ГОДИШНИК НА СОФИЙСКИЯ УНИВЕРСИТЕТ „СВ. КЛИМЕНТ ОХРИДСКИ“

ФАКУЛТЕТ ПО МАТЕМАТИКА И ИНФОРМАТИКА
Том 98

ANNUAIRE DE L'UNIVERSITE DE SOFIA „ST. KLIMENT OHRIDSKI“

FACULTE DE MATHEMATIQUES ET INFORMATIQUE
Tome 98

CYCLIC CODES AS INVARIANT SUBSPACES

DIANA RADKOVA, ASEN BOJILOV

The description of the linear cyclic codes as ideals in the algebra $\mathfrak{F}_n = F[x]/(x^n - 1)$, where F is a finite field, is well known in the coding theory. The map cyclic shift is a linear operator in F^n. Our aim is to consider a new method of describing the cyclic codes as invariant subspaces of F^n regarding this operator.

Keywords: Cyclic codes, invariant subspaces.

2000 MSC: main 94B15, secondary 47A15

1. INTRODUCTION

The linear cyclic codes are traditionally described using the methods of the commutative algebra (see [2] and [3]). Since the linear codes have the structure of linear subspaces of F^n, the description of the linear cyclic codes in terms of the linear algebra is natural.

The main purpose of this paper is to study some properties of the cyclic codes as invariant linear subspaces. Some generalizations for consta-cyclic codes are considered.

2. SOME LINEAR ALGEBRA

Let $F = \mathrm{GF}(q)$ and let F^n be the n-dimensional vector space over F with standard basis $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 1)$.

Let

$$\varphi : \begin{cases} F^n \to F^n \\ (x_1, x_2, \dots, x_n) \mapsto (x_n, x_1, \dots, x_{n-1}) \end{cases}.$$

Then $\varphi \in \operatorname{Hom} F^n$ and has the following matrix

$$A = \begin{pmatrix} 0\,0\,0 \dots 1 \\ 1\,0\,0 \dots 0 \\ 0\,1\,0 \dots 0 \\ \vdots\ \vdots\ \vdots\ \ddots\ \vdots \\ 0\,0\,0 \dots 0 \end{pmatrix}$$

in the basis $e_1, e_2, \dots, e_n$. Note that $A^t = A^{-1}$ and $A^n = E$. The characteristic polynomial of A is

$$f_A(x) = \begin{vmatrix} -x & 0 & 0 & \dots & 1 \\ 1 & -x & 0 & \dots & 0 \\ 0 & 1 & -x & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & -x \end{vmatrix} = (-1)^n(x^n - 1).$$

Let us denote it by $f(x)$.

We show the following well known fact.

Proposition 2.1. *Let U be a φ-invariant subspace of V and $\dim_F V = n$. Then $f_{\varphi|_U}(x)$ divides $f_\varphi(x)$. In particular, if $V = U \oplus W$ and W is φ-invariant subspace of F^n then $f_\varphi(x) = f_{\varphi|_U}(x) f_{\varphi|_W}(x)$.*

Proof: Let $\dim_F U = k$ and let $g_1, \dots, g_k$ be a basis of U over F. We complement this basis to a basis $g_1, \dots, g_k, g_{k+1}, \dots, g_n$ of V. Then the coordinates of the vectors $\varphi(g_1), \dots, \varphi(g_k)$ from the $(k+1)$-th vanish and hence in this basis φ has the matrix

$$A' = \begin{pmatrix} \alpha_{11} \dots \alpha_{1k} & \alpha_{1,k+1} & \dots & \alpha_{1n} \\ \dots\dots\dots\dots & & & \\ \alpha_{k1} \dots \alpha_{kk} & \alpha_{k,k+1} & \dots & \alpha_{kn} \\ 0 \ \dots \ 0 & \alpha_{k+1,k+1} & \dots & \alpha_{k+1,n} \\ \dots\dots\dots\dots & & & \\ 0 \ \dots \ 0 & \alpha_{n,k+1} & \dots & \alpha_{n,n} \end{pmatrix} = \begin{pmatrix} A_1 & B \\ 0 & A_2 \end{pmatrix}.$$

