In this article, we shall study the structure of $(a + bu)$-constacyclic codes of arbitrary length over the ring $R = F_q + uF_q + \cdots + u^{e-1}F_q$, where $u^e = 0$, $q$ is a power of a prime number $p$ and $a, b$ are non-zero elements of $F_q$. Also we shall find a minimal spanning set for these codes. For a constacyclic code $C$ we shall determine its minimum Hamming distance with some properties of $Tor(C)$ as an $a$-constacyclic code over $F_q$.

1. INTRODUCTION

Constacyclic codes are some generalizations of cyclic codes. These codes are important in theory of error-correcting codes and have practical applications as they can be encoded with shift register.

The class of constacyclic codes over finite fields have been studied [1, 2]. Recently, the structures of constacyclic codes whose lengths are powers of a prime $p$ have been studied over $F_{p^m} + uF_{p^m}$, where $u^2 = 0$, by Dinh [3]. Also, Jitman and Udomkavanich, in [4], determined
the structure of constacyclic codes of lengths \( p^s \) over \( F_p^k + uF_p^k + \cdots + u^{e-1}F_p^k \), where \( u^m = 0 \).

In [2], Kai, Zhu and Li specify the structure of \( (1 + \lambda u) - \) Constacyclic codes over \( \frac{F_q[x]}{<x^m - \lambda>} \).

Let \( F_q \) be a finite field with \( q = p^r \) elements and \( p \) a prime number. Consider the ring \( R = F_q + uF_q + \cdots + u^{e-1}F_q \), where \( u^e = 0 \). In fact, \( R \) is a finite chain ring with \( q^e \) elements and with the maximal ideal \( < u > \). A code \( C \) of length \( n \) over \( R \) is a subset of \( R^n \). We say that the code is linear, if \( C \) is an \( R \)-submodule of \( R^n \). For a given unit \( \lambda \in R \), a code \( C \) is said to be \( \lambda \)-constacyclic, if \( (\lambda c_{n-1}, c_0, \ldots, c_{n-2}) \in C \), for \( (c_0, c_1, \ldots, c_{n-1}) \in C \).

In \( R^n \), any \( n \)-array \( (c_0, c_1, \ldots, c_{n-1}) \) corresponds to a polynomial with degree less than \( n \), say \( \sum_{i=0}^{n-1} c_i x^i \). With this corresponding, any \( \lambda \)-constacyclic code of length \( n \) over \( R \) is identified with an ideal of the quotient ring \( \frac{R[x]}{<x^n - \lambda>} \).

In this paper, we are concerned with the \( \lambda \)-constacyclic codes of arbitrary length \( n \) over \( R = F_q + uF_q + \cdots + u^{e-1}F_q \), where \( u^e = 0 \) and \( \lambda = a + bu \) for some \( a, b \in F_q^* \). We completely determine the structure of constacyclic codes of length \( n \) over \( R \) as the ideals of the principal ideal ring \( \frac{R[x]}{<x^n - (a + bu)>} \). Also, we shall find a minimal spanning set for these codes. Finally, for an \( (a + bu) - \) constacyclic code \( C \) over \( R \) we introduce \( Tor(C) \), as an ideal of \( \frac{F_q[x]}{<x^n - a>} \) and we shall show that \( d_H(C) = d_H(Tor(C)) \).

From now on, we suppose that \( n = p^s m \), where \( gcd(p, m) = 1 \), unless stated otherwise. Let \( a, b \) be non-zero elements in \( F_q \) and \( S = \frac{R[x]}{<x^n - (a + bu)>} \).

2. Some characterizations of \((a + bu) - \text{constacyclic codes}\)

First, note that every polynomial \( k(x) \) in \( R[x] \) can be uniquely written as \( k(x) = k_0(x) + uk_1(x) + \cdots + u^{e-1}k_{e-1}(x) \), where \( k_i(x) \in F_q[x] \), \( 0 \leq i \leq e - 1 \).

We have the following lemma whose proof is straightforward.

**Lemma 2.1.** For any \( i \), \( 0 \leq i \leq e - 1 \), let \( k_i(x) \) be polynomials of degree less than \( n \) in \( F_q[x] \). Suppose that \( k_0(x) + uk_1(x) + \cdots + u^{e-1}k_{e-1}(x) = 0 \) in \( S \). Then \( k_0(x) = k_1(x) = \cdots = k_{e-1}(x) = 0 \) in \( F_q[x] \).

**Corollary 2.2.** Every polynomial \( k(x) \) in \( S \) can be uniquely written as \( k(x) = k_0(x) + uk_1(x) + \cdots + u^{e-1}k_{e-1}(x) \), where \( k_i(x) \in F_q[x] \), \( 0 \leq i \leq e - 1 \), and \( \deg k_i < n \).

Consider the ring \( T_e = \frac{F_q[x]}{<x^n - a>} \). Since \( F_q[x] \) is a principal ideal domain, every ideal of \( T_e \) is principal. Hence \( T_e \) is a principal ideal ring. By the division algorithm in \( F_q[x] \), every element \( k(x) \in T_e \) with \( \deg k < e n \) can be uniquely written as

\[
k(x) = k_0(x) + k_1(x)(x^n - a) + \cdots + k_{e-1}(x)(x^n - a)^{e-1},
\]

where \( \deg k_i < n \) ( \( 0 \leq i \leq e - 1 \)).

