CYCLIC CODES AND QUASI-TWISTED CODES: AN ALGEBRAIC APPROACH

D. RADKOVA, A. BOJILOV
and
A. J. VAN ZANTEN

Abstract

In coding theory the description of linear cyclic codes in terms of commutative algebra is well known. Since linear codes have the structure of linear subspaces of F^n, the description of linear cyclic codes in terms of linear algebra is natural. We observe that the cyclic shift map is a linear operator in F^n. Our approach is to consider cyclic codes as invariant subspaces of F^n with respect to this operator and thus obtain a description of cyclic codes. A new algebraic approach to quasi-twisted codes is also introduced.

CONTENTS

1. INTRODUCTION

In coding theory it is common practice to require that $(n, q) = 1$, where n is the word length and $F = \mathrm{GF}(q)$ is the alphabet. We shall stick to this practice too.

The main purpose of this report is to regard quasi-twisted codes as invariant linear subspaces of F^n with respect to an $a-$constacyclic shift map over k positions, where k is a devisor of the length n and $0 \neq a \in F$. Some important classes of codes are realized as special cases of quasi-twisted codes. The case $k = 1$ gives constacyclic codes, while $k = 1$ and $a = 1$ yields cyclic codes. The linear cyclic codes are traditionally described by using the methods of commutative algebra (see [1]). Since linear codes have the structure of linear subspaces of F^n, the description of linear cyclic codes in terms of linear algebra is natural.

2. LINEAR CYCLIC CODES AS INVARIANT SUBSPACES

Let $F = \mathrm{GF}(q)$ and let F^n be the n-dimensional vector space over F with the standard basis $\mathbf{e}_1 = (1, 0, \dots, 0)$, $\mathbf{e}_2 = (0, 1, \dots, 0), \dots, \mathbf{e}_n = (0, 0, \dots, 1)$.

Let

$$\varphi : \begin{cases} F^n \to F^n \\ (x_1, x_2, \dots, x_n) \mapsto (x_n, x_1, \dots, x_{n-1}) \end{cases} . \tag{2.1}$$

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

$$A = \begin{pmatrix} 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix} \tag{2.2}$$

with respect to the basis $e = (\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n)$. Note that $A^t = A^{-1}$ and $A^n = E$. The characteristic polynomial of A is

$$f_A(x) = \begin{vmatrix} -x & 0 & 0 & \dots & 1 \\ 1 & -x & 0 & \dots & 0 \\ 0 & 1 & -x & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & -x \end{vmatrix} = (-1)^n (x^n - 1). \tag{2.3}$$

Let us denote it by $f(x)$. For our purposes we need the following well known fact.

Proposition 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 a φ-invariant subspace of F^n then $f_\varphi(x) = f_{\varphi|_U}(x) f_{\varphi|_W}(x)$.*

Let $f(x) = (-1)^n f_1(x) \dots f_t(x)$ be the factorization of $f(x)$ into irreducible factors over F. We assume that $(n, q) = 1$. In that case $f(x)$ has distinct factors $f_i(x),\ i = 1, \dots, t$, which are monic. Furthermore, we consider the homogeneous set of equations

$$f_i(A)\mathbf{x} = \mathbf{0},\ \mathbf{x} \in F^n \tag{2.4}$$

for $i = 1, \dots, t$. If U_i stands for the solution space of (2.4), then we may write $U_i = \operatorname{Ker} f_i(\varphi)$.

Theorem 1. *The subspaces U_i of F^n satisfy the following conditions:*

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

2) if W is a $\varphi-$invariant subspace of F^n and $W_i = W \cap U_i$ for $i = 1, \dots, t$, then W_i is $\varphi-$invariant and $W = W_1 \oplus \dots \oplus W_t$;

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

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

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

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

Proof:

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

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 $\mathbf{w} \in W$ the equality $\mathbf{w} = a_1(A)\hat{f}_1(A)\mathbf{w} + \dots + a_t(A)\hat{f}_t(A)\mathbf{w}$ holds. Let $\mathbf{w}_i = a_i(A)\hat{f}_i(A)\mathbf{w} \in W$. Then $f_i(A)\mathbf{w}_i = a_i(A)f(A)\mathbf{w} = \mathbf{0}$ because of (2.4), and so $\mathbf{w}_i \in V_i \cap W = W_i$. Hence,

$$W = W_1 + \dots + W_t.$$

Assume that $\mathbf{w} \in W_i \cap \sum_{j \neq i} W_j$, then $f_i(A)\mathbf{w} = \mathbf{0},\ \hat{f}_i(A)\mathbf{w} = \mathbf{0}$. Since $(f_i(x), \hat{f}_i(x)) = 1$, 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 $a(A)f_i(A)\mathbf{w} + b(A)\hat{f}_i(A)\mathbf{w} = \mathbf{w} = \mathbf{0}$, so that $W_i \cap \sum_{j \neq i} W_j = \{\mathbf{0}\}$. Thus

$$W = W_1 \oplus \dots \oplus W_t.$$

3) This follows from 2) with $W = F^n$.

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

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

Consider the polynomial $t(x) = x^k - c_{k-1}x^{k-1} - \cdots - c_0 \in F[x]$. Since $(t(\varphi))(\mathbf{g}) = (f_i(\varphi))(\mathbf{g}) = \mathbf{0}$, it follows that $[(t(x), f_i(x))(\varphi)](\mathbf{g}) = \mathbf{0}$. But $(t(x), f_i(x))$ is equal to 1 or to $f_i(x)$. 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 $\mathbf{g}, \varphi(\mathbf{g}), \ldots, \varphi^{k_i}(\mathbf{g})$ are linearly dependent, since $(f_i(\varphi))(\mathbf{g}) = \mathbf{0}$, 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 $\dim{}_F U_i = k_i$.

5) Let $g^{(i)} = (\mathbf{g}_1^{(i)}, \ldots, \mathbf{g}_{k_i}^{(i)})$ be a basis of U_i over F, $i = 1, \ldots, t$ and let A_i be the matrix of $\varphi|_{U_i}$ with respect to that basis. Let $\tilde{f}_i = f_{\varphi|_{U_i}}$. Suppose that $(\tilde{f}_i, f_i) = 1$. 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 $f_i(A_i) = O$, which contradicts the last equation.