The matrix $A_1 = \begin{pmatrix} \alpha_{11} \dots \alpha_{1k} \\ \dots\dots\dots \\ \alpha_{k1} \dots \alpha_{kk} \end{pmatrix}$ is obviously the matrix of φ in $g_1, \dots, g_k$. Then

$$f_\varphi(x) = \det(A' - xE) = \det \begin{pmatrix} A_1 - xE & B \\ 0 & A_2 - xE \end{pmatrix} =$$

$$= f_{\varphi|_U}(x) \det(A_2 - xE). \qquad \square$$

Let m be the multiplicative order of q modulo n, i.e., m is the smallest natural number with the property that n divides $q^m - 1$. Then $\mathrm{GF}(q^m)$ is the splitting field of $f(x)$ over F. Let $f(x) = (-1)^n f_1(x) \dots f_t(x)$ be the factorization of $f(x)$ into irreducible factors. We assume that $(n, q) = 1$. In that case $f(x)$ has distinct factors $f_i(x),\ i = 1, \dots, t$, which are monic.

Let denote by U_i the space of the solutions of the homogeneous system with matrix $f_i(A)$ for each $i = 1, \dots, t$, i.e., $U_i = \operatorname{Ker} f_i(\varphi)$.

Theorem 2.1. *The subspaces U_i of F^n satisfy the following conditions:*

1) *U_i is a φ-invariant subspace of F^n;*

2) $F^n = U_1 \oplus \dots \oplus U_t$;

3) $\dim U_i = \deg f_i = k_i$;

4) $f_{\varphi|_{U_i}}(x) = (-1)^{k_i} f_i(x)$;

5) *U_i is a minimal φ-invariant subspace of F^n.*

Proof: 1) Let $u \in U_i$, i.e., $f_i(A)u = \mathbf{0}$. Then $f_i(A)\varphi(u) = f_i(A)Au = Af_i(A)u = \mathbf{0}$, so that $\varphi(u) \in U_i$.

2) Let $\hat{f}_i(x) = \frac{f(x)}{f_i(x)}$ for $i = 1, \dots, t$. Since $(\hat{f}_1(x), \dots, \hat{f}_t(x)) = 1$, by the Euclidean algorithm there are polynomials $a_1(x), \dots, a_t(x) \in F[x]$ such that

$$a_1(x)\hat{f}_1(x) + \dots + a_t(x)\hat{f}_t(x) = 1.$$

Then for every vector $v \in V$ the condition $v = a_1(A)\hat{f}_1(A)v + \dots + a_t(A)\hat{f}_t(A)v$ holds. Let $v_i = a_i(A)\hat{f}_i(A)v$. Then $f_i(A)v_i = a_i(A)f(A)v = \mathbf{0}$ so that $v_i \in U_i$. Hence

$$F^n = U_1 + \dots + U_t.$$

Assume that $v \in U_i \cap \sum_{j \neq i} U_j$, then $f_i(A)v = \mathbf{0}$, $\hat{f}_i(A)v = \mathbf{0}$. Since $(f_i, \hat{f}_i) = 1$, there are polynomials $a(x), b(x) \in F[x]$, such that $a(x)f_i(x) + b(x)\hat{f}_i(x) = 1$. Hence $a(A)f_i(A)v + b(A)\hat{f}_i(A)v = v = \mathbf{0}$, so that $U_i \cap \sum_{j \neq i} U_j = \{\mathbf{0}\}$. Thus

$$F^n = U_1 \oplus \dots \oplus U_t.$$

3) Let $g \in U_i$ be an arbitrary nonzero vector and let $k \geq 1$ be the smallest natural number with the property that the vectors $g, \varphi(g), \dots, \varphi^{k-1}(g)$ are linearly independent. Then there are elements $c_0, \dots, c_{k-1} \in F$, at least one of which is nonzero, such that

$$\varphi^k(g) = c_0 g + c_1\varphi(g) + \dots + c_{k-1}\varphi^{k-1}(g).$$

Consider the polynomial $t(x) = x^k - c_{k-1}x^{k-1} - \dots - c_0 \in F[x]$. Since $(t(\varphi))(g) = (f_i(\varphi))(g) = \mathbf{0}$, it follows that $[(t(x), f_i(x))(\varphi)](g) = \mathbf{0}$. But $(t(x), f_i(x))$ is 1 or $f_i(x)$. Hence $(t(x), f_i(x)) = f_i(x)$ and $f_i(x)$ divides $t(x)$. Thus $k_i = \deg f_i(x) \leq$

