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 WITH LENGTH DIVISIBLE BY THE FIELD CHARACTERISTIC AS INVARIANT SUBSPACES

DIANA RADKOVA, ASEN BOJILOV

In the theory of cyclic codes it is a common practice to require $(n, q) = 1$, where n is the word length and F_q is the alphabet. However, much of the theory also goes through without this restriction on n and q. We observe that the cyclic shift map is a linear operator in F_q^n. Our approach is to consider cyclic codes as invariant subspaces of F_q^n with respect to this operator and thus obtain a description of cyclic codes in this more general setting.

Keywords: Cyclic codes, invariant subspaces.

2000 MSC: main 94B15, secondary 47A15

1. INTRODUCTION

The main purpose of this paper is the study of some properties of the cyclic codes as linear subspaces without the requirement that the field characteristic is coprime with n. We already considered the case of coprime field characteristic and word length in [4].

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

2. SOME LINEAR ALGEBRA

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

Let $\varphi : F^n \to F^n$ be the linear map given by the formula $\varphi(x_1, x_2, \dots, x_n) = (x_n, x_1, \dots, x_{n-1})$.

Then φ 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 $\varphi(e_1) = e_2$, $\varphi(e_2) = e_3, \dots$, $\varphi(e_{n-1}) = e_n$, $\varphi(e_n) = e_1$.

We observe that $A^t = A^{-1}$ and $A^n = E$. The characteristic polynomial of A is

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

We will denote the polynomial $f_A(x)$ by $f(x)$.

We will assume that $(n, q) = p^s = d$ and $n = dn_1$, $(p, n_1) = 1$, where $p = \Gamma F$. Let $x^{n_1} - 1 = f_1(x)\dots f_t(x)$ be the factorization of $x^{n_1} - 1$ into irreducible monic factors over F. Then the factorization of $f(x)$ is

$$f(x) = (-1)^n(x^n - 1) = (-1)^n\Big(x^{n_1} - 1\Big)^d = (-1)^n\Big(f_1(x)\Big)^d\Big(f_2(x)\Big)^d \dots \Big(f_t(x)\Big)^d.$$

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

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) $f_i^d(x)$ is the monic polynomial of minimal degree in $F[x]$ such that $f_i^d(A)u = \mathbf{0}$ for all $u \in U_i$;

4) $f_{\varphi|_{U_i}} = (-1)^{d \deg f_i} f_i^d$. In particular, $\dim U_i = \deg f_{\varphi|_{U_i}} = d \deg f_i$:

5) There exist a vector $u_i \in U_i$ such that the vectors

$$u_i, \varphi(u_i), \dots, \varphi^{\dim U_i - 1}(u_i)$$

are basis of U_i;

6)For each vector u in U_i there exists a polynomial $g \in F[x]$ such that $u = \Big(g(A)\Big)(u_i)$.

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

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

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

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

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

Let us assume that $v \in U_i \cap \sum_{j \neq i} U_j$. Then $f_i^d(A)v = \mathbf{0}$ and $\hat{f}_i(A)v = \mathbf{0}$. Since $(f_i^d, \hat{f}_i) = 1$, there are polynomials $a(x), b(x) \in F[x]$, such that $a(x)f_i^d(x) + b(x)\hat{f}_i(x) = 1$. Hence $a(A)f_i^d(A)v + b(A)\hat{f}_i(A)v = v = \mathbf{0}$ and we conclude that $U_i \cap \sum_{j \neq i} U_j = \{\mathbf{0}\}$. Thus

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

3) Let $m_i(x) \in F[x]$ be the monic polynomial of smallest degree such that $m_i(A)u = \mathbf{0}$ for all $u \in U_i$. By the division algorithm in $F[x]$ there are polynomials $q_i(x), r_i(x)$ such that $f_i^d(x) = m_i(x)q_i(x) + r_i(x)$, where $\deg r_i(x) < \deg m_i(x)$. Then for each vector $u \in U_i$ we have $f_i^d(A)u = q_i(A)m_i(A)u + r_i(A)u$ and hence $r_i(A)u = \mathbf{0}$. But this contradicts the choice of $m_i(x)$ unless $r_i(x)$ is identically zero. Thus, $m_i(x)$ divides $f_i^d(x)$ for all $i = 1, \ldots, t$. Therefore there are numbers $0 \leq s_i \leq d$ such that $m_i(x) = f_i^{s_i}(x)$. Set $m(x) = m_1(x) \ldots m_t(x)$. Since $m(A)u = \mathbf{0}$ for all $u \in F^n$ and $m(x)$ divides the minimal polynomial $x^n - 1$ of A, we conclude that $x^n - 1 = m(x)$. Then

$$f_1^d(x) \ldots f_t^d(x) = x^n - 1 = f_1^{s_1}(x) \ldots f_t^{s_t}(x).$$

Now the statement follows from the uniqueness of the factorization of a polynomial into irreducible factors.

