (f>_0, £>!, \cdots, £_{n-1})$ by $^{b}i = {}^{h}nei>^{l}$ $= 0, 1, \cdots, n-1$. Then,

$$\sum_{i=0}^{n-1} *_i A- = 0.$$

Hence, b e $4>^{d}$. But from the reversal preserving property it follows that the transform vector of b has nonzeros in the conjugacy classes $T_{neki}, T_{neki}, \cdots, T_n ek_u$- Let $** denote the set of all such vectors obtained from <J>*. We have shown that <&** is contained in $4>^{d}$ and $** has nonzeros in the conjugacy classes $T_{nekj}, T_{n\_eki}, \cdots, r_{neku}$. We proceed to show that <&** is same as $<t>^{d}$.

It is known that, as a group $<t^{d}$ is contained in the coset group GF"(<?)/$ [12]. So it is sufficient to show that $|<t>\|4>^{**}| = q''$, where |O| denotes the number of elements in 3>. Let e_x, $e_2, \cdots, e_u$ be the exponents of the conjugacy classes 1^, 1^, —, r^. Then,

$$|\Phi| = q^{(n-(e_1+e_2+\cdots+e_u))}$$

and

$$|\Phi^{**}| = (q^{e_1})(q^{e_2})\cdots(q^{e_u}) = q^{(e_1+e_2+\cdots+e_u)}.$$

Hence,

$$|<J>\|<£^{**}| = q''. \quad \square$$

Since (1 is a semisimple ring every ideal of it has a unique idempotent generator. Moreover, since the idempotent generator of the ideals of a finite field are 0 and 1, every idempotent generator of fl is an n-tuple which has 0 in some conjugacy classes and 1 in all other conjugacy classes. Because DFT is an isomorphism, these n -tuples should be transform vectors of the idempontent generators of the abelian codes. Now, using Theorem 2, given the idempotent generator of an abelian code in the transform domain, obtaining the transform vector of the idempotent generator of its dual code is straightforward. If the idempotent generator of the given abelian code has zeros in the conjugacy classes $T_{k_1}, T_{k_2}, \cdots, T_{k_u}$ then one obtains the idempotent generator of its dual code by having nonzeros in the conjugacy classes $T_{nBki}, T_{nek2}, \cdots, T_{n\&kii}$. For length 9 binary abelian codes, all idempotent generators are given in Table I.

V. EXAMPLES

The exponent e of an abelian group is less than the order of the group n, unless it is isomorphic to a cyclic group in which case the exponent is n. Hence, for cyclic case, the choice of the extension field GF(^m) is such that n divides $(q^m - 1)$. So, in general, for the same order n, the extension field required in the abelian case is a subfield of the extension field required for the cyclic case. In some cases, it so happens that all the cyclic codes of length n may turn out to be abelian codes also for some noncyclic abelian group of order n. The conditions under which this happens can be found in [12]. In such cases, one can work in a smaller extension field to study the cyclic codes considering them as abelian codes. Finally, this advantage is illustrated in the following examples which is discussed in detail to illustrate the other ideas also of this correspondence.

Example 1: Consider the noncyclic abelian group G of order 9 that is the direct product of two cyclic groups of order 3 each. Let us consider binary abelian codes, i.e., over GF(2), of length

9. The exponent of G is 3. Hence, the extension field is $GF(2^2)$. The mixed-radix number system considered has mixed-radixes $m_0 = 3$ and $m_1 = 3$. Let a be an element of order 3 in $GF(2^2)$ Then, for a nine-tuple,

a ~ (fl<00>°<01>'a<02>' a<10>>a<ll)>a<12>> a<20>>fl<21>> a<22>)>

the DFT is given by

» 0 W , > = £ L «lW0«''iyi«<.v>> ;0.;i = 0 , i , 2.
(limits: 2, 2; $i_o = 0$, $i_1 = 0$)

The conjugacy classes are {00}, {01,02}, {10,20}, {11,22}, and {12,21}. There are 5 conjugacy classes and every conjugacy class can take either zero or nonzero elements. Hence, there are total 32 codes including the trival codes. The transform vectors of the idempotent generators of all the nontrivial codes are listed in Table I. In Table I, the codes are labeled <*>, j = 1 to 15 and dual code of $, is denoted by <&. The entries 0 and 1 represent additive and multiplicative identities of the extension field $GF(2^2)$.

Explicitly, the codewords of the abelian code $<t>_u$ are

0 1 1 0 1 1 0 1 1
1 0 1 1 0 1 1 0 1
1 1 0 1 1 0 1 1 0 -
0 0 0 0 0 0 0 0 0

It is seen that the codewords are closed under cyclic shifts also. **It** can **be checked that** codes "!>2>^>i3>^)i5>^2'*i3'*i5 are cyclic codes also. These are the only cyclic codes of length 9. If one were to study these codes without considering them as abelian codes the extension field required is $GF(2^6)$.