By property 3) we obtain that $g = (\mathbf{g}_1^{(1)}, \ldots, \mathbf{g}_{k_1}^{(1)}, \ldots, \mathbf{g}_1^{(t)}, \ldots, \mathbf{g}_{k_t}^{(t)})$ is a basis of F^n and φ is represented by the following matrix

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

with respect to that basis. Beside this $A' = T^{-1}AT$, where T is the transformation matrix from the standard basis of F^n to the basis g. 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 $\mathbf{g}_j^{(i)} = \lambda_{j1}^{(i)}\mathbf{e}_1 + \cdots + \lambda_{j\,n}^{(i)}\mathbf{e}_n$, $j = 1, \ldots, k_i$. Since $\mathbf{g}_j^{(i)} \in U_i$, we obtain that

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

where 1 is on the $(k_1 + \cdots + k_{i-1} + j)-$th position. According to the last equation $f_i(A_i) = O$. 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 that $\tilde{f}_i = (-1)^{k_i} f_i$.

6) Let U be φ-invariant subspace of F^n and let $\{\mathbf{0}\} \neq U \subseteq U_i$. Then by Proposition 1 we obtain that $f_{\varphi|_U}$ divides f_i. Since the polynomial f_i is irreducible, $\dim{}_F U = \dim{}_F U_i$ and $U = U_i$.

$\square$

Proposition 2. *Let U be a $\varphi-$invariant subspace of F^n. Then U is a direct sum of some of the minimal $\varphi-$invariant subspaces U_i of F^n.*

Proof: This follows immediately from property 2) of Theorem 1. $\square$

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

The following statement is clear from the definitions.

Proposition 3. *A linear code C with length n over F is cyclic iff C is a $\varphi-$invariant subspace of F^n.*

Theorem 2. *Let C be a linear cyclic code with length n over F. Then the following facts hold.*

1) $C = U_{i_1} \oplus \dots \oplus U_{i_s}$ for some minimal $\varphi-$invariant subspaces U_{i_r} of F^n and $k := \dim_F C = k_{i_1} + \dots + k_{i_s}$, where k_r is the dimension of U_{i_r};

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

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

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

5) $\mathrm{r}\,(g(A)) = n - k$, where $\mathrm{r}\,(g(A))$ is the rank of the matrix $g(A)$.

Proof:

1) This follows from Proposition 2.

2) Let $(\mathbf{g}_1^{(i_r)}, \dots, \mathbf{g}_{k_{i_r}}^{(i_r)})$ be a basis of U_{i_r} over F, $r = 1, \dots, s$. Then $(\mathbf{g}_1^{(i_1)}, \dots, \mathbf{g}_{k_{i_1}}^{(i_1)}, \dots, \mathbf{g}_1^{(i_s)}, \dots, \mathbf{g}_{k_{i_s}}^{(i_s)})$ is a basis of C over F and $\varphi|_C$ is represented by the following matrix

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

with respect to that basis. Hence,

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

Note that A_{i_r} and $\tilde{f}_{i_r}(x)$ are defined as in the proof of Theorem 1.

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

Conversely, suppose that $g(A)\mathbf{c} = \mathbf{0}$ for some $\mathbf{c} \in F^n$. According to Theorem 1 we have that $\mathbf{c} = \mathbf{u}_1 + \dots + \mathbf{u}_t$, $\mathbf{u}_i \in U_i$. Then $g(A)\mathbf{c} = (-1)^k[(f_{i_1} \dots f_{i_s})(A)\mathbf{u}_1 + \dots + (f_{i_1} \dots f_{i_s})(A)\mathbf{u}_t] = \mathbf{0}$, so that $g(A)[\mathbf{u}_{j_1} + \dots + \mathbf{u}_{j_l}] = \mathbf{0}$, where $\{j_1, \dots j_l\} = \{1, \dots, t\} \backslash \{i_1, \dots, i_s\}$. Let $\mathbf{v} = \mathbf{u}_{j_1} + \dots + \mathbf{u}_{j_l}$ 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 $a(x)$, $b(x) \in F[x]$ so that $a(x)h(x) + b(x)g(x) = 1$. Hence $\mathbf{v} = a(A)h(A)\mathbf{v} + b(A)g(A)\mathbf{v} = \mathbf{0}$ and $\mathbf{c} = \mathbf{u}_{i_1} + \cdots + \mathbf{u}_{i_s} \in C$.

4) Suppose that $b(x) \in F[x]$ is a nonzero polynomial of smallest degree such that $b(A)\mathbf{c} = \mathbf{0}$ for all $\mathbf{c} \in C$. 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 $\mathbf{c} \in C$ we have $g(A)\mathbf{c} = q(A)b(A)\mathbf{c} + r(A)\mathbf{c}$ and hence $r(A)\mathbf{c} = \mathbf{0}$. 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 that $b(x) = (-1)^{k_{i_1}+\cdots+k_{i_m}} f_{i_1} \ldots f_{i_m}$ and $m < s$. Let us consider the code $C' = U_{i_1} \oplus \cdots \oplus U_{i_m} \subset C$. Then $b(x) = f_{\varphi|_{C'}}$ and by the equation $g(A)\mathbf{c} = \mathbf{0}$ for all $\mathbf{c} \in C$ we obtain that $C \subseteq C'$. This contradiction proves the statement.

5) By property 3) C is the solution space of the homogeneous set of equations $g(A)\mathbf{x} = \mathbf{0}$. Then $\dim_F C = k = n - \mathrm{r}\,(g(A))$, which proves the statement.

□

Definition 2. *Let $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1 \ldots, y_n)$ be two vectors in F^n. We define an inner product over F by $\langle \mathbf{x}, \mathbf{y} \rangle = x_1y_1 + \cdots + x_ny_n$. If $\langle \mathbf{x}, \mathbf{y} \rangle = 0$, we say that $\mathbf{x}$ and $\mathbf{y}$ are orthogonal to each other.*

Definition 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.,*

$$C^\perp = \{\mathbf{v} \in F^n \mid \langle \mathbf{v}, \mathbf{c} \rangle = 0, \ \forall \mathbf{c} \in C\}.$$

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

Proposition 4. *The dual of a linear cyclic code is also cyclic.*

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

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

which proves the statement.

□

Proposition 5. *The matrix H, the rows of which are an arbitrary set of $n-k$ linearly independent rows of $g(A)$, is a parity check matrix of C.*

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

□

Let $\mathbf{g}_{l_1}, \ldots, \mathbf{g}_{l_{n-k}}$ be a basis of $C^\perp$, where $\mathbf{g}_{l_r}$ is a l_r-th vector row of $g(A)$. By the equation $g(A)h(A) = O$ we obtain that $\langle \mathbf{g}_{l_r}, \mathbf{h}_i \rangle = 0$ for each $i = 1, \ldots, n$, $r = 1, \ldots, n-k$. The last equation gives us that the columns $\mathbf{h}_i$ of $h(A)$ are codewords in C.