$\deg t(x) = k$. On the other hand, the vectors $g, \varphi(g), \dots, \varphi^{k_i}(g)$ are linearly dependent, since $(f_i(\varphi))(g) = \mathbf{0}$, and from the minimality of k we obtain $k = k_i$. Then $\dim U_i \geq k_i$. Therefore

$$n = \dim{}_F F^n = \sum_{i=1}^{t} \dim{}_F U_i \geq \sum_{i=1}^{t} k_i = \sum_{i=1}^{t} \deg f_i = \deg f = n$$

and $\dim{}_F U_i = k_i$.

4) Let $g_1^{(i)}, \dots, g_{k_i}^{(i)}$ be a basis of U_i over F, $i = 1, \dots, t$, and let A_i be the matrix of $\varphi|_{U_i}$ in that basis. Let $\tilde{f}_i = f_{\varphi|_{U_i}}$. Suppose $(\tilde{f}_i, f_i) = 1$. Hence there are polynomials $a(x), b(x) \in F[x]$, such that $a(x)\tilde{f}_i(x) + b(x)f_i(x) = 1$. Then $a(A_i)\tilde{f}_i(A_i) + b(A_i)f_i(A_i) = E$. Therefore $b(A_i)f_i(A_i) = E$. We will show that $f_i(A_i) = \mathbf{0}$, which contradicts the last equation.

By the property 2) we obtain that $g_1^{(1)}, \dots, g_{k_1}^{(1)}, \dots, g_1^{(t)}, \dots, g_{k_t}^{(t)}$ is the basis of F^n and the matrix of φ in that basis is

$$A' = \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_t \end{pmatrix}.$$

Beside this $A' = T^{-1}AT$, where T is the change basis matrix from the standard basis of F^n to that one. Then

$$f_i(A') = \begin{pmatrix} f_i(A_1) & & & \\ & f_i(A_2) & & \\ & & \ddots & \\ & & & f_i(A_t) \end{pmatrix} = f_i(T^{-1}AT) = T^{-1}f_i(A)T.$$

Let $g_j^{(i)} = \lambda_{j1}^{(i)}e_1 + \dots + \lambda_{j\,n}^{(i)}e_n$, $j = 1, \dots, k_i$. Since $g_j^{(i)} \in U_i$, we obtain

$$f_i(A') \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} = T^{-1}f_i(A)T \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} = T^{-1}f_i(A) \begin{pmatrix} \lambda_{j1}^{(i)} \\ \vdots \\ \lambda_{j\,n}^{(i)} \end{pmatrix} = \mathbf{0},$$

where 1 is on the $(k_1 + \dots + k_{i-1} + j)-$th position. According to the last equation, $f_i(A_i) = \mathbf{0}$. Therefore $(f_i, \tilde{f}_i) \neq 1$. Since f_i and $\tilde{f}_i$ are polynomials of the same degree k_i and f_i is monic and irreducible, we obtain $\tilde{f}_i = (-1)^{k_i} f_i$.

5) Let $\{\mathbf{0}\} \neq U \subseteq U_i$. Then by Proposition 2.1 we obtain $f_{\varphi|_U}$ divides f_i. Since the polynomial f_i is irreducible, $\dim{}_F U = \dim{}_F U_i$ and $U = U_i$. □

Proposition 2.2. *Let U be a $\varphi-$invariant subspace of F^n. Then U is a direct sum of some minimal $\varphi-$invariant subspaces U_i of F^n.*

Proof: Let $\widetilde{U}_i = U \cap U_i$, $i = 1, \dots, t$. Then $\widetilde{U}_i$ is $\{\mathbf{0}\}$ or U_i, since U_i are minimal. Therefore

$$U = U \cap F^n = U \cap (U_1 \oplus \cdots \oplus U_t) = \widetilde{U}_1 \oplus \cdots \oplus \widetilde{U}_t = \bigoplus_{U_i \leq U} U_i. \qquad \square$$

3. LINEAR CYCLIC CODES

Definition 3.1. A code C with length n over F is called cyclic, if whenever $x = (c_1, c_2, \dots, c_n)$ is in C, so is its cycle shift $y = (c_n, c_1, \dots, c_{n-1})$.

