Serdica
Bulgariacae mathematicae publicationes

Сердика
Българско математическо списание

WEAK CYCLIC CODES

B. D. SHARMA, SIRI KRISHAN WASAN

We introduce a class of weak cyclic codes which have cyclic structure not over the whole word length but over its different parts which are assumed to be of equal length. It is shown that an abelian code can be regarded as a weak cyclic code. It is shown that weak cyclic codes of special type occur as subcodes of arithmetic codes. Product of weak cyclic codes is considered and a product different from Elia's product is defined for quasi cyclic codes of constant rate and it is shown that under this product the product of quasi cyclic codes of constant rate is also quasi cyclic code of the same rate.

1. Introduction. Cyclic codes are easy to implement and have the added advantage of possessing simple algebraic proporties. However, only one set of shift registers can be employod for their implementation and the decoding again is to be handled by taking the whole of the codeword. This is somewhat restrictive.

In practice what might sometimes be more suitable is to devise our system in such a way that different parts are separately dealt with and synchronized for communication. This puts us in a comfortable position with respect to decoding also where different parts of a received vector can also be independently decoded with possible different objectives. Such a situation demands that we regard codewords as composed of different parts, each having its own structure.

Cyclic codes can be defined as ideals in a group algebra of a cyclic group over a finite field. Abelian codes which are ideals in the group algebra of a finite abelian group over a finite field are a natural generalization (Berman [1], Delsarte [2] and Mac-William [3]).

Wasan introduced a more general class of codes called quasi-abelian codes. A quasi-abelian code is defined as a linear sub-space of the group algebra $GF(q)G$, which is a $GF(q)H$-module for a subgroup H of the finite abelian group G. It is shown that a quasi-abelian code can be regarded as a direct sum of abelian codes (Wasan [4]).

In this paper we study a special class of codes which are subcodes of direct sum of cyclic codes. We call them weak-cyclic codes and they possess cyclic structure not over the whole word length cut over its different parts which are here considered to be of equal length. It is easy to see that an abelian code can be regarded as a weak-cyclic code. It is shown that weak-cyclic codes occur as subcodes of arithmetic codes. A notion of weak-circulant and weak-quasi cyclic code is also introduced. Product of weak-cyclic codes is considered and a product different from Elia's product is considered for quasi cyclic codes of constant rate.

2. Weak-cyclic codes. In defining this class of codes we would like to have that cyclic structure is not over the whole word length but over its different

SERDICA Bulgaricae mathematicae publicationes. Vol. 5, 1979, p. 321—326.

parts which are here considered to be of equal length. To be precise we have the following definition:

Definition. *A linear code A of block length $n=pr$ is called n/r-weak cyclic if*

$$(a_1, \ldots, a_r, a_{r+1}, \ldots, a_{2r}, \ldots \quad \ldots a_{(p-1)r+1}, \ldots, a_{pr}) \in A$$
$$\Longrightarrow (a_r, a_1, \ldots, a_{r-1}, \ldots, a_{2r}, a_{r+1}, \ldots, a_{2r-1}, \ldots, a_{pr}, \ldots, a_{pr-1}) \in A.$$

Example 1. The code generated by the matrix

$$G = \begin{bmatrix} 00001 & 00010 & 00100 & 01000 & 10000 \\ 10000 & 00001 & 00010 & 00100 & 01000 \\ 01000 & 10000 & 00001 & 00010 & 00100 \\ 00100 & 01000 & 10000 & 00001 & 00010 \\ 00010 & 00100 & 01000 & 10000 & 00001 \end{bmatrix}$$

is 25/5-weak cyclic code which is also a quasi cyclic code.

Example 2. The r-th order Reed Muller code of block length $n=2^m$ with $r=1$ and $m=3$ is 8/4-weak cyclic code.

Example 3. The linear code, generated by the matrix $G=(C_1, C_2, \ldots, C_r)$, where each C_i $(i=1, \ldots, r)$ is $r\times r$ circulant matrix over $GF(q)$ and the j-th row of C_i is $(j-1)$-th row of C_{i-1}, is r^2/r-weak cyclic.

2.1. Arithmetic codes. An arithmetic code is a code in which the coded form of the number N is the n-digit radix-r representation of AN, where A is constant. These codes have an interesting analogy with cyclic codes. For any number A, such that $(r, A)=1$, there exists a smallest number n such that r^n-1 is divisible by A. If n is taken as the number of digits in a codeword then every cyclic shift of codewords is also a codeword.