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

Proposition 6. *The matrix G, the rows of which are an arbitrary set of k linearly independent rows of $(h(A))^t$, is a generator matrix of the code C.*

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

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 2 it follows that $\tilde{h}$ is the polynomial of the smallest degree such that $\tilde{h}(A)\mathbf{u} = \mathbf{0}$ for every $\mathbf{u} \in C^\perp$. Let $h^*(x) = \tilde{h}(x) q(x) + r(x)$, where $\deg r(x) < \deg \tilde{h}(x)$. Then by Lemma 1 $h^*(A) = A^{n-k}(h(A))^t = \tilde{h}(A) q(A) + r(A)$, hence for every vector $\mathbf{u} \in C^\perp$ the assertion $A^{n-k}(h(A))^t \mathbf{u} = q(A)\tilde{h}(A)\mathbf{u} + r(A)\mathbf{u}$ holds, so that $r(x) = 0$. Thus $\tilde{h}(x)$ divides $h^*(x)$. Since both are polynomials of the same degree , $h^*(x) = \alpha \tilde{h}(x)$, where $\alpha \in F$ is the leading coefficient of the product $f^*_{j_1}(x) \dots f^*_{j_l}(x)$. Thus

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

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

Now we show that $C^\perp = U_{s_1} \oplus \cdots \oplus U_{s_l}$. By Theorem 2 $C^\perp$ is the solution space of the homogeneous system with matrix $\tilde{h}(A)$. Let $\mathbf{u} \in U = U_{s_1} \oplus \cdots \oplus U_{s_l}$ and let $\mathbf{u} = \mathbf{u}_{s_1} + \cdots + \mathbf{u}_{s_l}$ for $\mathbf{u}_{s_r} \in U_{s_r}$, $r = 1, \dots, l$. Then

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

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

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

Thus we have proved the following theorem.

Theorem 3. *Let $C = U_{i_1} \oplus \cdots \oplus U_{i_s}$ be a linear cyclic code over F, and $\{j_1, \ldots, j_l\} = \{1, \ldots, t\} \backslash \{i_1, \ldots, i_s\}$. Then the dual code of C is given by $C^{\perp} = U_{s_1} \oplus \cdots \oplus U_{s_l}$ and $\tilde{f}_{s_r}(x) = (-1)^{k_{s_r}} f_{s_r}(x) = (-1)^{k_{s_r}} \frac{1}{\alpha_{j_r}} f^*_{j_r}(x)$, where $f^*_{j_r}(x)$ is the reciprocal polynomial of $f_{j_r}(x)$ with leading coefficient equal to α_{j_r}, $r = 1, \ldots, l$.*

Example 1. Consider the matrix A of (2.2) for $n = 7$ and $q = 2$. Then we have

$$f(x) := f_A(x) = x^7 + 1.$$

Factorizing $f(x)$ into irreducible factors over $GF(2)$ yields

$$f(x) = f_1(x) f_2(x) f_3(x) = (x+1)(x^3+x+1)(x^3+x^2+1).$$

The factors $f_i(x)$ define minimal $\varphi-$invariant spaces U_i, for $i = 1, 2, 3$. We define the cyclic linear code C

$$C := U_1 \oplus U_3.$$

According to Theorem 2, we have $\dim C = 4$ and

$$g(x) := f_{\varphi|_C}(x) = (x+1)(x^3+x^2+1) = x^4 + x^2 + x + 1.$$

It follows that

$$g(A) = \begin{pmatrix} 1&0&0&1&0&1&1 \\ 1&1&0&0&1&0&1 \\ 1&1&1&0&0&1&0 \\ 0&1&1&1&0&0&1 \\ 1&0&1&1&1&0&0 \\ 0&1&0&1&1&1&0 \\ 0&0&1&0&1&1&1 \end{pmatrix}$$

The rank of this matrix is $\mathrm{r}\,(g(A)) = 7 - 4 = 3$. Taking 3 independent rows yields by Proposition 5 a parity check matrix for the code C, i.e.,

$$H\mathbf{c} = \begin{pmatrix} 1&0&1&1&1&0&0 \\ 0&1&0&1&1&1&0 \\ 0&0&1&0&1&1&1 \end{pmatrix} \mathbf{c} = \mathbf{0}$$

Notice that the columns of H represent integers $1, 2, \ldots, 7$ in binary. So the code C is equivalent to the Hamming code H_3.

Furthermore, the polynomial $h(x) = \frac{f(x)}{g(x)}$ is equal to $x^3 + x + 1$, and therefore we have

$$h(A) = \begin{pmatrix} 1&0&0&0&1&0&1 \\ 1&1&0&0&0&1&0 \\ 0&1&1&0&0&0&1 \\ 1&0&1&1&0&0&0 \\ 0&1&0&1&1&0&0 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&0&1&1 \end{pmatrix}.$$

We can immediately verify that $g(A)h^t(A) = O$ and also that $\mathrm{r}\,(h(A)) = 4$. Taking 4 independent columns of $h(A)$ yields a generator matrix for C, e. g.

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Example 2. Consider the matrix A of (2.2) for $n = 8$ and $q = 3$ (so $(n, q) = 1$ again). Then

$$f(x) := f_A(x) = x^8 - 1.$$

Factorizing $f(x)$ into irreducible factors over $GF(3)$ yields

$$f(x) = f_1(x)f_2(x)f_3(x)f_4(x)f_5(x) = (x+1)(x-1)(x^2+1)(x^2+x-1)(x^2-x-1).$$

Next, we define

$$C := U_2 \oplus U_3 \oplus U_4 \oplus U_5,$$

corresponding to the function

$$g(x) := f_{\varphi|_C}(x) = f_2(x)f_3(x)f_4(x)f_5(x) = \frac{f(x)}{f_1(x)} = x^7-x^6+x^5-x^4+x^3-x^2+x-1.$$

It follows immediately that

$$g(A) = (-1\ 1\ -1\ 1\ -1\ 1\ -1\ 1)_c\,,$$

where the matrix $g(A)$ is represented by its first row. The other rows can be obtained by cyclic permutations of the first row, as is indicated by the subindex c. It will be obvious that $\mathrm{r}\,(g(A)) = 1$, and hence that $\dim C = 8 - 1 = 7$ (cf. also Proposition 5). The parity check matrix H for C is a $(1, 8)-$matrix which consists of the first row of $g(A)$. A generator matrix for C is obtained from $h(x) = x + 1$, which provides us with

$$h(A) = (1\ 0\ 0\ 0\ 0\ 0\ 0\ 1)_c\,.$$

Any $(7, 8)-$submatrix of $h^t(A)$ is a generator matrix for C.