In the ring \( S \) we have \( u = b^{-1}(x^n - a) \). Now, applying Corollary 2.2, there exists an isomorphism \( \psi \) from \( S \) onto \( T_e \) which maps \( u \) to \( b^{-1}(x^n - a) \). In fact, we have the following proposition.
Proposition 2.3. Let \( \psi : S \to T_e \) be defined by
\[
\psi(\sum_{i=0}^{e-1} u^i k_i(x)) = \sum_{i=0}^{e-1} b^{-i}(x^n - a)^i k_i(x),
\]
where \( k_i(x) \in F_q[x] \), for any \( i \), \( 0 \leq i \leq e - 1 \) and \( \deg k_i < n \). Then \( \psi \) is a ring isomorphism as well as an \( F_q[x] \)-homomorphism.

Proof. Obviously, \( \psi \) is an additive homomorphism. Assume that \( k(x) = \sum_{i=0}^{e-1} u^i k_i(x) \) and \( l(x) = \sum_{i=0}^{e-1} u^i l_i(x) \) are two elements of \( S \), where \( k_i(x), l_i(x) \in F_q[x] \), \( \deg k_i < n \) and \( \deg l_i < n \), \( 0 \leq i \leq e - 1 \). Now,
\[
k(x)l(x) = \sum_{i=0}^{e-1} u^i(\sum_{j=0}^{i} k_j(x)l_{i-j}(x))
\]
\[
= \sum_{i=0}^{e-1} \sum_{j=0}^{i} u^i k_j(x)l_{i-j}(x).
\]

Assume that for any \( i \), \( 0 \leq i \leq e - 1 \), \( h_i(x) \in F_q[x] \) is coefficient of \( u^i \). we can see that \( \deg h_i \leq 2n - 2 \). In \( F_q[x] \), there exist \( q_i(x) \) and \( s_i(x) \) such that \( h_i(x) = (x^n - a)q_i(x) + s_i(x) \), where \( \deg s_i < n \) and \( \deg q_i < n - 2 \). So in \( S \), \( h_i(x) = buq_i(x) + s_i(x) \). Hence
\[
k(x)l(x) = s_0(x) + \sum_{i=1}^{e-1} u^i(bq_{i-1}(x) + s_i(x)).
\]

Thus
\[
\psi(k(x)l(x)) = s_0(x) + \sum_{i=1}^{e-1} b^{-i}(x^n - a)^i(bq_{i-1}(x) + s_i(x)).
\]

Also,
\[
\psi(k(x))\psi(l(x)) = \sum_{i=0}^{e-1} \sum_{j=0}^{i} b^{-i}(x^n - a)^j k_j(x)l_{i-j}(x)
\]
\[
= \sum_{i=0}^{e-1} b^{-i}(x^n - a)^i((x^n - a)q_i(x) + s_i(x))
\]
\[
= \sum_{i=0}^{e-1} b^{-i}(x^n - a)^{i+1}q_i(x) + (x^n - a)^i s_i(x)
\]
\[
= s_0(x) + \sum_{i=1}^{e-1} b^{-i}(x^n - a)^i(bq_{i-1}(x) + s_i(x)).
\]

Therefore \( \psi(k(x)l(x)) = \psi(k(x))\psi(l(x)) \). This show that \( \psi \) is a ring homomorphism. Suppose that \( k(x) \in T_e \) and \( \deg k < en \). By the division algorithm in \( F_q[x] \),
\[ k(x) = k_0(x) + k_1(x)(x^n - a) + \cdots + k_{e-1}(x)(x^n - a)^{e-1}, \]

where \( \text{deg } k_i < n \) \((0 \leq i \leq e - 1)\). We can see that \( \psi(\sum_{i=0}^{e-1} b_i u^i k_i(x)) = k(x) \). Hence \( \psi \) is an epimorphism. The rest of the proof is straightforward. □

**Remark 2.4.**

i) Since \( T_e \) is a principal ideal ring, \( S \) is too. We shall now determine the unique form of a generator of an ideal of \( S \).

ii) Note that, here \( b \neq 0 \). The reader should be careful that the ideals of \( S \) are different from the ideals of the ring \( \frac{R[x]}{\langle x^n - a \rangle} \) (this ring is not a principal ideal ring).

Let \( a = a_0^{p^e} \), where \( a_0 \in F_q^* \) (note that \( a \) has a unique \( p^e \)-th root in \( F_q^* \)). Thus \((x^n - a) = (x^m - a_0)^{p^e}\). Assume that \( x^n - a_0 = f_1 f_2 \cdots f_\eta \), where \( f_i \), \( 1 \leq i \leq \eta \), are distinct monic irreducible polynomials in \( F_q[x] \). Hence \((x^n - a) = \prod_{i=1}^{\eta} f_i^{p^e} \). Every ideal of \( T_e \) has a monic generator of the form \( \prod_{i=1}^{\eta} f_i^{\alpha_i} \), \( 0 \leq \alpha_i \leq ep^e \) and a result of the following lemma is the uniqueness of this generator.

**Lemma 2.5.** Let \( C = \langle \prod_{i=1}^{\eta} f_i^{\alpha_i} \rangle \) and \( D = \langle \prod_{i=1}^{\eta} f_i^{\beta_i} \rangle \) be two ideals of \( T_e \), where \( 0 \leq \alpha_i, \beta_i \leq ep^e \). If \( C \subseteq D \), then \( \beta_i \leq \alpha_i \) for any \( i \), \( 1 \leq i \leq \eta \) and in fact, in \( F_q[x] \), \( \prod_{i=1}^{\eta} f_i^{\beta_i} \mid \prod_{i=1}^{\eta} f_i^{\alpha_i} \).