The following statement is clear from the definitions.

Proposition 3.1. *A linear code C with length n over F is cyclic iff C is a $\varphi-$invariant subspace of F^n.*

Theorem 3.1. *Let C be a linear cyclic code with length n over F. Then the following facts hold.*

1) $C = U_{i_1} \oplus \cdots \oplus U_{i_s}$ *for some minimal $\varphi-$invariant subspaces U_{i_r} of F^n and* $\dim_F C = k_{i_1} + \cdots + k_{i_s} = k$;

2) $f_{\varphi|_C}(x) = (-1)^k f_{i_1}(x) \dots f_{i_s}(x) = g(x)$;

3) $c \in C$ *iff* $g(A)c = \mathbf{0}$;

4) *the polynomial $g(x)$ has the smallest degree with the property* 3;

5) $\mathrm{r}\,(g(A)) = n - k$.

Proof: 1) This follows from Proposition 2.2.

2) Let $g_1^{(i_r)}, \dots, g_{k_{i_r}}^{(i_r)}$ be a basis of U_{i_r} over F, $r = 1, \dots, s$. Then $g_1^{(i_1)}, \dots, g_{k_{i_1}}^{(i_1)}, \dots, g_1^{(i_s)}, \dots, g_{k_{i_s}}^{(i_s)}$ is a basis of C over F and $\varphi|_C$ has a matrix

$$\begin{pmatrix} A_{i_1} & & & \\ & A_{i_2} & & \\ & & \ddots & \\ & & & A_{i_s} \end{pmatrix}$$

in that basis. Hence

$$f_{\varphi|_C}(x) = \tilde{f}_{i_1}(x) \dots \tilde{f}_{i_s}(x) = (-1)^{k_{i_1} + \cdots + k_{i_s}} f_{i_1}(x) \dots f_{i_s}(x).$$

Note that A_{i_r} and $\tilde{f}_{i_r}(x)$ are defined as in Theorem 2.1.

3) Let $c \in C$. Then $c = u_{i_1} + \cdots + u_{i_s}$ for some $u_{i_r} \in U_{i_r}$, $r = 1, \dots, s$ and $g(A)c = (-1)^k[(f_{i_1} \dots f_{i_s})(A)u_{i_1} + \cdots + (f_{i_1} \dots f_{i_s})(A)u_{i_s}] = \mathbf{0}$.

Conversely, suppose $g(A)c = \mathbf{0}$ for some $c \in F^n$ and let $c = u_1 + \cdots + u_t$, $u_i \in U_i$. Then $g(A)c = (-1)^k[(f_{i_1} \dots f_{i_s})(A)u_1 + \cdots + (f_{i_1} \dots f_{i_s})(A)u_t] = \mathbf{0}$, so that $g(A)[u_{j_1} + \cdots + u_{j_l}] = \mathbf{0}$, where $\{j_1, \dots j_l\} = \{1, \dots, t\} \backslash \{i_1, \dots, i_s\}$. Let $v = u_{j_1} + \cdots + u_{j_l}$ and

$$h(x) = \frac{(-1)^n[x^n - 1]}{g(x)} = \frac{f(x)}{g(x)}.$$

Since $(h(x), g(x)) = 1$, there are polynomials $a(x)$, $b(x) \in F[x]$ such that $a(x)h(x) + b(x)g(x) = 1$. Hence $a(A)h(A)v + b(A)g(A)v = v = \mathbf{0}$ and $c = u_{i_1} + \cdots + u_{i_s} \in C$.

4) Suppose $b(x) \in F[x]$ is a nonzero polynomial of smallest degree such that $b(A)c = \mathbf{0}$ for all $c \in C$. By the division algorithm in $F[x]$ there are polynomials $q(x), r(x)$ such that $g(x) = b(x)q(x) + r(x)$, where $\deg r(x) < \deg b(x)$. Then for each vector $c \in C$ we have $g(A)c = q(A)b(A)c + r(A)c$ and hence $r(A)c = \mathbf{0}$. But this contradicts the choice of $b(x)$ unless $r(x)$ is identically zero. Thus, $b(x)$ divides $g(x)$. If $\deg b(x) < \deg g(x)$, then $b(x)$ is a product of some of the irreducible factors of $g(x)$ and without loss of generality we can suppose $b(x) = (-1)^{k_{i_1} + \cdots + k_{i_q}} f_{i_1} \dots f_{i_q}$ and $q < s$. Let us consider the code $C' = U_{i_1} \oplus \cdots \oplus U_{i_q} \subset C$. Then $b(x) = f_{\varphi|_{C'}}$ and by the equation $g(A)c = \mathbf{0}$ for all $c \in C$ we obtain $C \subseteq C'$. This contradiction proves the statement.