Another possible choice for a liner cyclic code would be

$$C' := U_2 \oplus U_4,$$

with

$$g(x) = (x-1)(x^2+x-1) = x^3+x+1,$$

and

$$h(x) = (x+1)(x^2+1)(x^2-x-1) = x^5-x^3-x^2+x-1.$$

Consequently, we have $\dim C' = 3$. A parity check matrix for C' can be obtained by taking 5 independent rows from the matrix

$$g(A) = (1\ 0\ 0\ 0\ 0\ 1\ 0\ 1)_c\,,$$

e. g.

$$H = \begin{pmatrix} 1&0&1&1&0&0&0&0\\ 0&1&0&1&1&0&0&0\\ 0&0&1&0&1&1&0&0\\ 0&0&0&1&0&1&1&0\\ 0&0&0&0&1&0&1&1 \end{pmatrix}.$$

A generator matrix can be obtained by taking 3 independent columns from

$$h(A) = (1\ 0\ {-1}\ {-1}\ 1\ {-1}\ 0\ 0)_c\,,$$

e. g.

$$G = \begin{pmatrix} 1&0&0&-1&1&-1&-1&0\\ 0&1&0&0&-1&1&-1&-1\\ 0&0&-1&1&-1&-1&0&1 \end{pmatrix}.$$

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

Theorem 4. *$C = \Omega_1 \cup \ldots \cup \Omega_s$, where Ω_i are G-orbits and $k_i = |\Omega_i|$ is a divisor of $|G| = n$. In particular, $|C| = \sum\limits_{i=1}^{s} k_i$.*

Now we give a generalization of the previous results for constacyclic codes, which were first introduced in [2].

Definition 4. *Let a be a nonzero element of F. A code C with length n over F is called constacyclic with respect to a, if whenever $\mathbf{x} = (c_1, c_2, \ldots, c_n)$ is in C, so is $\mathbf{y} = (ac_n, c_1, \ldots, c_{n-1})$.*

Let a be a nonzero element of F and let

$$\psi_a : \begin{cases} F^n \to F^n \\ (x_1, x_2, \ldots, x_n) \mapsto (ax_n, x_1, \ldots, x_{n-1}) \end{cases}. \tag{2.5}$$

Then $\psi_a \in \mathrm{Hom}\, F^n$ and it has the following matrix

$$B_n(a) = B_n = \begin{pmatrix} 0&0&0&\ldots&a\\ 1&0&0&\ldots&0\\ 0&1&0&\ldots&0\\ \vdots&\vdots&\vdots&\ddots&\vdots\\ 0&0&0&\ldots&0 \end{pmatrix} \tag{2.6}$$

with respect to the basis $e = (\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n)$. Note that the relations $B_n(a)^{-1} = B_n(\frac{1}{a})^t$ and $B_n^n = aE$ hold. The characteristic polynomial of B_n is $f_{B_n}(x) = (-1)^n(x^n - a)$. We shall denote it by $f_a(x)$. We assume that $(n, q) = 1$. The polynomial $f_a(x)$ has no multiple roots and splits to distinct irreducible monic factors $f_a(x) = (-1)^n f_1(x) \ldots f_t(x)$. Let $U_i = \operatorname{Ker} f_i(\psi_a)$. It's easy to see that Theorem 1 and Proposition 2 are true in this case too. The following statement is clear from the definition.

Proposition 7. *A linear code C with length n over F is constacyclic iff C is a ψ_a-invariant subspace of F^n.*

The next theorem is analogous to Theorem 2 and so we omit its proof.

Theorem 5. *Let C be a linear constacyclic 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 $k := \dim_F C = k_{i_1} + \cdots + k_{i_s}$, where k_{i_r} is the dimension of U_{i_r};

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

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

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

5) $\mathrm{r}\,(g(B_n)) = n - k$, where $\mathrm{r}\,(g(B_n)) = n - k$ is the rank of the matrix $g(B_n)$.

Proposition 8. *The dual of a linear constacyclic code with respect to a is constacyclic with respect to $\dfrac{1}{a}$.*

Proof: The proof follows from the equality

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

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

$\square$

Example 3. As an example of a linear constacyclic code we take $n = 8,\ q = 3$ and $a = -1$ in (2.6). We than have the following characteristic polynomial

$$f(x) = f_{B_8}(x) = x^8 + 1.$$

When splitting this polynomial into irreducible polynomials over $GF(3)$, we find

$$f(x) = f_1(x) f_2(x) = (x^4 + x^2 - 1)(x^4 - x^2 - 1),$$

where the factors $f_1(x)$ and $f_2(x)$ define minimal ψ_a-invariant subspaces U_1 and U_2, respectively, both of dimension 4 according to Theorem 5. If we define

$$C = U_1,\ C' = U_2,$$

then we find, similarly as in Example 2, that a parity check matrix H for code C is obtained from

$$g(B_8) = f_1(B_8) = \begin{pmatrix} -1 & 0 & 0 & 0 & -1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 & 0 & -1 & 0 & -1 \\ 1 & 0 & -1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & -1 \\ 1 & 0 & 1 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & -1 \end{pmatrix}$$

by taking 4 independent rows, whereas a parity check matrix H' for C' is obtained in the same way from

$$g'(B_8) = f_2(B_8) = \begin{pmatrix} -1 & 0 & 0 & 0 & -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 & 0 & -1 & 0 & 1 \\ -1 & 0 & -1 & 0 & 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & -1 & 0 & 0 & 0 & -1 \\ 1 & 0 & -1 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 & 0 & -1 \end{pmatrix}.$$

Similarly to the case of cyclic matrices, we shall denote the above matrices by

$$g(B_8) = f_1(B_8) = (-1\ 0\ 0\ 0\ -1\ 0\ -1\ 0)_{ac}$$

and

$$g'(B_8) = f_2(B_8)) = (-1\ 0\ 0\ 0\ -1\ 0\ 1\ 0)_{ac}\,,$$

respectively. The index ac means that each next row can be obtained from its predecessor by applying the operator ψ_a as defined in (2.5). Furthermore, we have the matrices

$$h(B_8) = f_2(B_8),\ h'(B_8) = f_1(B_8).$$

It is an easy task to verify that the following relations hold

$$g(B_8)h(B_8) = O,\ g'(B_8)h'(B_8) = O.$$

Actually, both equalities are equivalent to the relation $f_1(B_8)f_2(B_8) = O$, and the codes C and C' are each other's dual.