**Proof.** Since \( C \subseteq D \), there exist polynomials \( k(x) \) and \( h(x) \) in \( F_q[x] \) such that

\[
\prod_{i=1}^{\eta} f_i^{\alpha_i} = \prod_{i=0}^{\eta} f_i^{\beta_i} k(x) + (x^n - a)^{\epsilon} h(x), \text{ in } F_q[x].
\]

Since \( 0 \leq \beta_i \leq ep^e \), \( \prod_{i=1}^{\eta} f_i^{\beta_i} \mid (x^n - a)^{\epsilon} \) and hence \( \prod_{i=1}^{\eta} f_i^{\beta_i} \mid \prod_{i=1}^{\eta} f_i^{\alpha_i} \) in \( F_q[x] \). Thus for any \( i \), \( 1 \leq i \leq \eta \), \( \beta_i \leq \alpha_i \). □

For the rest of this paper, all notations \( \psi, S, T_e \) and \( f_i \) \((1 \leq i \leq \eta)\) are fixed as defined above.

**Proposition 2.6.** Let \( C \) be an \((a + bu)\)-constacyclic code of length \( n = mp^e \) over \( R \). Then as an ideal of \( S \), \( C \) has a unique generator of the form \( \prod_{i=1}^{\eta} f_i^{\alpha_i} \), where \( 0 \leq \alpha_i \leq ep^e \) and \( f_i \) are distinct monic irreducible divisors of \( x^m - a_0 \) in \( F_q[x] \).

**Proof.** Since \( C \subseteq S \), \( \psi(C) \subseteq T_e \) (by Proposition 2.3). Hence by Lemma 2.5, \( \psi(C) \) has a unique generator of the form \( \prod_{i=0}^{\eta} f_i^{\alpha_i} \), where \( 0 \leq \alpha_i \leq ep^e \). Since \( \psi(f_i) = f_i \), we are done. □

**Remark 2.7.** (i) Showing the uniqueness of the generators of constacyclic codes is open to doubt, (see, for example [1], Theorems 4.3, 4.5 and Corollary 4.7). Dinh et. al. [3] and also Guenda et. al. [5] seem to have used the uniqueness of the generators of constacyclic codes, implicitly, to calculate their numbers, although they have not pointed to it.
(ii) The authors of [2] and [3] have calculated $|C|$, where $C$ is a constacyclic code, which seems not to be very accurate (for example, when the power of the distinct monic irreducible divisors of $x^n - a_0$ are greater than $p^s$, the equality does not hold). We shall find the exact number $|C|$, in the following corollary.

**Corollary 2.8.** (i) Let $C = \langle \prod_{i=1}^{\eta} f_i^{\alpha_i} \rangle$ and $D = \langle \prod_{i=1}^{\eta} f_i^{\beta_i} \rangle$ be ideals of $S$, where $0 \leq \alpha_i, \beta_i \leq ep^s$. If $C \subseteq D$, then for any $i$, $1 \leq i \leq \eta$, $\beta_i \leq \alpha_i$, that is, in $F_q[x]$, $\prod_{i=1}^{\eta} f_i^{\beta_i} \mid \prod_{i=0}^{\eta} f_i^{\alpha_i}$.

(ii) The number of $(a + bu)$–constacyclic codes of length $n = mp^s$ over $R$ is $(ep^s + 1)^{\eta}$.

(iii) If $C = \langle \prod_{i=1}^{\eta} f_i^{\alpha_i} \rangle$ is an $(a + bu)$–constacyclic code over $R$, then $|C| = q^{en - \sum_{i=1}^{\eta} \alpha_i \deg f_i}$.

**Proof.** (i) Suppose that $C \subseteq D$. Thus with the previous notations, $\psi(C) \subseteq \psi(D)$. Since $\psi(f_i) = f_i$, the result follows by Lemma 2.8.

(ii) By the uniqueness of generators of these codes, the proof is straightforward.

(iii) Since $|C| = |\psi(C)|$ and $\psi(C)$ is an ideal of $T_e$, $|C| = q^{en - \sum_{i=1}^{\eta} \alpha_i \deg f_i}$. □

**Lemma 2.9.** Let $C = \langle \prod_{i=1}^{\eta} f_i^{\alpha_i} \rangle$ be an ideal of $S$, $0 \leq \alpha_i \leq ep^s$. Then for a non-negative integer $l$, $<u^l > \subseteq C$ if and only if for any $i$, $1 \leq i \leq \eta$, $0 \leq \alpha_i \leq lp^s$.