4) Let $k_i = \dim U_i$, $i = 1, \ldots, t$ and let $\tilde{f}_i(x) = f_{\varphi|_{U_i}}$. We choose a basis $g_1^{(i)}, \ldots, g_{k_i}^{(i)}$ of U_i over F, $i = 1, \ldots, t$. Denote by A_i the matrix of $\varphi|_{U_i}$ in that basis.

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

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

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

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

Note that $\tilde{f}_i(A_i) = \mathbf{0}$. Let $g_j^{(i)} = \lambda_{j1}^{(i)}e_1 + \cdots + \lambda_{j\,n}^{(i)}e_n$, $j = 1, \ldots, k_i$. Since $g_j^{(i)} \in U_i$, we obtain

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

where 1 is on the $(k_1 + \cdots + k_{i-1} + j)-$th position. Therefore $f_i^d(x)$ divides $\tilde{f}_i$ for all $i = 1, \ldots, t$. Let $\tilde{f}_i(x) = f_i^d(x)g_i(x)$. Then

$$f(x) = \tilde{f}_1(x)\ldots\tilde{f}_t(x) = f_1^d(x)\ldots f_t^d(x)g_1(x)\ldots g_t(x).$$

It follows from the last identity that $g_i(x) = (-1)^{d\deg f_i(x)}$.

5) Let $e_1 = u_1 + u_2 + \cdots + u_t$ for $u_i \in U_i$, $i = 1, \ldots, t$. Then

$$\begin{array}{lllllll} e_2 = & \varphi(e_1) & = & \varphi(u_1) & + & \varphi(u_2) & + \cdots + \ \varphi(u_t) \\ e_3 = & \varphi(e_2) & = & \varphi^2(u_1) & + & \varphi^2(u_2) & + \cdots + \ \varphi^2(u_t) \\ \multicolumn{7}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots} \\ e_n = & \varphi(e_{n-1}) = & & \varphi^{n-1}(u_1) + & & \varphi^{n-1}(u_2) + & \cdots + \varphi^{n-1}(u_t) \end{array}.$$

Let v be an arbitrary vector from F^n. Then

$$\begin{array}{c} v = \lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_n e_n = \\ = \ \lambda_1(u_1 + u_2 + \cdots + u_t) + \lambda_2(\varphi(u_1) + \varphi(u_2) + \cdots + \varphi(u_t)) + \\ + \cdots + \lambda_n(\varphi^{n-1}(u_1) + \varphi^{n-1}(u_2) + \cdots + \varphi^{n-1}(u_t)) = \\ = (\lambda_1 u_1 + \lambda_2\varphi(u_1) + \cdots + \lambda_n\varphi^{n-1}(u_1)) + \\ + \cdots + (\lambda_1 u_t + \lambda_2\varphi(u_t) + \cdots + \lambda_n\varphi^{n-1}(u_t)) \end{array}.$$

Hence $v_i = \lambda_1 u_i + \lambda_2\varphi(u_i) + \cdots + \lambda_n\varphi^{n-1}(u_i)$ holds for each vector $v_i \in U_i$ and all $i = 1, \ldots, t$. Therefore $U_i = l\{u_i, \varphi(u_i), \ldots, \varphi^{n-1}(u_i)\}$. Since $\dim U_i = k_i$, the vectors

$$u_i, \varphi(u_i), \ldots, \varphi^{k_i - 1}(u_i)$$

are a basis of U_i.