Example 2: Consider binary, length 25, cyclic codes and abelian codes where the abelian group is the direct product of two cyclic groups of order 5 each. The exponent of this abelian group is 5. The least integer m such that 25 divides $2^m - 1$ is 20. Hence, the cyclic codes require the extension field $GF(2^{20})$. Whereas in the case of abelian codes since the least integer m such that 5 divides $2^m - 1$ is 4, the extension field required is $GF(2^4)$. It can be shown [12] that, also in this case, all the cyclic codes are included in the set of abelian codes.

VI. CONCLUSION

Abelian codes over finte fields are characterized in the transform domain using DFT defined over an appropriate extension field. A simple transform domain description of the dual code of a given abelian code is obtained. Also, it is shown that the idempotent generator of the dual of a given abelian code can be easily obtained from the idempotent generator of the given abelian code. It will be of considerable interest to extend the transform decoding that has been obtained for cyclic codes [9] to abelian codes.

REFERENCES

[1] W. W. Peterson and E. J. Weldon, *Error Correcting Codes,* 2nd ed. Cambridge, MA: MIT Press, 1972.
[2] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes.* Amsterdam: North Holland, 1977.
[3] S. D. Berman, "On the theory of group codes," *Kibernetika,* vol. 3, no. 1, 1967.
[4] ———, "Semisimple cyclic and abelian codes," *Kibemetika,* vol. 3, pp. 21-30, 1967.
[5] P. Camion, "Abelian codes," Tech. Rep. No. 1059, Mathematical Res. Center, 1971.
[6] P. Delsarte, "Automorphisms of abelian codes," *Phillips Res. Rep.,* vol. 25, pp. 389-402, 1970.
[7] F. J. MacWilliams, "Binary codes which are ideals in the group algebra of an abelian group," *BSTJ,* vol. 49, pp. 987-1011, 1970.
[8] R. E. Blahut, "Algebraic codes in the frequency domain," CISM Courses and Lectures, no. 258, pp. 447-494, 1979.
[9] ———, *Theory and Practice of Error Control Codes.* New York: Addison-Wesley, 1983.
[10] M. U. Siddiqi, "A study of permutation-invariant linear systems," Ph.D. thesis, Indian Inst. of Technol., Kanpur, 1976.
[11] M. Hall, Jr., *The Theory of Groups.* New York: MacMillan, 1964.
[12] H. S. Madhusudhana, "On abelian codes which are closed under cyclic shifts," M. Tech thesis, Indian Inst. of Technol., Kanpur, 1987.

Weighted Reed-Muller Codes and Algebraic-Geometric Codes

Anders Bjaert Sprensen

Abstract—**A generalization of the Reed-Muller codes, the weighted Reed-Muller codes, is presented. The code parameters are estimated and the duals are shown to also be weighted Reed-Muller codes. It is shown how the minimum distance of certain algebraic-geometric codes in many cases can be determined exactly or an upper bound can be found, using subcodes which are weighted Reed-Muller codes.**

Index Terms—**Error-correcting codes, Reed-Muller codes, finite projective geometry, algebraic-geometric codes.**

I. INTRODUCTION

The so called generalized Reed-Muller codes were introduced by Kasami, Lin, and Peterson [1], [3] and Weldon [2] about 1970. The multivariable approach [4] and the introduction of algebraic-geometric codes in the eighties inspired Lachaud [5] to introduce the projective Reed-Muller codes. Their parameters and cyclic structure were determined in [6] by the author. In this correspondence, we generalize some of the results of [6] by the presentation of so called weighted Reed-Muller codes and study their connection to algebraic-geometric codes.

In Section II, we define the affine and projective version of the weighted Reed-Muller codes, the WARM-codes and WPRM-codes, and we determine their code parameters (for the minimum distance in the projective case we give only an estimate). In Section III, we show that the dual of a WARM-code is again a WARM-code and that the dual of a WPRM-code is almost a WPRM-code. In Section IV, we show that a certain class of algebraic-geometric codes are in fact WARM-codes, and as an example we show that the curve used by Pellikaan *et al.* in [7], as a basis to prove that all linear codes are weakly algebraic-geometric, gives codes which are WARM-codes. Hence, the minimum distance of these codes are determined. Furthermore, we study the Hansen-Stichtenoth codes [10], [11] and we give an upper bound of the minimum distance using maximal WARM-subcodes.

Manuscript received July 23, 1991. This work was supported by the Danish Natural Science Research Council and by the Danish Research Academy.

The author is with the Department of Mathematics, University of Aarhus, 8000 Aarhus C, DK-Denmark and the Institute of Experimental Mathematics, University of Essen, Ellernstrasse 29, 4300 Essen 12, Germany.

IEEE Log Number 9201545.