**Proof.** $<u^l > \subseteq C$ if and only if $\psi(<u^l>) \subseteq \psi(C)$ if and only if $<x^n - a > \subseteq < \prod_{i=1}^{\eta} f_i^{\alpha_i} >$ if and only if $< \prod_{i=1}^{\eta} f_i^{lp^s} > \subseteq < \prod_{i=1}^{\eta} f_i^{\alpha_i} >$ if and only if $0 \leq \alpha_i \leq lp^s$ for any $i$, $1 \leq i \leq \eta$ (by Lemma 2.8). □

Let $C = \langle \prod_{i=1}^{\eta} f_i^{\alpha_i} \rangle$ be an $(a + bu)$–constacyclic code over $R$, where $0 \leq \alpha_i \leq ep^s$. Assume that there exists $k$, $0 \leq k \leq e - 1$ such that $kp^s \leq \alpha_i \leq (k + 1)p^s$, for $i$, $1 \leq i \leq \eta$. Let $\alpha_i = kp^s + \beta_i$, $0 \leq \beta_i < p^s$. Then

$$\prod_{i=1}^{\eta} f_i^{\alpha_i} = (\prod_{i=1}^{\eta} f_i^{lp^s})^k \prod_{i=1}^{\eta} f_i^{\beta_i} = (x^n - a)^k \prod_{i=1}^{\eta} f_i^{\beta_i} = b^k u^k \prod_{i=1}^{\eta} f_i^{\beta_i}.$$

Obviously, $g(x) = \prod_{i=1}^{\eta} f_i^{\beta_i}$ divides $x^n - a$ in $F_q[x]$ and $C = < u^k g(x) >$.

In order to give a characterization of the generators of an $(a + bu)$–constacyclic code, we construct the following polynomials $g_i(x) \in F_q[x]$. Suppose that $f(x) = \prod_{i=1}^{\eta} f_i^{\alpha_i}$, where $0 \leq \alpha_i \leq ep^s$, $1 \leq i \leq \eta$. Changing the indices so that for the non-negative integers $0 =
\( s_0 \leq s_1 \leq \ldots \leq s_e = \eta, \ 0 \leq \alpha_1, \alpha_2, \ldots, \alpha_{s_1} \leq p^s < \alpha_{s_1+1}, \ldots, \alpha_{s_2} \leq 2p^s < \ldots < (e-1)p^s < \alpha_{s_{e-1}+1}, \ldots, \alpha_{s_e} \leq ep^s \). Suppose that
\[
\alpha_{s_1+j_1} = p^s + \beta_{s_1+j_1}, \quad 0 < \beta_{s_1+j_1} \leq p^s
\]
\[
\alpha_{s_2+j_2} = 2p^s + \beta_{s_2+j_2}, \quad 0 < \beta_{s_2+j_2} \leq p^s
\]
\[\vdots\]
\[
\alpha_{s_{e-1}+j_{e-1}} = (e-1)p^s + \beta_{s_{e-1}+j_{e-1}}, \quad 0 < \beta_{s_{e-1}+j_{e-1}} \leq p^s.
\]
We have
\[
g_0(x) = \gcd(f(x), x^n - a) = (f^{\alpha_{s_0+1}}_{s_0+1} \ldots f^{\alpha_{s_1+1}}_{s_1+1})(\prod_{i=s_1+1}^{\eta} f_i^{p^s})
\]
\[
g_1(x) = \gcd\left(\frac{f(x)}{g_0(x)}, g_0(x)\right) = (f^{\beta_{s_1+1}}_{s_1+1} \ldots f^{\beta_{s_2+1}}_{s_2+1})(\prod_{i=s_2+1}^{\eta} f_i^{p^s})
\]
\[\vdots\]
\[
g_{e-2}(x) = \gcd\left(\frac{f(x)}{g_0(x)g_1(x) \ldots g_{e-3}(x)}, g_{e-3}(x)\right) = (f^{\beta_{s_{e-2}+1}}_{s_{e-2}+1} \ldots f^{\beta_{s_{e-1}+1}}_{s_{e-1}+1})(\prod_{i=s_{e-1}+1}^{\eta} f_i^{p^s})
\]
\[
g_{e-1}(x) = \gcd\left(\frac{f(x)}{g_0(x)g_1(x) \ldots g_{e-2}(x)}, g_{e-2}(x)\right) = (f^{\beta_{s_{e-1}+1}}_{s_{e-1}+1} \ldots f^{\beta_{s_{e}}}_{s_{e}}).
\]
(If \( s_j = s_{j+1} \), we have \( g_j(x) = \prod_{i=s_j+1}^{\eta} f_i^{p^s} \).) We can see that \( g_{e-1}(x) \mid \ldots \mid g_1(x) \mid g_0(x) \mid x^n - a \) in \( F_q[x] \) and \( \prod_{i=1}^{\eta} f_i^{\alpha_i} = \prod_{i=0}^{e-1} g_i(x) \). Therefore, we have the following form of the generators of an \((a + bu)\)-constacyclic code over \( R \).

**Proposition 2.10.** Let \( C \) be an \((a + bu)\)-constacyclic code over \( R \). Then \( C =< g_0g_1 \ldots g_{e-1}, \) where \( g_i \) are monic polynomials in \( F_q[x] \) such that \( g_{e-1}(x) \mid \ldots \mid g_1(x) \mid g_0(x) \mid x^n - a \). Also \( \mid C \mid = q^{e\eta - \sum_{i=0}^{e-1} \alpha_i} \) where \( \deg g_i = t_i \).

**Note.** From now on, for an \((a + bu)\)-constacyclic code \( C \), the related polynomials \( g_0(x), g_1(x), \ldots, g_{e-1}(x) \) with \( \deg g_i = t_i, 0 \leq i \leq e - 1 \), are fixed.

