PUBLICATIONS DE L'INSTITUT MATHEMATIQU
Nouvelle séric, tome 21 (35), 1977. pp. 201—206

QUASI ABELIAN CODES*

Siri Krishan Wasan

(Received September 30, 1976)

Abstract

We introduce a class of codes which we call Quasi abelian codes. A linear subspace of the group algebra $GF(q)\,G$ of a finite abelian group G over a finite field $GF(q)$ which is $GF(q)$ H-module for some subgroup H of G is called a quasi abelian code in $GF(q)\,G$ with regard to H. It is shown that a quasi abelian code can be regarded as a direct sum of abelian codes. In particular, a quasi abelian code in $GF(q)\,G$ with respect to a cyclic subgroup of G is a quasi cyclic code. Direct sum of codes are considered and is shown that under certain conditions product of two codes which are direct sum of quasi cyclic codes is also a direct sum of quasi cyclic codes.

1. Introduction

Cyclic codes can be viewed as ideals in the group algebra of a cyclic group over a finite field. Berman (1967), Mac-William (1970) and Camion (1970) have investigated a more general class of codes, called Abelian codes, which are ideals in a group algebra of a finite abelian group over a finite field. Another extension of cyclic codes is a class of quasi cyclic codes. A quasi cyclic code is one in which every codeword shifted by r digits is also a codeword. Chen, Peterson and Weldon (1969) have shown that these codes have many interesting properties.

Since a linear code of block length n over $GF(q)$ is cyclic (i.e. every codeword shifted by one digit is also a codeword) iff it is an ideal in the group algebra $GF(q)\,C_n$. Therefore, a quasi cyclic code of length n over $GF(q)$, which is not cyclic, is not an ideal in $GF(q)\,C_n$ but it may be a module over $GF(q)\,H$ for some subgroup H of C_n (C_n being a multiplicative cyclic group of order n).

We introduce a more general class of codes which we call Quasi abelian codes. A linear subspace of the group algebra $GL(q)\,G$ of a finite abelian group G over the finite field $GF(q)$ which is module over $GF(q)\,H$ for some subgroup H of G, is called a quasi abelian code in $GF(q)\,G$. It is shown that a quasi

* This paper was presented at the Conference of General Algebra held at the University of Delhi in March, 1976.

abelian code can be regarded as a direct sum of abelian codes, in particular, a quasi abelian code in $GF(q)G$ with respect to a cyclic subgroup H of G is a quasi cyclic code. Direct sum of codes are considered and it is shown that under certain conditions product of two linear codes which are direct sum of linear quasi cyclic codes is also a direct sum of quasi cyclic codes.

2. Quasi abelian codes

Let G be a finite abelian group of order n.

Let $F=GF(q)$ be a finite field with $(n, q)=1$, so that the group algebra FG is semi-simple.

Definition 1: — A linear subspace A, of the group algebra FG such that A is FH-module (the defining map $FHXA \to A$, being the multiplication in FG), for some subgroup H of G, is called a quasi abelian code.

Example: — Let $F=GF(2)$ and let $C_9=<a>$ be a multiplicative cyclic group of order 9 with a as its generator.

Let $A=\{0,\ a^2+a^4+a^6,\ 1+a^5+a^7,\ a+a^3+a^8,$

$1+a+a^3+a^5+a^7+a^8,\ 1+a^2+a^4+a^5+a^6+a^7,$

$a+a^2+a^3+a^4+a^6+a^8,\ 1+a+a^2+a^3+a^4+a^5+a^6+a^7+a^8\}$

It is easy to check that the subspace A of FC_9 is not an ideal in FC_9 but is FH-module, where $H=\{1,\ a^3,\ a^6\}$ is a subgroup of C_9.

Thus, A is a quasi abelian code in FC_9 with respect to a subgroup H but it is not an abelian code. In fact, A is a (9,3) quasi cyclic code with a generator matrix

$$\begin{bmatrix} 001 & 010 & 100 \\ 100 & 001 & 010 \\ 010 & 100 & 001 \end{bmatrix}$$

Definition 2: — A linear code $\mathcal{C}$ of block length n over F whose coordinates are numbered with the elements of the group G, is called a G—H code over F if the mapping

$$h: x \to h \cdot x \qquad (x \in G)$$

for every h in a subgroup H of G, acting as a permutation on the coordinates of the code transforms any codeword into another codeword in $\mathcal{C}$. In case $H=G$, then the G—H code is simply G-code (Delsarte 1970).

Theorem 1: — *There is one-one correspodence between G—H codes over F and the quasi abelian codes in FG with respect to the subgroup H of G.*

Proof; — Let $\mathcal{C}$ be a linear code, of block length n over F, whose coordinates are numbered with the elements of G (order of G being n)

The mapping

$$f: a=(a(g_1), \ldots . a(g_n)) \in F^n \to a=\sum_{g \in G=\{g_1, \ldots, g_n\}} ga(g) \in FG$$

is an isomorphism between vector spaces F^n and FG. Let $f(\mathcal{C})=A$.