3. **LINEAR QUASI-TWISTED CODES AS INVARIANT SUBSPACES**

Let $F = \mathrm{GF}(q)$ and let F^n be the n-dimensional vector space over F with the standard basis $\mathbf{e}_1 = (1, 0, \dots, 0)$, $\mathbf{e}_2 = (0, 1, \dots, 0), \dots, \mathbf{e}_n = (0, 0, \dots, 1)$.

Let a be a nonzero element of F and let

$$\psi_a : \begin{cases} F^n \to F^n \\ (x_1, x_2, \dots, x_n) \mapsto (ax_n, x_1, \dots, x_{n-1}) \end{cases}. \tag{3.1}$$

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

$$B_n(a) = B_n = \begin{pmatrix} 0 & 0 & 0 & \dots & a \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix} \tag{3.2}$$

with respect to the basis $e = (\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n)$. The characteristic polynomial of B_n is

$$f_{B_n}(x) = \begin{vmatrix} -x & 0 & 0 & \dots & a \\ 1 & -x & 0 & \dots & 0 \\ 0 & 1 & -x & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & -x \end{vmatrix} = (-1)^n (x^n - a). \tag{3.3}$$

Let k be a fixed divisor of n and let $n = kl$. Let us consider the operator $\varphi = (\psi_a)^k$. We define a new basis $g = (\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_n)$ of F^n as follows:

$$\begin{array}{llllll} \mathbf{g}_1 & = \mathbf{e}_1, \ \mathbf{g}_2 & = \mathbf{e}_{1+k}, & \dots, & \mathbf{g}_l & = \mathbf{e}_{1+(l-1)k} \\ \mathbf{g}_{l+1} & = \mathbf{e}_2, \ \mathbf{g}_{l+2} & = \mathbf{e}_{2+k}, & \dots, & \mathbf{g}_{2l} & = \mathbf{e}_{2+(l-1)k} \\ \dots\dots & \dots\dots & \dots\dots & \dots & \dots & \dots\dots \\ \mathbf{g}_{(k-1)l+1} & = \mathbf{e}_k, \ \mathbf{g}_{(k-1)l+2} & = \mathbf{e}_{2k}, & \dots, & \mathbf{g}_{kl} & = \mathbf{e}_{k+(l-1)k} \end{array}.$$

Then φ is represented by the following matrix

$$B = \begin{pmatrix} B_l & & & \\ & B_l & & \\ & & \ddots & \\ & & & B_l \end{pmatrix} \tag{3.4}$$

with respect to g, where the k matrices B_l are defined as in (3.1) with $n = l$. Therefore the characteristic polynomial of B is

$$f_B(x) = (f_{B_l}(x))^k = (-1)^n (x^l - a)^k.$$

Let us denote by $f(x)$ the polynomial $x^l - a$ and let $f(x) = f_1(x) f_2(x) \dots f_t(x)$ be the factorization of $f(x)$ into irreducible factors over F. According to the Theorem of Cayley-Hamilton the matrix B of (3.4) satisfies

$$f(B) = O. \tag{3.5}$$

We assume that $(n, q) = 1$. In that case $f(x)$ has distinct factors $f_i(x)$, $i = 1, \dots, t$, which are monic. Furthermore, we consider the homogeneous set of equations

$$f_i(B)\mathbf{x} = \mathbf{0},\ \mathbf{x} \in F^n \tag{3.6}$$

for $i = 1, \dots, t$. If U_i stands for the solution space of (3.6), then we may write $U_i = \operatorname{Ker} f_i(\varphi)$. We also introduce the following linear subspaces of F^n :

$$\begin{array}{l} V_1 = \ell(\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_l), \\ V_2 = \ell(\mathbf{g}_{l+1}, \mathbf{g}_{l+2}, \dots, \mathbf{g}_{2l}), \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ V_k = \ell(\mathbf{g}_{(k-1)l+1}, \mathbf{g}_{(k-1)l+2}, \dots, \mathbf{g}_{kl}) \end{array}.$$

Note that $V_1, \dots, V_k$ are $\varphi-$invariant subspaces of F^n.

The next proposition is analogous to Theorem 1 properties 1), 2) and so we omit its proof.

Proposition 9. *The subspaces $U_1, U_2, \dots, U_t$ of F^n are $\varphi-$invariant. If W is a $\varphi-$invariant subspace of F^n and $W_i = W \cap U_i$ for $i = 1, \dots, t$, then W_i is $\varphi-$invariant and $W = W_1 \oplus \cdots \oplus W_t$.*

Corollary 1. $F^n = U_1 \oplus \cdots \oplus U_t$.

Proof: This follows from Proposition 9 with $W = F^n$.

□

Let us denote $U_{ij} = U_i \cap V_j$ for all $i = 1, \dots, t$ and $j = 1, \dots, k$. Then we have the following result.

Corollary 2. $V_j = U_{1j} \oplus \cdots \oplus U_{tj}$, $j = 1, \dots, k$.

Proof: This follows from Proposition 9 with $W = V_j$.

□

Theorem 6. *The subspaces U_{ij} of F^n satisfy the following properties:*

1) U_{ij} is a φ-invariant subspace of F^n;

2) if $\mathbf{v}$ is a nonzero vector of U_{ij}, then the vectors $\mathbf{v}$, $\varphi(\mathbf{v})$, $\dots$, $\varphi^{\deg f_i - 1}(\mathbf{v})$ form a basis of U_{ij} and in particular $\dim U_{ij} = \deg f_i$;

3) U_{ij} is a minimal φ-invariant subspace of F^n;

4) $U_{i1} \cong U_{i2} \cong \cdots \cong U_{ik}$;

5) $U_i = U_{i1} \oplus \cdots \oplus U_{ik}$;

6) $F^n = \bigoplus_{i,j} U_{ij}$.

Proof:

1) This is clear from the definition of U_{ij}.