**Lemma 2.11.** Let \( C =< g_0g_1 \ldots g_{e-1} > \) be an \((a + bu)\)-constacyclic code over \( R \) and \( l \) be a non-negative integer less than \( e \). Then \( < u' > \subseteq C \) if and only if \( g_l = g_{l+1} = \cdots = g_{e-1} = 1 \).

**Proof.** By Lemma 2.10, \( < u' > \subseteq C \) if and only if \( C =< \prod_{i=1}^{\eta} f_i^{\alpha_i}, \) where \( 0 \leq \alpha_i \leq lp^s \). The rest of the proof is similar to the discussion preceding Proposition 2.11. \( \square \)

**Lemma 2.12.** Let \( C =< g_0g_1 \ldots g_{e-1} > \) be an \((a + bu)\)-constacyclic code over \( R \). If \( f(x) \in F_q[x] \) is a polynomial of the lowest degree such that \( u^{e-1} f(x) \in C \), then \( f(x) = g_{e-1} \).
Proof. First note that \( g_0g_1 \ldots g_{e-1} \mid g_{e-1}(x^n - a)^{e-1} \). Thus \( u^{e-1}g_{e-1} \in C \). By the division algorithm in \( F_q[x] \),

\[ g_{e-1}(x) = f(x)g(x) + s(x), \text{ where } \text{deg } s < \text{deg } f. \]

Since \( u^{e-1}g_{e-1}(x) \) and \( u^{e-1}f(x) \) are in \( C \), \( u^{e-1}s(x) \in C \). Hence \( s(x) = 0 \). Thus \( g_{e-1}(x) = f(x)g(x) \). Since \( u^{e-1}f(x) \in C \), \( (x^n - a)^{e-1}f(x) \in \psi(C) \), where \( \psi \) is the isomorphism in Proposition 2.13. So there exists \( h(x) \in T_e \), where \( \text{deg } h < en - \sum_{i=0}^{e-1} t_i \), such that \( (x^n - a)^{e-1}f(x) = g_0g_1 \ldots g_{e-1}h(x) \). Since the degree of two sides of the above equality is lower than \( en \), we can consider this equality in \( F_q[x] \). Hence \( (x^n - a)^{e-1} = g_0g_1 \ldots g_{e-2}g(x)h(x) \). Let \( D = \langle g_0g_1 \ldots g_{e-2}g \rangle \leq \mathcal{S} \). Then \( u^{e-1} = (x^n - a)^{e-1} \in D \) and \( g(x) \mid g_{e-2}(x) \mid \ldots \mid g_1(x) \mid g_0(x) \mid x^n - a \). By Lemma 2.11 for \( D \), \( g(x) = 1 \). Hence \( f(x) = g_{e-1} \).

**Proposition 2.13.** Let \( C = \langle g_0g_1 \ldots g_{e-1} \rangle \) be an \((a + bu)-\text{constacyclic code over } R\). Then \( u^{e-1}g_{e-1} \) has the lowest degree between all non-zero elements of \( C \).

Proof. Assume that \( d(x) \in C \) has the lowest degree between all non-zero elements of \( C \). Let \( d(x) = \sum_{i=0}^{e-1} d_i(x)u^i \), where \( d_i(x) \in F_q[x] \) and \( \text{deg } d_i < n \), \( 0 \leq i \leq e - 1 \). There exists the smallest non-negative integer \( j \), \( 0 \leq j \leq e - 1 \), such that \( \text{deg } d_j = \text{deg } d \). For any \( l \), \( 0 \leq l \leq j - 1 \), \( \text{deg } d_l < \text{deg } d \). Now, \( u^{e-1}d_0(x) = u^{e-1}d(x) \in C \). Since \( d(x) \) has the lowest degree in \( C \) and \( \text{deg } d_0 = \text{deg } u^{e-1}d_0 < \text{deg } d \), \( u^{e-1}d_0(x) = 0 \) and so \( d_0(x) = 0 \). Also \( u^{e-1}d_1(x) = u^{e-2}d(x) \in C \). Since \( d(x) \) has the lowest degree in \( C \) and \( \text{deg } d_1 = \text{deg } u^{e-1}d_1 < \text{deg } d \), \( d_1(x) = 0 \). Similarly, \( d_2(x) = \ldots = d_{j-1}(x) = 0 \). Now \( u^{e-1}d_j(x) = u^{e-1}d(x) \in C \). Since \( \text{deg } u^{e-1}d_j = \text{deg } d_j = \text{deg } u^{e-1}d_j(x) \) has the lowest degree in \( C \). So by Lemma 2.12, \( d_j(x) = g_{e-1}(x) \). Hence \( \text{deg } d = \text{deg } d_j = \text{deg } g_{e-1} = \text{deg } u^{e-1}g_{e-1} \). Therefore, \( u^{e-1}g_{e-1} \) has the lowest degree between all non-zero elements of \( C \).

### 3. The minimal spanning set of constacyclic codes

In this section we shall determine the minimal spanning set for an \((a + bu)-\text{constacyclic code over } R\). Let us define the following notations. If \( h_j(x) \), \( -1 \leq j \leq r \), are polynomials in \( F_q[x] \) such that \( \text{deg } h_j = t_j \) and

\[ h_r(x) \mid \ldots \mid h_0(x) \mid h_{-1}(x), \]

then we assign the underlying set \( \{ f(x), xf(x), \ldots, x^{t_{-1}-t_0-1}f(x) \mid f = \prod_{i=0}^{r} h_i \} \) for the property (\( \square \)). If \( t_{-1} = t_0 \), then the empty set \( \emptyset \) will be assigned to be the underlying set.