The following theorem will show that some weak cyclic codes are subcodes of arithmetic codes.

Theorem 1. *Suppose A is a constant such that $(r, A)=1$ and $n=mk$ is the smallest integer such that r^n-1 is divisible by A. If any row-vector of a matrix $G=(C, C, \ldots, C)_{k\times n}$, ($C$ is some $k\times k$ circulant matrix) is a codeword of the arithmetic code AN then every other row of G is also a codeword of AN.*

Proof. Let $(a_{k-1}, a_{k-2}, \ldots, a_0)$ be a row of the circulant matrix C such that the number

$$M = a_{k-1} r^{mk-1} + a_{k-2} r^{mk-2} + \cdots + a_0 r^{(m-1)k} + a_{k-1} r^{(m-1)k-1} + \cdots + a_0 r^{(m-2)k} + \cdots + a_{k-1} r^{k-1} + a_{k-2} + \cdots + a_0$$

is divisible by A. Then

$$a_{k-2} r^{mk-1} + a_{k-3} r^{mk-2} + \cdots + a_0 r^{(m-1)k+1} + a_{k-1} r^{(m-1)k} + a_{k-2} r^{(m-1)k-1} + \cdots + a_0 r^{(m-2)k+1} + a_{k-1} r^{(m-2)k} + \cdots + a_{k-2} r^{k-1} + a_{k-3} r^{k-2} + \cdots + a_0 r + a_{k-1}$$
$$= rM - (a_{k-1} r^{mk} + a_{k-1} r^{(m-1)k} + \cdots + a_{k-1} r^k) + a_{k-1} r^{(m-1)k} + a_{k-1} r^{(m-2)k} + \cdots + a_{k-1}$$
$$= rM - a_{k-1}(r^{mk}-1),$$

which is divisible by A.

Thus, if the row vector

$$(a_{k-1}, a_{k-2}, \ldots, a_0, \ldots, a_{k-1}, a_{k-2}, \ldots, a_0)$$

of the matrix G, is a codeword of the code AN then the vector

$$(a_{k-2}, a_{k-3}, \ldots, a_{k-1}, \ldots, a_{k-2}, a_{k-3}, \ldots, a_{k-1})$$

is also a codeword of AN. Hence the theorem.

The above theorem shows that if $(r, A)=1$ then the weak cyclic code generated by the matrix $G=(C, C, \ldots, C)$ is a subcode of the arithmetic code AN provided the digits of a row of G are the digits in the n-digit radix-r representation of a number divisible by A provided $n=mk$ is the smallest integer such that r^n-1 is divisible by A. For example, let $A=9$ and $r=2$ then 6 is the smallest number such that 9 divides 2^6-1 and the weak cyclic code over $GF(2)$, generated by

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

is subcode of the arithmetic code $9N$.

2.2. Abelian codes. Using Mac-William [3] technique we show that, an abelian code can be regarded as a weak cyclic code.

Theorem 2. *If A is an ideal (abelian code) in a group algebra KG of a finite abelian group G over a finite field K then for every prime number r dividing the order of G, A is n/r-weak cyclic code, n being the order of G.*

Proof. Let H be a cyclic subgroup of order r of the group G and let its elements be $h_1, h_2, \ldots, h_r$. Let $g_1H, g_2H, \ldots, g_mH$ $(mr=n)$ be all the cosets of G with respect to the subgroup H with $g_1=1 \in G$. We arrange the elements of G in the order $g_1h_1, \ldots, g_1h_r, g_2h_1, \ldots, g_2h_r, \ldots, g_mh_1, \ldots, g_mh_r$.

Let the coordinate places in KG be numbered with the elements in the above order. We can write an element in the group algebra KG as $\sum_{g \in G} ga(g)$ where $a(g) \in K$. Let an element a in the ideal A be written as

$$a=\sum_{i=1}^{m} g_i h_1 a(g_i h_1)+\cdots+g_i h_r a(g_i h_r).$$

Let

$$A_i=\left\{\sum_{j=1}^{r} g_i h_j a(g_i h_j) \,\middle|\, a \in A\right\}.$$

Since A is an ideal in KG, therefore, each A_i $(i=1, \ldots, m)$ is an ideal in KH.