If $\mathcal{C}$ is a G—H code over F then

$$a\in\mathcal{C}\Rightarrow h(a)=(a(h^{-1}g_1),\ldots.\ a(h^{-1}g_n))\in\mathcal{C},\ \text{for every } h\in H$$

That is, $a=\sum_{g\in G} g\,a(g)\in A\Rightarrow h(a)=\sum_{g\in G_1} g\,a(h^{-1}g)=ha\in A$, for every h in H.

Therefore, A is a FH-module and hence, A is quasi abelian code in FG with respect to the subgroup H of G.

Corollary: — *There is one-one correspondence between G-codes over F and abelian codes i.e., ideals in the group algebra FG.*

3. Direct sums

Let $M_1,\ldots.\ M_p$ be submodules of an R-module (R, an arbitrary ring with unity).

We write, $M=M_1\oplus\cdots\oplus M_p$

and call M the internal direct sum of $M_1,\ldots.\ M_p$ if

(i) $M=M_1+\cdots+M_p$

and

(ii) $m_1+\cdots+m_p=0$, $m_i\in M_i$ implies that each $m_i=0$.

If M is the internal direct sum of $M_1,\ldots.\ M_p$, M is isomorphic to the set of p-tuples $(m_1,\ldots.\ m_p)$, $m_i\in M_i$ with componentwise addition and module multiplication $r(m_1,\ldots.\ m_p)=(rm_1,\ldots.\ rm_p)$, $r\in R$. Now, let $M_1,\ldots.\ M_p$ be given set of R-modules, their external sum

$$M=M_1\pm,\ldots,\pm M_p$$

is the set of all p-tuples $(m_1,\ldots.,m_p)$, $m_i\in M_i$ where addition is performed componentwise and $r(m_1,\ldots.,m_p)=(rm_1,\ldots.,rm_p)$, $r\in R$.

Let $M_i'=\{(0,0,\ldots,m_i,\ldots,0)\mid m_i\in M_i\}$ then $M_i'\cong M_i$ and M_i' is a submodule of M. In fact,

$$M_1\pm M_2\pm,\ldots\pm M_p=M_1'\oplus M_2'\oplus,\ldots.\oplus M_p'$$

It is easy to check that there is one-one correspondence between the representations of the group G and FG-modules. An irreducible module is one that contains no nontrivial submodules and an irreducible representation of the group G is one such that its representation space contains no proper invariant subspace. Also, irreducible module over FG corresponds to an irreducible representation of G over F and every representation can be expressed as a direct sum of irreducible representation. Thus, every quasi abelian code is a direct sum of irreducible modules.

Theorem 2: — *Every quasi abelian code is a direct sum of abelian codes.*

Proof: — Let A be a quasi abelian code in FG with respect to a subgroup H of G.

Let $o(G)=n$, $o(H)=r$ and $pr=n$

Let $H=\{h_1,\ldots.,h_r\}$ and $g_1H,\ldots.,g_pH$ be the cosets of G with regard to the subgroup $H(g_i\in G,\ i=1,\ldots p\ \&\ g_1=1)$.

Let the coordinate places in FG be arranged in the order

$$g_1 h_1, \ldots, g_1 h_r, \ldots, \ldots, \ldots g_p h_1, \ldots g_p h_r$$

We regard the code A to consist of p blocks each of length equal to r. Let A_i be the part of A which lies in the coordinate places $g_i h_1, \ldots\ldots, g_i h_r$.

Each A_i as a linear code over F. $(i = 1, \ldots, p)$

Since A is a quasi abelian code in FG with respect to the subgroup H of G, therefore, A can be regarded as a G—H code over F.

Therefore, $a = (a(g_1 h_1), \ldots., a(g_1 h_r), \ldots\ldots\ldots, a(g_p h_1), \ldots a(g_p h_r)) \in A$ implies that $h(a) = (a(h^{-1} g_1 h_1), \ldots, a(h^{-1} g_1 h_r), \ldots\ldots, a(h^{-1} g_p h_1), \ldots, a(h^{-1} g_p h_r)) \in A$ for every h in H.

Thus, $a_i \in A_i$ implies that $ha_i \in A_i$ for every $h \in H$.

Therefore, A_i is an ideal in the group algebra FH and hence is an abelian code.

Now, every vector a in A is a p-tuple $(a_1, \ldots\ldots, a_p)$ such that $a_i \in A_i$.

Hence, the qausi abelian code A is the direct sum of abelian codes A_i 's, $i = 1, \ldots, p$.

Corollary: — *Every quasi abelian code in the group algebra FG with respect to a cyclic subgroup of G is quasi cyclic code over F.*

Proof: — Bu the above theorem if A is a quasi abelian code in FG with respect to a subgroup H, then A is the direct sum of abelian codes (ideals) in FH.

Now, if H is a cyclic subgroup then every ideal A_i in FH is a cyclic code.

Also, $A_i = g_i A_1$ for $i = 2, \ldots, p$.

Therefore, the code A is a direct sum of p copies of a cyclic code A_1 and hence is quasi cyclic code.