First we provide the minimal spanning set for two special cases.

In the following proposition, we determine the minimal spanning set for all constacyclic codes over \( R = F_q + uF_q \), where \( u^2 = 0 \). To do so, we need the following lemma whose proof is straightforward.
Lemma 3.1. Let $R = F_q + uF_q$, where $u^2 = 0$ and $g(x)$ be a divisor of $x^n - a$ in $F_q[x]$. If $g(x)k(x) = 0$ for some $k(x) \in S$, then there exists $h(x) \in F_q[x]$ such that $\deg h \leq n - 1$ and $k(x) = uh(x)$.

Proposition 3.2. Let $C = \langle g_0g_1 \rangle$ be an $(a+bu)$-constacyclic code over $R = F_q + uF_q$, where $u^2 = 0$ and $\deg g_i = t_i$, $i = 0, 1$. Suppose that $A_0$ is the underlying set for $g_1(x) \mid g_0(x) \mid x^n - a$ and $A_1$ is the underlying set for $g_1(x) \mid g_0(x)$. Then

$$\Delta = A_0 \cup uA_1 = \{g_0g_1, xg_0g_1, \ldots, x^{n-t_0-1}g_0g_1\} \cup \{ug_1, xug_1, \ldots, x^{t_0-t_1-1}ug_1\}$$

is a minimal spanning set for $C$ as an $R$-module.

Proof. First, we show that $\tilde{\Delta} = A_0 \cup uA_0 \cup uA_1$ is a linearly independent set over $F_q$. Suppose that

$$\sum_{i=0}^{n-t_0-1} (k_i + uk'_i)x^i g_0g_1 + \sum_{j=0}^{t_0-t_1-1} d_jx^j ug_1 = 0,$$

where $k_i$, $k'_i$ and $d_j$ are in $F_q$, $0 \leq i \leq n - t_0 - 1$, $0 \leq j \leq t_0 - t_1 - 1$. Let $k(x) = \sum_{i=0}^{n-t_0-1} k_ix^i$, $k'(x) = \sum_{i=0}^{n-t_0-1} k'_ix^i$ and $d(x) = \sum_{j=0}^{t_0-t_1-1} d_jx^j$. We show that $k(x)$, $k'(x)$ and $d(x)$ are zero. In $S$, $g_1(x)|k(x)g_0(x) + uk'(x)g_0(x) + ud(x)| = 0$. Hence by Lemma 3.1, $k(x)g_0(x) + uk'(x)g_0(x) + ud(x) = uh(x)$, where $h(x) \in F_q[x]$ and $\deg h < n$. Since in the above equation the degree of all polynomials are lower than $n$, we can consider that equation in $R[x]$. So $k'(x)g_0(x) + d(x) = h(x)$ and $k(x)g_0(x) = 0$ (in $F_q[x]$). Since $g_0(x) \neq 0$, $k(x) = 0$. Therefore, by (4),

$$uk'(x)g_0(x)g_1(x) + ud(x)g_1(x) = 0,$$

in $S$. Now, in $F_q[x]$, $k'(x)g_0(x)g_1(x) = (x^n - a)s(x) + q(x)$, where $\deg q \leq n - 1$ and $\deg s \leq t_1 - 1$. Also $g_0(x) | q(x)$. Assume that $q(x) = g_0(x)q'(x)$, $\deg q' \leq n - t_0 - 1$. Hence in $S$, $k'(x)g_0(x)g_1(x) = bus(x) + g_0(x)q'(x)$. Now using (3), $ug_0(x)q'(x) + ud(x)g_1(x) = 0$. So $g_0(x)q'(x) + d(x)g_1(x) = 0$ (by Lemma 2.1). Hence $g_0(x) | d(x)g_1(x)$. Since $\deg dg_1 < \deg g_0$, $d(x) = 0$. So $q'(x) = 0$. Therefore, $k'(x)g_0(x)g_1(x) = bus(x)$. Hence $us(x) \in C$. Since by Proposition 2.1, $ug_1(x)$ has the lowest degree in $C$, $s(x) = 0$. Thus $k'(x)g_0(x)g_1(x) = 0$ in $F_q[x]$. Hence $k'(x) = 0$. Now, $|\Delta| = 2n - t_0 - t_1$ is equal to the dimension of $C$ as a vector space over $F_q$ (by Corollary 2.3, part (iii)). So $\tilde{\Delta}$ is an spanning set for $C$ as an $F_q$-module. Hence $\Delta$ generate $C$ as an $R$-module. Also since $\tilde{\Delta}$ is linearly independent, $\Delta$ is a minimal spanning set for $C$. \qed

In the following lemma, we determine the minimal spanning set for the constacyclic code $C = \langle u^kg(x) \rangle$ over $R = F_q + uF_q + \cdots + u^{e-1}F_q$, where $u^e = 0$ and $g(x) \in F_q[x]$ is a divisor
of $x^n - a$ (see the discussion after Lemma 3.3). This lemma is used in the proof of Proposition 3.3.