Also, H being cyclic group each A_i $(i=1, \ldots, m)$ is a cyclic code. Thus,

$$\begin{aligned} &(a_1, \ldots, a_r, a_{r+1}, \ldots, a_{2r}, \ldots, a_{(m-1)r+1}, \ldots, a_{mr}) \in A \\ \Rightarrow\ &(a_{(i-1)r+1}, \ldots, a_{ir}) \in A_i \quad (i=1, \ldots, m) \\ \Rightarrow\ &(a_{ir}, \ldots, a_{ir-1}) \in A_i \qquad (\because A_i \text{ are cyclic}) \\ \Rightarrow\ &(a_r, a_1, \ldots, a_{r-1}, a_{2r}, \ldots, a_{2r-1}, \ldots, a_{mr}, a_{mr-1}) \in A. \end{aligned}$$

Hence A is n/r-weak cyclic code.

2.3. Weak quasi-cyclic codes. The extension of weak cyclic codes to weak quasi cyclic codes is analogous to that of the extension of cyclic codes to quasi cyclic codes.

Definition. *A linear code A of block length $n=pr$ is called $n/r-s$ weak quasi cyclic code $(s<r)$ if*

$$(a_1, \ldots, a_{r-(s-1)}, \ldots, a_r, \ldots, a_{(p-1)r+1}, \ldots, a_{pr-(s-1)}, \ldots, a_{pr}) \in A$$

$$\Rightarrow (a_{r-(s-1)}, \ldots, a_r, a_1, \ldots, a_{r-(s-2)}, \ldots, a_{pr-(s-1)}, \ldots, a_{pr}, \ldots, a_{pr-(s-2)}) \in A.$$

Circulant matrices have been used to study quasi cyclic codes. We now define weak circulant matrices which could be used to study weak quasi cyclic codes.

Definition. *A matrix in which every row shifted by s digits to the right, for some positive integer s, results in another row of the matrix is called a weak circulant matrix.*

We shall write a weak circulant matrix with n columns and in which rows preserve s shifts as n/s-weak circulant matrix.

Example. The linear code, generated by the matrix $G=(C_1, C_2, \ldots, C_r)$, where each C_i is r/s-weak circulant matrix over $GF(q)$ and j-th row of C_i is $(j-1)$-th row *pf* C_{i-1} $(i=1, \ldots, r)$, is r^2/r-s weak quasi cyclic code.

Theorem 3. *For some positive integers n and s with $s<n$, ann/s-weak. circulant matrix has $n/(n, s)$ distinct rows where (n, s) is the greatest common divisor of n and s.*

Proof. Let $v_1=(a_n, a_{n-1}, \ldots, a_s, \ldots, a_1)$ be the first row of an n/s-weak circulant matrix C. The other rows of A could be obtained by shifting v_1 to s digits to the right successively. Let v_i denotes the i-th row of A. In particular,

$$v_2=(a_s, \ldots, a_1, a_n, \ldots, a_{2s}, \ldots, a_{s+1}), v_3=(a_{2s}, \ldots, a_{s+1}, a_s, \ldots, a_1, a_n, \ldots, a_{2s+1})$$

If A has t distinct rows then $v_{t+1}=v_1$. This is true if $ts=0 \pmod n$. But $t=n/(n, s)$ is the least positive integer satisfying the above equation. Hence the theorem.

Corollary. *If $(n, s)=1$ then n/s-weak circulant matrix is circulant.*

3. Product codes. Wasan [4] has shown that the product of quasi cyclic codes of relatively prime lengths is also quasi cyclic code and the shift length preserved by the product code is the product of the shift lengths preserved by the subcodes. We prove a similar result for weak cyclic codes.

Theorem 4. *If A is n_1/r_1-weak cyclic code and B is n_2/r_2-weak cyclic code over $GF(q)$ then the product code AB is n_1n_2/r_1r_2-weak cyclic code over $GF(q)$ provided $(n_1, n_2)=1$.*

Proof. Let $n_1=p_1r_1$ and $n_2=p_2r_2$ with $(n_1, n_2)=1$ so that $(p_1, p_2)=1$ and $(r_1, r_2)=1$. We choose integers a and b such that $ap_1+bp_2=1 \pmod{p_1p_2}$ and integers c and d such that $cr_1+dr_2=1 \pmod{r_1r_2}$.

The product code AB is of block length $n_1n_2=p_1r_1p_2r_2$ and we can arrange its elements as $p_1r_1 \times p_2r_2$ arrays with rows as codewords in B and columns as codewords in A.

We regard a $p_1r_1 \times p_2r_2$ array as $p_1 \times p_2$ array of elements which are themselves $r_1 \times r_2$ arrays.

