Reed-Solomon group codes. In general, a group code over \( p \), denoted by \( C_\text{TM} \). This paper deals with MDS codes over \( C_\text{TM} \) of length \( p^m - 1 \) which is cyclic and MDS is called a Reed-Solomon group code. In general, a group code over \( C_\text{TM} \) need not be a linear code over \( GF(p^m) \) as shown in the following example.

**Example 1:** Consider length 4, code over \( C = \{1,x,y,xy\} \) consisting of the following 16 codewords:

\[
\begin{align*}
(1,1,1,1) & \quad (l,x,xy,y) \\
& \quad (l,y,y,x) \\
(x,l,xy,x) & \quad (x,x,l,x) \\
& \quad (x,y,y,y) \\
(y,x,x,l) & \quad (y,xy,x,l) \\
& \quad (y,y,xy,y) \\
(xy,l,1,x) & \quad (xy,y,xy,x) \\
& \quad (xy,xy,l,1) \\
& \quad (1,1,1,1)
\end{align*}
\]

The Hamming distance of this code is 3 and hence this is a MDS group code.

In [1], it is shown that if \( C \) is an \((n,k,n-k+1)\) group code over an abelian group \( G \) that is not elementary abelian, then there exists an \((n,k,n-k+1)\) group code over a smaller elementary abelian group \( G' \). In view of these results a natural question that arises is "Are all MDS group codes over \( C_\text{TM} \) linear over \( GF(p^m) \)?" Example 1 shows that this is not true, in general. But, if one considers only cyclic and length \( p^m - 1 \) group codes then it is true. In other words, all Reed-Solomon group codes over \( C_\text{TM} \) are conventional linear codes over \( GF(p^m) \). This can be shown by extending the well known transform approach for cyclic codes over finite fields [2] to group codes over elementary abelian groups.

**II. Transform approach to cyclic codes over elementary abelian groups:** Let \( C_\text{TM} \) denote the elementary abelian group isomorphic to direct sum of \( m \) cyclic groups of order \( p \) each. The ring of endomorphisms of \( C_\text{TM} \) is denoted by \( \text{End}(C_\text{TM}) \). The set of automorphisms of \( C_\text{TM} \), denoted by \( \text{Aut}(C_\text{TM}) \), form a group whose order is \( p^{m^2-m}n^\ell \), where \( n \) is the order of \( C_\text{TM} \). Among the cyclic subgroups of \( \text{Aut}(C_\text{TM}) \), there are maximal order subgroups have order \( (p^m-1) \). The ring \( \text{End}(C_\text{TM}) \) is isomorphic to \( \text{M}_n(p) \), ring of \( m \times m \) matrices over \( GF(p) \) [3]. This isomorphism gives matrix representation for elements of \( \text{End}(C_\text{TM}) \). It can be easily seen that, when this matrix representation is used, the groups of nonzero elements of \( GF(p^m) \) when represented by their companion matrices [4] corresponding to each irreducible polynomial of degree \( m \) coincides with a maximal order cyclic subgroup of \( \text{Aut}(C_\text{TM}) \).

**Definition 1:** For any \( C_\text{TM} \), let \( S \) denote a maximal order cyclic subgroup of \( \text{Aut}(C_\text{TM}) \). \( S \) with all zero matrix constitute an elementary abelian group isomorphic to \( C_\text{TM} \), considered along with matrix multiplication, form a ring called a canonical ring of \( C_\text{TM} \).

For example, the representation of a finite field with a canonical matrix and its powers along with all zero matrix, clearly gives a canonical ring of \( C_\text{TM} \).

**Definition 2:** Generalized Discrete Fourier Transform (GDFT): Let \( a^j = (a_0,a_1,...,a_{n-1}) \), where \( a \in C_\text{TM} \), \( i = 0,1,2,...,n-1 \). The transform vector of \( a \) denoted by \( \Delta_a \) is defined by

\[
\Delta_a = \sum_{i=0}^{n-1} a^j \phi^i, j = 0,1,...,n-1,
\]

where \( a \) is a generator of a cyclic subgroups of \( \text{Aut}(C_\text{TM}) \) of order \( n \) and \( \phi \) denotes group operation in \( C_\text{TM} \).

When \( C_\text{TM} \) is made \( GF(p^m) \) by imposing a multiplication structure with an irreducible polynomial \( g(x) \) then all non zero elements of \( GF(p^m) \) can be represented by the companion matrix of \( g(x) \) and its powers and \( a \) in Definition 2 can be replaced by the companion matrix of \( g(x) \). Then, Definition 2 coincides on the conventional DFT over \( GF(p^m) \), of length \( p^m - 1 \).

Using the GDFT given in Definition 2 and the properties of \( \text{Aut}(C_\text{TM}) \) and its matrix representation the following can be proved.

**Theorem 1:** Every cyclic and length \( p^m - 1 \) MDS group code is a conventional linear code over \( GF(p^m) \). In other words, all Reed-Solomon group codes over \( C_\text{TM} \) are conventional linear codes over \( GF(p^m) \).

**REFERENCES**