**Lemma 3.3.** Let $C = \langle u^k g(x) \rangle$ be an $(a + bu)$-constacyclic code over $R$, where $g(x) \mid x^n - a$, $0 \leq k \leq e - 1$ and $\deg g = t$. Suppose that $B_0$ is the underlying set for $1 \mid g(x) \mid x^n - a$ and $B_1$ is the underlying set for $1 \mid g(x)$, if $0 \leq k \leq e - 2$ and $\emptyset$, if $k = e - 1$. Then $\Omega = u^k B_0 \cup u^{k+1} B_1$ is a minimal spanning set for $C$ as an $R$-module. Also, $|C| = q^{(e-k)n-t}$.

**Proof.** First, we show that $\Omega$ is a spanning set. Let $c(x) \in C$. Thus $c(x) = u^k g(x) l(x)$ for some $l(x) \in \mathcal{S}$. If $\deg l \leq n - t - 1$, then we are done. Suppose that $\deg l \geq n - t$. In $R[x]$, $l(x) = (\frac{x^n - a}{g(x)}) q(x) + s(x)$, where $\deg s \leq n - t - 1$ and $\deg q \leq t - 1$.

Now in $\mathcal{S}$,

$$
c(x) = u^k g(x) ((\frac{x^n - a}{g(x)}) q(x) + s(x))
= u^k q(x) (x^n - a) + u^k g(x) s(x)
= bu^{k+1} q(x) + u^k g(x) s(x).
$$

(Note that if $k = e - 1$, then $bu^{k+1} q(x) = 0$.) Hence

$$
\Omega = \{ u^k g, xu^k g, \ldots, x^{n-t-1} u^k g, u^{k+1}, xu^{k+1}, \ldots, x^{t-1} u^{k+1} \}
$$
is a spanning set for $C$ if $0 \leq k \leq e - 2$. Also if $k = e - 1$, then

$$
\Omega = \{ u^{e-1} g, xu^{e-1} g, \ldots, x^{n-t-1} u^{e-1} g \}
$$
is a spanning set for $C$. We claim that $\Omega$ is a minimal spanning set. For, it is enough to show that

$$
\sum_{i=0}^{n-t-1} (\sum_{j=0}^{e-k-1} l_{ji} u^i) x^i g + \sum_{i'=0}^{t-1} (\sum_{j'=0}^{e-k-2} d_{ij'} u^{i'}) x^{i'} u^{k+1} = 0,
$$
implies that all coefficients $l_{ji}$ and $d_{ij'}$ are zero in $F_q[x]$. Consider polynomials $l_j(x) = \sum_{i=0}^{n-t-1} l_{ji} x^i$ and $d_j'(x) = \sum_{i'=0}^{t-1} d_{ij'} x^{i'}$, where $0 \leq j \leq e - k - 1$ and $0 \leq j' \leq e - k - 2$. Thus in $\mathcal{S}$,

$$
(\sum_{j=0}^{e-k-1} u^i l_j(x)) u^k g(x) + (\sum_{j'=0}^{e-k-2} u^{i'} d_j'(x)) u^{k+1} = 0.
$$

Since the degree of all polynomials in the above equality is lower than $n$, by applying Lemma 3.3.1, we have,

$$
l_0(x) g(x) = 0 \text{ and } l_j(x) g(x) + d_j(x) = 0, \text{ in } F_q[x], 1 \leq j \leq e - k - 1.
$$

Since $g(x) \neq 0$, $l_0(x) = 0$. Also $\deg (l_j g) > \deg d_j$ implies that $l_j(x) = d_j(x) = 0$.

To prove the last statement of the lemma, note that $\psi(C) = \langle (x^n - a)^k g(x) \rangle$ and $|\psi(C)| = q^{(e-k)n-t}$. Hence $|C| = q^{(e-k)n-t}$. □

For every positive integer $j$, set $T_j = \frac{F_q[x]}{<x^n - a>^j}$. If $i \leq j$, then clearly $T_i$ is a homomorphic image of $T_j$. Consider the natural ring epimorphism $\pi_{ji} : T_j \rightarrow T_i$ with $\ker \pi_{ji} = \frac{<x^n - a>^j}{<x^n - a>^i}$.

Note that for polynomials $h_1(x)$ and $h_2(x)$ in $F_q[x]$, if $h_1(x) \equiv h_2(x)$ (mod $(x^n - a)^j$), then
\[ \pi_{ji}(h_1(x)) \equiv \pi_{ji}(h_2(x)) \pmod{(x^n - a)^t}. \]

Obviously, every \( h(x) \in T_j \) has a unique representation \( h(x) = \sum_{l=0}^{z-1} h_l(x)(x^n - a)^l \), where \( h_l(x) \in F_q[x] \) and \( \deg h_l < n \) for any \( l, 0 \leq l \leq j - 1 \). Thus we have

\[
\pi_{ji}(h(x)) = \pi_{ji}(\sum_{l=0}^{z-1} h_l(x)(x^n - a)^l) = \sum_{l=0}^{z-1} h_l(x)(x^n - a)^l.
\]

For \( j \geq 2 \), consider the finite chain ring \( R_j = F_q + u_jF_q + \cdots + u_j^{z-1}F_q \), where \( u_j^z = 0 \) and the principal ideal rings \( S_j = \frac{R_j[x]}{<x^n - (a + bu_j)>} \). In the following proposition, we show that if \( i \leq j \), then \( S_j \) is a homomorphic image of \( S_i \).