Since A is n_1/r_1-weak cyclic code therefore p_1 subblocks of A of length r_1 are cyclic. Similarly, p_2 subblocks of B of length r_2 are cyclic.

We regard an element of the product code AB as a $p_1 \times p_2$ array

$$\begin{bmatrix} C_{11}, \ldots, C_{1p_2} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \\ C_{p_1 1}, \ldots, C_{p_1 p_2} \end{bmatrix}, \tag{1}$$

where each C_{ij} $(i = 1, \ldots, p_1 \ \& \ j = 1, \ldots, p_2)$ is $r_1 \times r_2$ array whose rows are r_2-tuple belonging to the j-th cyclic subblock of the code B and the columns are r_1-tuple belonging to i-th cyclic subblock of the code A.

We can associate with every $r_1 \times r_2$ arrary C_{ij} a codeword of a cyclic code of block length $r_1 r_2$ by relating an element of index (l, m) of the array with the coordinate of index t of cyclic code of length $r_1 r_2$ given by

$$t = l(dr_2) + m(cr_1) \pmod{r_1 r_2}. \tag{2}$$

With $p_1 \times p_2$ array (1) a $p_1 p_2$-tuple of $r_1 \times r_2$ arrays by relating an element of index (i, j) of the array (1) with the coordinate of index k of $p_1 p_2$-tuple (of $r_1 \times r_2$ arrays) given by

$$k = i(bp_2) + j(ap_1) \pmod{p_1 p_2}. \tag{3}$$

The mapping $(i, j) \to k$ given by (3) associates a $p_1 r_1 \times p_2 r_2$ array corresponding to an element of the product code AB to a $p_1 p_2$-tuple of $r_1 \times r_2$ arrays and the mapping $(l, m) \to t$ given by (2) applied to the coordinates of this $p_1 p_2$-tuple ultimately associates the array representing an element of the product code AB to an $n_1 n_2 = p_1 p_2 r_1 r_2$-tuple, which is a codeword in an $n_1 n_2 / r_1 r_2$-weak cyclic code.

We now introduce another product for quasi cyclic codes of constant rate.

Definition. *Let A be (mr, mk) linear code and B be (nr, nk) linear code with their generator matrices*

$$G_1 = \begin{bmatrix} A_{11}, \ldots, A_{1r} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \\ A_{k1}, \ldots, A_{kr} \end{bmatrix} \quad \textit{and} \quad G_2 = \begin{bmatrix} B_{11}, \ldots, B_{1r} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \\ B_{k1}, \ldots, B_{kr} \end{bmatrix}$$

respectively, A_{ij} being $m \times m$ circulant matrices and B_{ij} being $n \times n$ circulant matrices.

The linear code $A * B$ with generator matrix

$$G_1 * G_2 = \begin{bmatrix} C_{11}, \ldots, C_{1r} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \\ C_{k1}, \ldots, C_{kr} \end{bmatrix}$$

(where $C_{ij} = A_{ij} * B_{ij}$ is the tensor product of A_{ij} and B_{ij}) is called the blockwise tensor product of A and B.

The generator matrix of an (mr, mk) quasi cyclic code of shift length r can be put in the form

$$G = \begin{bmatrix} A_{11}, \ldots, A_{1r} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \\ A_{k1}, \ldots, A_{kr} \end{bmatrix},$$

where A_{ij} are $m \times m$ circulant matrices. Since the product of two quasi cyclic codes is again a quasi cyclic code, in particular, tensor product of two circulant matrices will be circulant, provided their block lengths are relatively prime. Hence we have the following theorem.

Theorem 5. *The blockwise tensor product of two quasi cyclic codes of constant rate and of relatively prime length is a quasi cyclic code of the same rate.*

REFERENCES

1. S. D. Berman. Semi simple cyclic and abelian codes. *Kibernetika*, **3**, 1967, No.3, 21—30.
2. P. Delsarte. Automorphisms of abelian codes. *Phillips Res. Rep.*, **25**, 1970, 389—403.
3. F. J. Mac William. Abelian group codes. *Bell System Tech. J.*, **49**, 1970, 987—1011.
4. Siri Krishan Wasan. Quasi abelian codes. *Publ. Inst. Math.*, **21**, 1977, 201—206.

Faculty of Mathematics
University of Delhi, Delhi

Department of Mathematics, Ramjas College
University of Delhi, Delhi

Received 4. 9. 1978