5) By the property 3) C is the space of the solutions of the homogeneous system with matrix $g(A)$. Then $\dim_F C = k = n - \mathrm{r}\,(g(A))$, which proves the statement.□

Definition 3.2. Let $x = (x_1, \dots, x_n)$ and $y = (y_1 \dots, y_n)$ be two vectors in F^n. We define an inner product over F by $\langle x, y \rangle = x_1y_1 + \cdots + x_ny_n$. If $\langle x, y \rangle = 0$, we say that x and y are orthogonal to each other.

Definition 3.3. Let C be a linear code over F. We define the dual of C (which is denoted by $C^\perp$) to be the set of all vectors which are orthogonal to all codewords in C, i.e.,

$$C^\perp = \{v \in F^n \mid \langle v, c \rangle = 0 \text{ for all} \, c \in C\}.$$

It is well known that if C is $k-$dimensional, then $C^\perp$ is $(n-k)-$dimensional.

Proposition 3.2. *The dual of a linear cyclic code is also cyclic.*

Proof: Let $h = (h_1, \dots, h_n) \in C^\perp$ and $c = (c_1, \dots, c_n) \in C$. We show that $\varphi(h) = (h_n, h_1, \dots, h_{n-1}) \in C^\perp$. We have

$$\langle \varphi(h), c \rangle = c_1h_n + \cdots + c_nh_{n-1} = \langle h, \varphi^{-1}(c) \rangle = \langle h, \varphi^{n-1}(c) \rangle = \mathbf{0},$$

which proves the statement. □

Proposition 3.3. *The matrix H, whose rows are arbitrary $n-k$ linear independent rows of $g(A)$, is a parity check matrix of C.*

Proof: The proof follows from the equation $g(A)c = \mathbf{0}$ for every vector $c \in C$ and the fact that $\mathrm{r}\,(g(A)) = n - k$. □

Let $g_{l_1}, \dots, g_{l_{n-k}}$ be a basis of $C^\perp$, where g_{l_r} is a l_r-th vector row of $g(A)$. By the equation $g(A)h(A) = \mathbf{0}$ we obtain that $\langle g_{l_r}, h_i \rangle = 0$ for each $i = 1, \dots, n$, $r =$

$1, \dots, n-k$. The last equation gives us that the columns h_i of $h(A)$ are codewords in C.

We show that $\mathrm{r}\,(h(A)) = k$. By Sylvester's inequality we obtain $\mathrm{r}\,(\mathbf{0}) = 0 \geq \mathrm{r}\,(g(A)) + \mathrm{r}\,(h(A)) - n$. Since $\mathrm{r}\,(h(A)) \leq n - \mathrm{r}\,(g(A)) = n-(n-k) = k$. On the other hand, Sylvester's inequality, applied to the product $h(A) = (-1)^{n-k} f_{j_1}(A) \dots f_{j_l}(A)$, gives $\mathrm{r}\,(h(A)) \geq r_{j_1} + \dots + r_{j_l} - n(l-1) = nl - k_{j_1} - \dots - k_{j_l} - nl + n = n - (k_{j_1} + \dots + k_{j_l}) = n - (n - k_{i_1} - \dots - k_{i_s}) = n - (n-k) = k$. Therefore $\mathrm{r}\,(h(A)) = k$. Thus we have proved the following:

Proposition 3.4. *The matrix G, whose rows are arbitrary k linear independent rows of $(h(A))^t$, is a generator matrix of the code C.*

Lemma 3.1. *If $g(x) \in F[x]$, then $g(A^{-1}) = g(A^t) = (g(A))^t$. In particular, if n divides* $\deg g(x)$, *then $g^*(A) = (g(A))^t$, where $g^*(x)$ is the reciprocal polynomial of $g(x)$.*

Proof: Let $g(x) = g_0 x^k + g_1 x^{k-1} + \dots + g_{k-1}x + g_k$, then $g(A) = g_0 A^k + g_1 A^{k-1} + \dots + g_{k-1}A + g_k E$. Transposing both sides of the last equation, we obtain $(g(A))^t = g_0 (A^k)^t + g_1 (A^{k-1})^t + \dots + g_{k-1} A^t + g_k E = g_0 (A^t)^k + g_1 (A^t)^{k-1} + \dots + g_{k-1} A^t + g_k E = g(A^t)$.