6)This follows from 5). □

Theorem 2.2. *Let U be a φ-invariant subspace of U_i for some $1 \le i \le t$. Then there exists a number $0 \le k \le d$ such that $U = \operatorname{Im} f_i^k(\varphi_{|U_i}) = \operatorname{Ker} f_i^{d-k}(\varphi_{|U_i}) = \operatorname{Ker} f_i^{d-k}(\varphi)$.*

Proof: Let the vector $u_i \in U_i$ be as in Theorem 2.1 and let us consider the set

$$J = \{g \in F[x] \mid \Big(g(A)\Big)(u_i) \in U\}.$$

It is easy to verify that J is a principal ideal in $F[x]$. Then there exists a monic polynomial $h \in F[x]$ such that $J = (h)$. We are going to show that $U = \operatorname{Im} h(\varphi_{|U_i})$. First, let $u \in U$. Then $u = g(A)u_i$ for a suitable polynomial $g(x) \in F[x]$ by Theorem 2.1, 6). Since $g(x) \in J$ then $g(x) = h(x)g_1(x)$. Hence $u = (hg_1)(A)u_i = h(A)g_1(A)u_i = h(A)v_i$, where $v_i \in U_i$. Thus $u \in \operatorname{Im} h(\varphi_{|U_i})$. Conversely, suppose $u \in \operatorname{Im} h(\varphi_{|U_i})$, i.e. $u = h(A)v$ for some $v \in U_i$. Then $v = g(A)u_i$ for a suitable polynomial $g(x) \in F[x]$ and hence $u = h(A)g(A)u_i = (hg)(A)u_i$. Since $h(x)g(x) \in J$, we conclude that $u \in U$.

Now we are going to show that $h(x) = f_i^k(x)$ for some $0 \le k \le d$. Since $f_i^d(A)u_i = \mathbf{0}$, then $f_i^d(x) \in J$. Therefore $h(x)$ divides $f_i^d(x)$. Since $f_i(x)$ is an irreducible polynomial, $h(x) = f_i^k(x)$ for some $0 \le k \le d$. Hence $U = \operatorname{Im} f_i^k(\varphi_{|U_i})$. It remains to prove that $U = \operatorname{Ker} f_i^{d-k}(\varphi_{|U_i})$. We have

$$f_i^{d-k}(A_i)f_i^k(A_i) = f_i^d(A_i) = \mathbf{0},$$

where A_i is the matrix of $\varphi_{|U_i}$.

Since each column of $f_i^k(A_i)$ is a solution of the homogeneous system with matrix $f_i^{d-k}(A_i)$, then $U = \operatorname{Im} f_i^k(\varphi_{|U_i}) \subseteq \operatorname{Ker} f_i^{d-k}(\varphi_{|U_i})$. It is easy to verify that $\operatorname{Ker} f_i^{d-k}(\varphi_{|U_i}) = \operatorname{Ker} f_i^{d-k}(\varphi)$. Now suppose $u \in \operatorname{Ker} f_i^{d-k}(\varphi)$, i.e. $f_i^{d-k}(A)u = \mathbf{0}$. Then $u \in \operatorname{Ker} f_i^d(\varphi) = U_i$ and $u = g(A)u_i$ for a suitable polynomial $g(x) \in F[x]$. Hence $f_i^{d-k}(A)g(A)u_i = \mathbf{0}$. Since $f_i^d(x)$ is the minimal polynomial with the property $f_i^d(A)u_i = \mathbf{0}$ we conclude that $f_i^k(x)$ divides $g(x)$. Thus $g(x) \in J$ and $u \in U$, which proves the statement. □

Proposition 2.1. *Let U be a φ-invariant subspace of F^n. Then U is a direct sum of subspaces of F^n of the form $\operatorname{Ker} f_i^{s_i}(\varphi)$, where $0 \le s_i \le d$.*

Proof: Let $\widetilde{U}_i = U \cap U_i$, $i = 1, \dots, t$. Then $\widetilde{U}_i = \operatorname{Ker} f_i^{s_i}(\varphi)$ for some $0 \le s_i \le d$. Therefore

$$U = U \cap F^n = U \cap (U_1 \oplus \cdots \oplus U_t) = \widetilde{U}_1 \oplus \cdots \oplus \widetilde{U}_t.$$ □

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 cyclic shift $y = (c_n, c_1, \dots, c_{n-1})$.*

The following statement is clear from the definition.

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) $C = \widetilde{U}_{i_1} \oplus \cdots \oplus \widetilde{U}_{i_m}$ for some $\varphi-$invariant subspaces $\widetilde{U}_{i_r} = \operatorname{Ker} f_{i_r}^{s_r}(\varphi)$ of F^n, $0 < s_r \leq d$, and $\dim_F C = \sum_{r=1}^{m} s_r \deg f_{i_r} = k$;

2) $f_{\varphi|_C}(x) = (-1)^k f_{i_1}^{s_1}(x) \dots f_{i_m}^{s_m}(x) = g(x)$;