2) Let $\mathbf{0} \neq \mathbf{v} \in U_{ij}$ be an arbitrary nonzero vector and let $m \geq 1$ be the smallest natural number with the property that the vectors $\mathbf{v}, \varphi(\mathbf{v}), \ldots, \varphi^m(\mathbf{v})$ are linearly dependent. Then there are elements $a_0, \ldots, a_{m-1} \in F$, at least one of which is nonzero, such that

$$\varphi^m(v) = a_0 v + a_1\varphi(v) + \cdots + a_{m-1}\varphi^{m-1}(v).$$

Consider the polynomial $t(x) = x^m - a_{m-1}x^{m-1} - \cdots - a_0 \in F[x]$. Since $(t(\varphi))(\mathbf{v}) = (f_i(\varphi))(\mathbf{v}) = \mathbf{0}$, it follows that $[(t(x), f_i(x))(\varphi)](\mathbf{v}) = \mathbf{0}$. But $(t(x), f_i(x))$ is equal to 1 or to $f_i(x)$. If we assume that $(t(x), f_i(x)) = 1$, then $\mathbf{v} = \mathbf{0}$, which contradicts the choice of $\mathbf{v}$. Hence, $(t(x), f_i(x)) = f_i(x)$ and $f_i(x)$ divides $t(x)$. Thus $\deg f_i(x) \leq \deg t(x) = m$. On the other hand, the vectors $\mathbf{v}, \varphi(\mathbf{v}), \ldots, \varphi^{\deg f_i}(\mathbf{v})$ are linearly dependent, since $(f_i(\varphi))(\mathbf{v}) = \mathbf{0}$, and from the minimality of m we obtain $m = \deg f_i$. Therefore $\dim U_{ij} \geq \deg f_i$, and so

$$l = \dim{}_F V_j = \sum_{i=1}^{t} \dim{}_F U_{ij} \geq \sum_{i=1}^{t} \deg f_i = \deg f = l$$

and $\dim{}_F U_{ij} = \deg f_i$.

3) Let V be a φ- invariant subspace of F^n and let $\{\mathbf{0}\} \neq V \subseteq U_{ij}$. If $\mathbf{0} \neq \mathbf{v} \in V$, then the vectors $\mathbf{v}, \varphi(\mathbf{v}), \ldots, \varphi^{\deg f_i - 1}(\mathbf{v}) \in V$ are linearly independent. Therefore $\dim{}_F V \geq \dim{}_F U_{ij}$ and $V = U_{ij}$.

4) This follows from the fact that $\dim{}_F U_{i1} = \dim{}_F U_{i2} = \cdots = \dim{}_F U_{ik} = \deg f_i$.

5) Let $\mathbf{v} \in U_i$. Since $F^n = V_1 \oplus \cdots \oplus V_k$, we have $\mathbf{v} = \mathbf{v}_1 + \cdots + \mathbf{v}_k$, where $\mathbf{v}_j \in V_j$, $j = 1, \ldots, k$. Then $f_i(\varphi)(\mathbf{v}) = f_i(\varphi)(\mathbf{v}_1) + \cdots + f_i(\varphi)(\mathbf{v}_k) = \mathbf{0}$, so that $f_i(\varphi)(\mathbf{v}_j) = \mathbf{0}$, i.e., $\mathbf{v}_j \in U_i$. Hence, $\mathbf{v}_j \in U_{ij}$ and

$$U_i = U_{i1} + \cdots + U_{ik}.$$

Assume that $\mathbf{v} \in U_{ij} \cap \sum_{s \neq j} U_{is}$, then $\mathbf{v} \in V_j$ and $\mathbf{v} \in \sum_{s \neq j} V_s$. But $V_j \cap \sum_{s \neq j} V_s = \{\mathbf{0}\}$, so we obtain that $\mathbf{v} = \mathbf{0}$. Thus

$$U_i = U_{i1} \oplus \cdots \oplus U_{ik}.$$

6) By property 5) we obtain that

$$F^n = \bigoplus_{i=1}^{t} U_i = \bigoplus_{i,j} U_{ij}.$$

$\square$

Proposition 10. *Let W be a φ-invariant subspace of U_i. Then there exists a natural number $s \leq k$ such that $W \cong U_{i1}^s$, where U_{i1}^s is isomorphic to the direct sum of s copies of U_{i1}.*

Proof: Let $\mathbf{0} \neq \mathbf{w}_1 \in W$. Then the vectors $\mathbf{w}_1$, $\varphi(\mathbf{w}_1), \dots, \varphi^{\deg f_i - 1}(\mathbf{w}_1)$ are linearly independent. We define $W_1 := \ell(\mathbf{w}_1, \varphi(\mathbf{w}_1), \dots, \varphi^{\deg f_i - 1}(\mathbf{w}_1))$. Let $\mathbf{0} \neq \mathbf{w}_2 \in W$ be a vector such that $\mathbf{w}_2 \notin W_1$. Then the vectors $\mathbf{w}_2$, $\varphi(\mathbf{w}_2), \dots, \varphi^{\deg f_i - 1}(\mathbf{w}_2)$ are linearly independent. Define $W_2 := \ell(\mathbf{w}_2, \varphi(\mathbf{w}_2), \dots, \varphi^{\deg f_i - 1}(\mathbf{w}_2))$. Note that $\dim W_1 = \dim W_2 = \deg f_i$. We will prove that the vectors

$$\mathbf{w}_1,\ \varphi(\mathbf{w}_1), \dots, \varphi^{\deg f_i - 1}(\mathbf{w}_1),\ \mathbf{w}_2,\ \varphi(\mathbf{w}_2), \dots, \varphi^{\deg f_i - 1}(\mathbf{w}_2)$$

are also linearly independent. Assume the opposite. Then there exist nonzero polynomials $h_1(x)$, $h_2(x) \in F[x]$, $\deg h_1, \deg h_2 < \deg f_i$, such that $h_1(B)\mathbf{w}_1 + h_2(B)\mathbf{w}_2 = \mathbf{0}$. Since f_i is irreducible, we have that $(h_2, f_i) = 1$, for $i = 1, \dots, t$, and therefore by the Euclidean algorithm there are polynomials $a(x), b(x) \in F[x]$, such that $a(x)h_2(x) + b(x)f_i(x) = 1$. Hence, $a(B)h_2(B)\mathbf{w}_2 + b(B)f_i(B)\mathbf{w}_2 = \mathbf{w}_2$. Now $\mathbf{w_2} \in U_i$ and therefore $f_i(B)\mathbf{w}_2 = \mathbf{0}$. Thus we obtain that $a(B)h_2(B)\mathbf{w}_2 = \mathbf{w}_2$. From $h_2(B)(\mathbf{w}_2) = -h_1(B)(\mathbf{w}_1)$ and the last equality we conclude that $\mathbf{w}_2 \in W_1$. This contradiction proves the statement. We proceed analogously until we obtain that $W = W_1 \oplus \dots \oplus W_s$ for some $s \leq k$. Since $\dim W_i = \deg f_i$, $i = 1, \dots, s$, it follows that $W \cong U_{i1}^s$.