In particular, if $\deg g(x) = ns$ for some $s \in \mathbb{N}$, then $g^*(A) = A^{ns} g(A^{-1}) = A^{ns} g(A^t) = g(A^t) = (g(A))^t$. □

Let $f_{\varphi|_{C^\perp}}(x) = \tilde{h}$. By Theorem 3.1 it follows that $\tilde{h}$ is the polynomial of the smallest degree such that $\tilde{h}(A)u = \mathbf{0}$ for every $u \in C^\perp$. Let $h^*(x) = \tilde{h}(x)q(x) + r(x)$, where $\deg r(x) < \deg \tilde{h}(x)$. Then by Lemma 3.1 $h^*(A) = A^{n-k}(h(A))^t = \tilde{h}(A)q(A) + r(A)$, hence for every vector $u \in C^\perp$ the assertion $A^{n-k}(h(A))^t u = q(A)\tilde{h}(A)u + r(A)u$ holds, so that $r(x) = 0$. Thus $\tilde{h}(x)$ divides $h^*(x)$. Since both are polynomials of the same degree , $h^*(x) = a\tilde{h}(x)$, where $a \in F$ is the leading coefficient of the product $f^*_{j_1}(x) \dots f^*_{j_l}(x)$. Thus

$$\tilde{h} = \frac{1}{a} h^* = (-1)^{n-k} \frac{1}{a} f^*_{j_1} \dots f^*_{j_l} = \prod_{r=1}^{l} \frac{1}{a_{j_r}} f^*_{j_r} = (-1)^{n-k} f_{s_1} \dots f_{s_l},$$

where a_{j_r} is the leading coefficient of $f^*_{j_r}(x)$. Note that the polynomials $f_{s_r}(x) = \frac{1}{a_{j_r}} f^*_{j_r}(x)$ are monic irreducible and divide $f(x) = (-1)^n[x^n - 1]$.

Now we show that $C^\perp = U_{s_1} \oplus \dots \oplus U_{s_l}$. By Theorem 3.1 $C^\perp$ is the space of the solutions of the homogeneous system with matrix $\tilde{h}(A)$. Let $u \in U = U_{s_1} \oplus \dots \oplus U_{s_l}$ and let $u = u_{s_1} + \dots + u_{s_l}$ for $u_{s_r} \in U_{s_r}$, $r = 1, \dots, l$. Then

$$\tilde{h}(A)u = (-1)^{n-k}[(f_{s_1} \dots f_{s_l})(A)u_{s_1} + \dots + (f_{s_1} \dots f_{s_l})(A)u_{s_l}] = \mathbf{0}.$$

Hence $U \leq C^\perp$. Since $\dim_F U = \dim_F C^\perp$, then

$$C^\perp = U_{s_1} \oplus \dots \oplus U_{s_l}.$$

Thus we have proved the following:

Theorem 3.2. *Let $C = U_{i_1} \oplus \cdots \oplus U_{i_s}$ be a linear cyclic code over F and $\{j_1, \dots, j_l\} = \{1, \dots, t\} \backslash \{i_1, \dots, i_s\}$. Then the dual code of C is given by $C^\perp = U_{s_1} \oplus \cdots \oplus U_{s_l}$ and $\tilde{f}_{s_r}(x) = (-1)^{k_{s_r}} f_{s_r}(x) = (-1)^{k_{s_r}} \frac{1}{a_{j_r}} f^*_{j_r}(x)$, where $f^*_{j_r}(x)$ is the reciprocal polynomial of $f_{j_r}(x)$ with leading coefficient equals to a_{j_r}, $r = 1, \dots, l$.*

Let $C \subset F^n$ be an arbitrary, not necessary linear, cyclic code. Let us consider the action of the group $G = \langle \varphi \rangle = \{\mathrm{id}, \varphi, \dots, \varphi^{n-1}\} \cong \mathbb{C}_n$ over F^n. Then the following theorem holds:

Theorem 3.3. *$C = \Omega_1 \cup \ldots \cup \Omega_s$, where Ω_i are G-orbits and $k_i = |\Omega_i|$ is a divisor of $|G| = n$. In particural, $|C| = \sum\limits_{i=1}^{s} k_i$.*

4. CONSTA-CYCLIC CODES

In this section we give a generalization of the results obtained in the previous sections.