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) The first part of the statement follows from Proposition 2.1. Now we are going to show that $\dim_F \operatorname{Ker} f_{i_r}^{s_r} = s_r \deg f_{i_r}$. Let us consider the following chain of linear subspaces of F^n

$$\operatorname{Ker} f_{i_r}(\varphi) \subset \operatorname{Ker} f_{i_r}^2(\varphi) \subset \cdots \subset \operatorname{Ker} f_{i_r}^d(\varphi) = U_{i_r}.$$

Since the characteristic polynomial of the restriction of φ to $\operatorname{Ker} f_{i_r}^l(\varphi)$ divides $f_{\varphi|_{U_{i_r}}} = (-1)^{d \deg f_{i_r}} f_{i_r}^d$ for all $l = 1, \dots d$, then for the dimensions of the respective subspaces we obtain the following inequalities of natural numbers

$$l_1 \deg f_{i_r} < l_2 \deg f_{i_r} < \cdots < l_d \deg f_{i_r} = d \deg f_{i_r}.$$

Thus $l_i = i$ for $i = 1, \dots, d$, which proves the statement. In particular, it follows from the proof that $f_{\varphi|_{\widetilde{U}_{i_r}}}(x) = (-1)^{s_r deg f_{i_r}} f_{i_r}^{s_r}(x)$.

2) Let us denote $\alpha_{i_r} = \dim \widetilde{U}_{i_r} = s_r \deg f_{i_r}$. We choose a basis $u_1^{(i_r)}, \dots, u_{\alpha_{i_r}}^{(i_r)}$ of $\widetilde{U}_{i_r}$ over F, $r = 1, \dots, m$ and denote by B_{i_r} the matrix of $\varphi|_{\widetilde{U}_{i_r}}$ in that basis. Then $u_1^{(i_1)}, \dots, u_{\alpha_{i_1}}^{(i_1)}, \dots, u_1^{(i_m)}, \dots, u_{\alpha_{i_m}}^{(i_m)}$ is a basis of C over F and $\varphi|_C$ has a matrix

$$\begin{pmatrix} B_{i_1} & & & \\ & B_{i_2} & & \\ & & \ddots & \\ & & & B_{i_m} \end{pmatrix}$$

in that basis. Hence

$$f_{\varphi|_C}(x) = f_{\varphi|_{\widetilde{U}_{i_1}}}(x) \dots f_{\varphi|_{\widetilde{U}_{i_m}}}(x) = (-1)^k f_{i_1}^{s_1}(x) \dots f_{i_m}^{s_m}(x).$$

3) Let $c \in C$. Then $c = u_{i_1} + \cdots + u_{i_m}$ for some $u_{i_r} \in \widetilde{U}_{i_r}$, $r = 1, \dots, m$ and $g(A)c = (-1)^k[(f_{i_1}^{s_1} \dots f_{i_m}^{s_m})(A)u_{i_1} + \cdots + (f_{i_1}^{s_1} \dots f_{i_m}^{s_m})(A)u_{i_m}] = \mathbf{0}$.

Conversely suppose that $g(A)c = \mathbf{0}$ for some $c \in F^n$ and let $c = u_1 + \cdots + u_t$, $u_i \in U_i$. Then $g(A)c = (-1)^k[(f_{i_1}^{s_1} \dots f_{i_m}^{s_m})(A)u_1 + \cdots + (f_{i_1}^{s_1} \dots f_{i_m}^{s_m})(A)u_t] = \mathbf{0}$, so that $g(A)[u_{j_1} + \cdots + u_{j_l}] = \mathbf{0}$, where $\{j_1, \dots j_l\} = \{1, \dots, t\} \setminus \{i_1, \dots, i_m\}$. Set $v_{j_r} = g(A)u_{j_r}$, for all $r = 1, \dots, l$. Hence $v_{j_r} \in U_{j_r}$ and $v_{j_1} + \cdots + v_{j_l} = \mathbf{0}$. Therefore $v_{j_r} = \mathbf{0}$ for all $r = 1, \dots l$. Since $(g, f_{j_r}^d) = 1$ there are polynomials $a(x), b(x) \in F[x]$, such that $a(x)g(x) + b(x)f_{j_r}^d(x) = 1$. Then $u_{j_r} = a(A)g(A)u_{j_r} + b(A)f_{j_r}^d(A)u_{j_r} = \mathbf{0}$. Thus $c = u_{i_1} + \cdots + u_{i_m} \in C$.

We omit the proofs of 4) and 5), since they are clear. □

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. Besides the dual of a linear cyclic code is also cyclic.