Burton & Weldon (1965) have shown that product of two cyclic codes of relatively prime length is also cyclic code. Thus they have established that product cyclic codes offer a compromise between good random error correcting codes and good burst error correcting codes. We will now consider the product of codes which are themselves direct sum of quasi cyclic codes.

By an r-quasi cyclic code we shall mean a linear code in which every code word shifted by r-digits is also a code word.

Lemma: — *If A is r-quasi cyclic code of length* n_1 *and B is* r_2*-quasi cyclic code of length* n_2 *then the product AB is* $r_1 r_2$*-quasi cyclic code provided* $(n_1, n_2) = 1$, (n_1, n_2) *being the greatest common divisor of* n_1, n_2.

Proof: — Since $(n_1, n_2) = 1$, therefore we can choose integers a and b such that

$$an_1 + bn_2 = 1 \pmod{n_1 n_2}$$

We arrange the elements of the product code AB, which is of length $n_1 n_2$, as $n_1 \times n_2$ arrays with the rows as vectors in B and columns as vectors in A.

We define a correspondence f between the elements of $n_1 \times n_2$ array and the coordinates of a codeword in a code $\mathcal{C}$ of length $n_1 n_2$ by relating the

element of index (i_1, i_2) in the array with a coordinate of index i of a codeword in $\mathcal{C}$ given by

$$f(i_1, i_2) = i = i_1 r_2 (bn_2) + i_2 r_1 (an_1) \qquad (\text{mod } n_1 n_2)$$

Since A is r_1-quasi cyclic and B r_2-quasi cyclic therefore the correspondence

$$(i_1, i_2) \longrightarrow (i_1 + r_1,\ i_2 + r_2)$$

in the indeces of $n_1 \times n_2$ array corresponding to a codeword in AB gives an array corresponding to another codeword in AB.

Now

$$\begin{aligned} f(i_1 + r_1,\ i_2 + r_2) &= (i_1 + r_1) r_2 (bn_2) + (i_2 + r_2) r_1 (an_1) \ (\text{mod } n_1 n_2) \\ &= i_1 r_2 (bn_2) + i_2 r_1 (an_2) + r_1 r_2 (bn_2 + an_1) \ (\text{mod } n_1 n_2) \\ &= i + r_1 r_2 \ (\text{mod } n_1 n_2). \end{aligned}$$

Thus f relates the elements of $n_1 \times n_2$ array corresponding to a codeword in AB to the coordinates of a codeword in $r_1 r_2$-quasi cyclic code $\mathcal{C}$ of length $n_1 n_2$.

Hence the product code AB is equivalent to $r_1 r_2$-quasi cyclic code $\mathcal{C}$ of length $n_1 n_2$.

Theorem 3: — *Let A_i $(i = 1, \ldots, p)$ be (n_i, k_i) quasi cyclic codes and B_j $(j = 1, \ldots, r)$ be (n_j', n_j') quasi cyclic codes over F with $(n_i, n_j') = 1$. Then, the product of the direct sums $A = \sum_{i=1}^{p} \oplus A_i$ and $B = \sum_{j=1}^{r} \oplus B_j$ is also a direct sum of quasi cyclic codes over F.*

Proof: — Let G_i be the generator matrix of A_i and G_j' be the generator matrix of B_j.

Let G and G' be the generator matrices of A and B respectively, then

$$G = \sum_{i=1}^{p} \oplus G_i$$

$$\text{and } G' = \sum_{j=1}^{r} \oplus G_j'$$

Since, $(n_i, n_j') = 1$, therefore, by the above lemma, the product code $A_i B_j$ is quasi cyclic and its generator matrix is the tensor product $G_i \otimes G_j'$.

Also, the generator matrix of the product code AB is $G \otimes G'$.

Since, the tensor product of matrices is distributive over the direct sum, therefore,

$$G \otimes G' = \sum_{i,j} \oplus (G_i \otimes G_j').$$

Thus, the product code $AB = \sum_{i,j} \oplus A_i B_j$ is the direct sum of quasi cyclic codes.

Acknowledgement

The author is very grateful to Dr. B. D. Sharma and Dr. Ravinder Kumar of the University of Delhi for their help.

REFERENCES

[1] Berman, S. D. (1967), *Semi simple cyclic and abelian codes*, Kibernetika 3,3, 21—30.

[2] Burton, H. O. and Weldon, E. J; Jr. (1965). *Cyclic product codes*, IEEE Trans. Information Theory, IT-11, 3, 433—439.

[3] Camion, P. (1970). *Abelian codes*, Inst. of Statist. Mimeo. Ser. 600, 32 Univ. of of North Carolina.

[4] Chen, C. L., Peterson, W. W., and Weldon, E. J. Jr. (1969), *Some results on quasi cyclic codes*, Information and Control 15, 407—423.

[5] Delsarte, P. (1970), *Automorphisms of abelian codes*, Phillips Res. Rep. 25, 389—403.

[6] Mac Williams, F. J., (1970), *Abelian group codes*, Bell System Tech. Journal 49, 6, 987—1011.