Definition 4.1. Let a be a nonzero element of F. A code C with length n over F is called consta-cyclic with respect to a, if whenever $x = (c_1, c_2, \dots, c_n)$ is in C, so is $y = (ac_n, c_1, \dots, c_{n-1})$.

Let $a \in F$. We consider the linear operator $\psi_a \in \mathrm{Hom}\, F^n$

$$\psi_a : (x_1, x_2, \dots, x_n) \mapsto (ax_n, x_1, \dots, x_{n-1}).$$

Its matrix in the standard basis e_1, $e_2, \dots e_n$ of F^n is

$$B_a = \begin{pmatrix} 0 & 0 & 0 & \dots & a \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

The relations $B_a^{-1} = B^t_{\frac{1}{a}}$ and $B_a^n = aE$ hold. The characteristic polynomial of B_a is $f_{B_a}(x) = (-1)^n(x^n - a)$. Let denote it by $f_a(x)$. We assume that $(n, q) = 1$. The polynomial f_a has no multiple roots and splits to distinct irreducible monic factors $f_a(x) = (-1)^n f_1(x) \dots f_t(x)$. Let $U_i = \mathrm{Ker}\, f_i(\psi_a)$. It's easy to see that Theorem 2.1 and Proposition 2.2 are true in this case, too.

The following statement is clear from the definition.

Proposition 4.1. *A linear code C with length n over F is consta-cyclic iff C is a ψ_a-invariant subspace of F^n.*

The next theorem is analogous to Theorem 3.1 and we omit its proof.

Theorem 4.1. *Let C be a linear consta-cyclic code with length n over F. Then the following facts hold.*

1) $C = U_{i_1} \oplus \cdots \oplus U_{i_s}$ *for some minimal* ψ_a-*invariant subspaces* U_{i_r} *of* F^n *and* $\dim_F C = k_{i_1} + \cdots + k_{i_s} = k$;

2) $f_{\psi_a|_C}(x) = (-1)^k f_{i_1}(x) \dots f_{i_s}(x) = g(x)$;

3) $c \in C$ *iff* $g(B_a)c = \mathbf{0}$;

4) the polynomial $g(x)$ *has the smallest degree with the property 3);*

5) $\mathrm{r}\,(g(B_a)) = n - k$.

Proposition 4.2. *The dual of a linear consta-cyclic code with respect to a is consta-cyclic with respect to* $\dfrac{1}{a}$.

Proof: The proof follows from the equality

$$\langle \psi_a(c), h\rangle = \langle B_a c, h\rangle = \langle c, B_a^t h\rangle = \langle c, B_{\frac{1}{a}}^{-1} h\rangle = a\langle c, \psi_{\frac{1}{a}}^{n-1}(h)\rangle = 0$$

for every $c \in C$ and $h \in C^{\perp}$. □

Acknowledgements. The authors are greatly indebted to Prof. S. Dodunekov for posing of this interesting problem.

REFERENCES

1. Фаддеев, Д. К., В. Н. Фаддеева. Вычислительные методы линейной алгебры. Государсвенное издательство физико-математической литературы, Москва, 1963.
2. MacWilliams, F. G., N. J. A. Sloane. The Theory of Error Correcting Codes. The Netherlands: North-Holland, Amsterdam, 1977.
3. van Lint, J. H. The Theory of Error-Correcting codes. Berlin-Heidelberg-New York, Springer, Amsterdam, 1971.

Received on October 6, 2005

Faculty of Mathematics and Informatics
"St. Kl. Ohridski" University of Sofia
5, J. Bourchier blvd., 1164 Sofia
BULGARIA
E-mail: dradkova@fmi.uni-sofia.bg
bojilov@fmi.uni-sofia.bg