Proposition 3.2. *The matrix H, which rows are arbitrary $n-k$ linearly 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 us denote

$$h(x) = \frac{f(x)}{g(x)} = (-1)^{n-k} f_1^{d-s_1}(x) \dots f_t^{d-s_t}(x),$$

where $0 \le s_r \le d$ for all $r = 1, \dots, t$.

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 that $\mathrm{r}(\mathbf{0}) = 0 \ge \mathrm{r}(g(A)) + \mathrm{r}(h(A)) - n$. Thus $\mathrm{r}(h(A)) \le n - \mathrm{r}(g(A)) = n - (n-k) = k$.

On the other hand, Sylvester's inequality, applied to the product $h(A) = (-1)^{n-k} f_1^{d-s_1}(A) \dots f_t^{d-s_t}(A)$, gives us that $\mathrm{r}(h(A)) \ge r(f_1^{d-s_1}(A)) + \cdots + r(f_t^{d-s_t}(A)) - n(t-1) = nt - d\sum_{i=1}^t \deg f_i + \sum_{i=1}^t s_i \deg f_i - nt + n = k$. Therefore $\mathrm{r}(h(A)) = k$. Thus we have proved the following:

Proposition 3.3. *The matrix G, which rows are arbitrary k linearly independent rows of $(h(A))^t$, is a generator matrix of the code C.*

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 $h^*(A) = A^{n-k}(h(A^t)) = \tilde{h}(A)q(A) + r(A)$, 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 $(f_1^*(x))^{d-s_1} \dots (f_t^*(x))^{d-s_t}$. Thus

$$\tilde{h} = \frac{1}{a}h^* = (-1)^{n-k}\frac{1}{a}(f_1^*(x))^{d-s_1} \dots (f_t^*(x))^{d-s_t} =$$

$$(-1)^{n-k}\prod_{i=1}^{t}\frac{1}{a_i}(f_i^*(x))^{d-s_i} = (-1)^{n-k}\prod_{i=1}^{t} f_{n_i}^{d-s_i}(x),$$

where a_i is the leading coefficient of $(f_i^*(x))^{d-s_i}$. Note that the polynomials $f_{n_i}(x)$ are monic irreducible and divide $f(x) = (-1)^n(x^n - 1)$.

Now we show that $C^\perp = \overline{U_{n_1}} \oplus \cdots \oplus \overline{U_{n_t}}$, where $\overline{U_{n_i}} = \operatorname{Ker} f_{n_i}^{d-s_i}(\varphi)$. By Theorem 3.1 $C^\perp$ is the space of the solutions of the homogeneous system with matrix $\tilde{h}(A)$. Let $u \in U = \overline{U_{n_1}} \oplus \cdots \oplus \overline{U_{n_t}}$ and let $u = u_{n_1} + \cdots + u_{n_t}$ for $u_{n_r} \in U_{n_r}$, $r = 1, \dots, t$. Then

$$\tilde{h}(A)u = (-1)^{n-k}[(f_{n_1}^{d-s_1} \dots f_{n_t}^{d-s_t})(A)u_{n_1} + \cdots + (f_{n_1}^{d-s_1} \dots f_{n_t}^{d-s_t})(A)u_{n_t}] = \mathbf{0}.$$

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

$$C^\perp = \overline{U_{n_1}} \oplus \cdots \oplus \overline{U_{n_t}}.$$

Thus we have proved the following:

Theorem 3.2. *Let $C = \widetilde{U}_1 \oplus \cdots \oplus \widetilde{U}_t$ be a linear cyclic code over F, where $\widetilde{U}_i = \operatorname{Ker} f_i^{s_i}(\varphi)$, $0 \leq s_i \leq d$. Then the dual code of C is given by $C^\perp = \overline{U_{n_1}} \oplus \cdots \oplus \overline{U_{n_t}}$ and $f_{\varphi|_{\overline{U_i}}}(x) = (-1)^{d-s_i}\frac{1}{a_i}(f_i^*(x))^{d-s_i} = (-1)^{d-s_i} f_{n_i}^{d-s_i}(x)$ where $(f_i^*(x))^{d-s_i}$ is the reciprocal polynomial of $f_i^{d-s_i}(x)$ with leading coefficient equals to a_i, $i = 1, \dots, t$.*

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.

4. Radkova, D., A. Bojilov. Cyclic codes as invariant subspaces. to appear in *Ann. de L'Univ. de Sofia*, vol. 98.

Received on October 6, 2005
Revised on April 23, 2006

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
E-mail: bojilov@fmi.uni-sofia.bg