□

Theorem 7. *Let W be a $\varphi-$invariant subspace of F^n. Then*

$$W \cong U_{11}^{s_1} \oplus \dots \oplus U_{t1}^{s_t}$$

for integers $s_i \leq k$, $1 \leq i \leq t$. In particular,

$$\dim W = \sum_{i=1}^{t} s_i \deg f_i.$$

Proof: This follows immediately from Proposition 9 and Proposition 10 .

□

Definition 5. *A code C with length n over F is called a k-quasi-twisted code with respect to $a \in F^*$ iff any codeword in C is again a codeword in C after an a-constacyclic shift over k positions.*

The following statement is clear from the definition.

Proposition 11. *A linear code C with length n over F is k-quasi-twisted iff C is a $\varphi-$invariant subspace of F^n.*

Theorem 8. *Let C be a linear $k-$quasi-twisted code with length n over F. Then*

$$C \cong U_{11}^{s_1} \oplus \cdots \oplus U_{t1}^{s_t}$$

for integers $s_i \leq k$, $1 \leq i \leq t$. In particular,

$$\dim C = \sum_{i=1}^{t} s_i \deg f_i.$$

Proof: This follows from Theorem 7 and Proposition 11.

□

Example 4. Substituting $n = 15,\ q = 2,\ k = 5,\ l = 3$ and $a = 1$ in (3.2) and (3.4) gives the representation matrix

$$B = \begin{pmatrix} B_3 & & & & \\ & B_3 & & & \\ & & B_3 & & \\ & & & B_3 & \\ & & & & B_3 \end{pmatrix}$$

for the operator φ with respect to the basis g, with

$$B_3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

For the characteristic polynomial of B we have

$$f_B(x) = (-1)(x^3 - 1)^5 = -(f(x))^5,$$

where $f(x)$ can be factorized into irreducible polynomials over $GF(2)$ as

$$f(x) = f_1(x) f_2(x) = (x+1)(x^2+x+1).$$

Let $U_i = \operatorname{Ker} f_i(\varphi)$ for $i = 1, 2$. We define the following linear code

$$C = U_2.$$

According to Theorem 6 we can write

$$U_2 = U_{21} \oplus \cdots \oplus U_{25},$$

where $U_{2j} = U_2 \cap V_j$ and $U_{21} \cong \cdots \cong U_{25}$. If we introduce subcodes $C_i := U_{2i}$ for $i = 1, \ldots 5$, then $\dim C_i = \deg f_2 = 2$, again by Theorem 6. One can almost immediately infer that

$$g(B_3) = f_2(B_3) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

and

$$h(B_3) = f_1(B_3) = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

So a parity check matrix for the subcode $C_i,\ i = 1, \ldots, 5$, restricted to its support, is the row matrix $(1, 1, 1)$. For C itself we find the parity check matrix

$$H = \begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix},$$

where $\mathbf{1}$ stands for $(1, 1, 1)$ and $\mathbf{0}$ for $(0, 0, 0)$. Hence, $\dim C = 15 - 5 = 10$, which is in agreement with Theorem 8.

Taking two independent columns of $h(B_3)$ yields a generator matrix for C_i (restricted to its support), e.g.

$$G_i = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

This gives rise to the following generator matrix for C itself

$$G = \begin{pmatrix} \mathbf{a} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{b} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{a} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{b} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{a} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{b} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{a} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{b} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{a} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{b} \end{pmatrix},$$

with $\mathbf{0} = (0, 0, 0),\ \mathbf{a} = (1, 1, 0)$ and $\mathbf{b} = (0, 1, 1)$. This generator matrix G has been written with respect to the basis g. When writing the rows of G with respect to the standard basis e, the matrix takes the following form

$$G = \begin{pmatrix}
1&0&0&0&0&1&0&0&0&0&0&0&0&0&0 \\
0&0&0&0&0&1&0&0&0&0&1&0&0&0&0 \\
0&1&0&0&0&0&1&0&0&0&0&0&0&0&0 \\
0&0&0&0&0&0&1&0&0&0&0&1&0&0&0 \\
0&0&1&0&0&0&0&1&0&0&0&0&0&0&0 \\
0&0&0&0&0&0&0&1&0&0&0&0&1&0&0 \\
0&0&0&1&0&0&0&0&1&0&0&0&0&0&0 \\
0&0&0&0&0&0&0&0&1&0&0&0&0&1&0 \\
0&0&0&0&1&0&0&0&0&1&0&0&0&0&0 \\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&1 \\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&1 \\
0&0&0&1&0&0&0&0&0&0&0&0&0&1&0
\end{pmatrix}.$$

Example 5. Now we take $n = 18,\ q = 5,\ k = 3,\ l = 6$ and $a = 2$, providing us with matrices

$$B = \begin{pmatrix} B_6 & & \\ & B_6 & \\ & & B_6 \end{pmatrix}, \quad B_6 = \begin{pmatrix} 0&0&0&0&0&2 \\ 1&0&0&0&0&0 \\ 0&1&0&0&0&0 \\ 0&0&1&0&0&0 \\ 0&0&0&1&0&0 \\ 0&0&0&0&1&0 \end{pmatrix}.$$

The characteristic polynomial of B is

$$f_B(x) = (x^6 - 2)^3 = (f(x))^3.$$

It turns out that we can write

$$f(x) = f_1(x)f_2(x)f_3(x) = (x^2 + 2)(x^2 + x + 2)(x^2 + 4x + 2),$$

where the f_i are irreducible polynomials over $GF(5)$.

Again we define $U_i = \operatorname{Ker} f_i(\varphi)$ for $i = 1, 2, 3$, and we introduce the linear code

$$C = U_1 \oplus U_2.$$

The defining polynomial of C is

$$g(x) = f_1(x)f_2(x) = x^4 + x^3 + 4x^2 + 2x + 4,$$

from which we obtain the matrix

$$g(B_6) = \begin{pmatrix} 4&0&2&2&3&4 \\ 2&4&0&2&2&3 \\ 4&2&4&0&2&2 \\ 1&4&2&4&0&2 \\ 1&1&4&2&4&0 \\ 0&1&1&4&2&4 \end{pmatrix}.$$

The code of length 6 determined by $g(x)$ is a constacyclic code $\overline{C}$ with respect to $2 \in GF(5)$ with dimension 4 (cf. Theorem 5). Hence, the matrix $g(B_6)$ has rank $6 - 4 = 2$, as one can easy verify. By taking two independent rows, e. g. the first two, one obtains a parity check matrix for $\overline{C}$. A generator matrix for $\overline{C}$ can be constructed from the polynomial $h(x) = f_3(x) = x^2 + 4x + 2$ which determines the matrix

$$h(B_6) = \begin{pmatrix} 2&0&0&0&2&3 \\ 4&2&0&0&0&2 \\ 1&4&2&0&0&0 \\ 0&1&4&2&0&0 \\ 0&0&1&4&2&0 \\ 0&0&0&1&4&2 \end{pmatrix}.$$

By taking the first four columns of $h(B_6)$ we obtain a generator matrix for $\overline{C}$:

$$G_{\overline{C}} = \begin{pmatrix} 2&4&1&0&0&0 \\ 0&2&4&1&0&0 \\ 0&0&2&4&1&0 \\ 0&0&0&2&4&1 \end{pmatrix}.$$

That this matrix really generates a constacyclic code with respect to 2, can rather easily be verified. It is sufficient to check that $(2\,0\,0\,0\,2\,4)$ -which is the constacyclic permutation of the last word of the matrix- is a linear combination of the first three.

Just like in Example 4, it follows that the following matrix generates the complete code C :

$$G = \begin{pmatrix} G_{\overline{C}} & O & O \\ O & G_{\overline{C}} & O \\ O & O & G_{\overline{C}} \end{pmatrix},$$

where O stands for the $(4,6)-$zeromatrix. The rows in this matrix are codewords of C with respect to the basis g. To obtain a generator with respect to the standard basis e, one has to carry out the basis transformation, described on page 9.

Example 6. Like in Example 5 we take again $n = 18,\ q = 5,\ k = 3,\ l = 6$ and $a = 2$. Now we consider the codes $C_1 := U_1$ and $C_2 := U_2$.

The code C_1 is defined by $g_1(x) = f_1(x) = x^2 + 2$. Similarly as in all previous examples we find the matrices

$$g_1(B_6) = \begin{pmatrix} 2&0&0&0&2&0 \\ 0&2&0&0&0&2 \\ 1&0&2&0&0&0 \\ 0&1&0&2&0&0 \\ 0&0&1&0&2&0 \\ 0&0&0&1&0&2 \end{pmatrix}$$

and

$$h_1(B_6) = \begin{pmatrix} 4&0&2&0&1&0 \\ 0&4&0&2&0&1 \\ 3&0&4&0&2&0 \\ 0&3&0&4&0&2 \\ 1&0&3&0&4&0 \\ 0&1&0&3&0&4 \end{pmatrix}.$$

Since $\dim C_1 = 2$, a generator matrix $G_{\overline{C_1}}$ for $\overline{C_1}$ (the restriction of C_1 with respect to its support) is obtained by taking 2 independent columns of $h_1(B_6)$.

The code C_2 is defined by $g_2(x) = f_2(x) = x^2 + x + 2$. For this code we find the matrices

$$g_2(B_6) = \begin{pmatrix} 2&0&0&0&2&2 \\ 1&2&0&0&0&2 \\ 1&1&2&0&0&0 \\ 0&1&1&2&0&0 \\ 0&0&1&1&2&0 \\ 0&0&0&1&1&2 \end{pmatrix}$$

and

$$h_2(B_6) = \begin{pmatrix} 4&0&2&3&3&1 \\ 3&4&0&2&3&3 \\ 4&3&4&0&2&3 \\ 4&4&3&4&0&2 \\ 1&4&4&3&4&0 \\ 0&1&4&4&3&4 \end{pmatrix}.$$

A generator matrix $G_{\overline{C_2}}$ for $\overline{C_2}$ can be obtained by taking 2 independent columns of $h_2(B_6)$.

Finally, the code $C_3 := U_3$ is defined by $g_3(x) = f_3(x) = x^2 + 4x + 2$. This code is the dual of $C = C_1 \oplus C_2$. So, the matrix $g_3(B_6)$ is equal to the matrix $h(B_6)$ presented in Example 5. Indeed, we find

$$g_3(B_6) = \begin{pmatrix} 2&0&0&0&2&3 \\ 4&2&0&0&0&2 \\ 1&4&2&0&0&0 \\ 0&1&4&2&0&0 \\ 0&0&1&4&2&0 \\ 0&0&0&1&4&2 \end{pmatrix},$$

while

$$h_3(B_6) = \begin{pmatrix} 4&0&2&2&3&4 \\ 2&4&0&2&2&3 \\ 4&2&4&0&2&2 \\ 1&4&2&4&0&2 \\ 1&1&4&2&4&0 \\ 0&1&1&4&2&4 \end{pmatrix}.$$

A generator matrix $G_{\overline{C_3}}$ for $\overline{C_3}$ is obtained by taking 2 independent columns of $h_3(B_6)$.

It will be obvious that the matrix

$$G_i = \begin{pmatrix} G_{\overline{C_i}} & O & O \\ O & G_{\overline{C_i}} & O \\ O & O & G_{\overline{C_i}} \end{pmatrix}$$

is a generator matrix for the complete code C_i, for $i = 1, 2, 3$.

One can easily check that the six rows of the matrices G_i, $i = 1, 2, 3$, are independent. So, it follows that

$$F^n = U_1 \oplus U_2 \oplus U_3$$

(cf. Corollary 1). Furthermore, the minimal $\varphi-$invariant subspace U_i, is spanned by the rows of the submatrix $(G_{\overline{C_i}}\ O\ O)$. We shall denote this fact by

$$U_{i1} = \ell(G_{\overline{C_i}}\ O\ O),\ \ i = 1, 2, 3.$$

Similarly, we can write

$$U_{i2} = \ell(O\ G_{\overline{C_i}}\ O),\ \ i = 1, 2, 3,$$

and

$$U_{i3} = \ell(O\ O\ G_{\overline{C_i}}),\ \ i = 1, 2, 3.$$

It follows immediately that

$$U_i = U_{i1} \oplus U_{i2} \oplus U_{i3}$$

and

$$V_j = U_{1j} \oplus U_{2j} \oplus U_{3j},$$

which illustrates Theorem 6 (5) and Corollary 2, respectively.

4. REFERENCES

1. MacWilliams F. G., Sloane N. J. A. The Theory of Error Correcting Codes. North-Holland Publ. Company, Amsterdam, 1977.
2. Berlekamp E. R., Algebraic Coding Theory, Mc Graw-Hill Book Company, New York, 1968.