**Proposition 3.4.** Let \( i \) and \( j \) be two integers such that \( 1 < i \leq j \). Then there exists an epimorphism \( \beta_{ji} : S_j \to S_i \) such that \( \beta_{ji}(\sum_{l=0}^{j-1} h_l(x)u_j^l) = \sum_{l=0}^{i-1} h_l(x)u_i^l \), where \( h_l(x) \in F_q[x] \) and \( \deg h_l < n \) for any \( l, 0 \leq l \leq j - 1 \). Also \( \ker \beta_{ji} \) is the ideal of \( S_j \) generated by \( u_j^i \).

**Proof.** Similar to the proof of Proposition 3.3, consider \( \psi_j : S_j \to T_j \) by

\[
\psi_j(\sum_{l=0}^{j-1} u_j^l k_l(x)) = \sum_{l=0}^{j-1} b^{-l}(x^n - a)^l k_l(x),
\]

where \( k_l(x) \in F_q[x] \), for any \( l, 0 \leq l \leq j - 1 \) and \( \deg k_l < n \). Now we set \( \beta_{ji} = \psi_i^{-1} \pi_{ji} \psi_j \) in

\[
S_j \xrightarrow{\psi_j} T_j \xrightarrow{\pi_{ji}} T_i \xrightarrow{\psi_i^{-1}} S_i.
\]

We can see that \( \beta_{ji} \) is an epimorphism and \( \ker \beta_{ji} = \psi_j^{-1}(\ker \pi_{ji}) \). Hence \( \ker \beta_{ji} =< u_j^i > \).

Furthermore, \( \beta_{ji}(u_j^l) = u_i^l \). Since \( \pi_{ji}((x^n - a)^l) = 0 \) for all \( l, l \geq i \),

\[
\beta_{ji}(u_j^l) = \begin{cases} 
0 & \text{if } l \geq i \\
u_i^l & \text{if } l < i
\end{cases}.
\]

Every element of \( S_j \) has a unique representation \( \sum_{l=0}^{j-1} u_j^l h_l(x) \), where \( h_l(x) \in F_q[x] \), for any \( l, 0 \leq l \leq j - 1 \) and \( \deg h_l < n \). Thus \( \beta_{ji}(\sum_{l=0}^{j-1} h_l(x)u_j^l) = \sum_{l=0}^{i-1} h_l(x)u_i^l \).

**Corollary 3.5.** If \( 1 < i \leq j \), then \( \frac{S_j}{<u_j^i>} \simeq S_i \).

**Lemma 3.6.** Suppose that \( 1 < i \leq j \) and \( h(x) \) is a polynomial in \( F_q[x] \) such that \( \deg h < ni \). Then \( \beta_{ji}(h(x)) = h(x) \).

**Proof.** Since \( \deg h < ni \), there exist polynomials \( h_l(x) \in F_q[x], 0 \leq l \leq i - 1 \), of degree less than \( n \) such that \( h(x) = \sum_{l=0}^{i-1}(x^n - a)^l h_l(x) \). In \( S_j \), \( h(x) = \sum_{l=0}^{i-1} b^l u_j^l h_l(x) \) and hence \( \beta_{ji}(h(x)) = h(x) \).

**Lemma 3.7.** Let \( C = \langle \prod_{l=1}^{q} f_l^{\alpha_l} \rangle \) be an \((a + bu)\)-constacyclic code over \( R_j \), where \( 0 \leq \alpha_l \leq jp^n \). If \( i \leq j \) and \( <u_j^i> \subseteq C \), then \( \beta_{ji}(C) \) as an ideal of \( S_i \) generated by \( \prod_{l=1}^{q} f_l^{\alpha_l} \).
Proof. Since \( u^j \subseteq C \), by Lemma 4.3, \( 0 \leq \alpha_l \leq ip^l \) for any \( l, 1 \leq l \leq \eta \). Hence \( \deg (\prod_{i=1}^{\eta} f_i^{\alpha_i}) < ni \). So \( \beta_{ji}(\prod_{i=1}^{\eta} f_i^{\alpha_i}) = \prod_{i=1}^{\eta} f_i^{\alpha_i} \), by Lemma 4.4. Since \( C \) contains \( \ker \beta_{ji} \), we can see that \( \beta_{ji}(C) \) is an ideal of \( S_i \) generated by \( \beta_{ji}(\prod_{i=1}^{\eta} f_i^{\alpha_i}) \). \( \square \)

With the previous notations, let \( R_3 = F_q + uF_q + u^2F_q \) and \( R_2 = F_q + vF_q \), where \( u^3 = 0 \) and \( v^2 = 0 \). Consider \( S_3 = \frac{R_3[x]}{<x^n-(a+bu)>} \) and \( S_2 = \frac{R_2[x]}{<x^n-(a+bu)>} \).

**Proposition 3.8.** Let \( g_1(x) \mid g_0(x) \mid x^n - a \) and \( \deg g_i = t_i, \ i = 0, 1, \) and let \( k_0(x), k_1(x) \in F_q[x], \deg k_0 \leq n - t_0 - 1 \) and \( \deg k_1 \leq t_0 - t_1 - 1 \). If in \( S_3 \),

\[
2k_0(x)g_0g_1 + u^2k_1(x)g_1 = 0,
\]

then \( k_0(x) = k_1(x) = 0 \) in \( F_q[x] \).

**Proof.** If \( g_0(x) = x^n - a \), then the result holds by Lemma 4.1. Let \( g_0(x) \neq x^n - a \) and \( C = < g_0g_1 > \) be the \((a + bu)\)-constacyclic code over \( R_3 \). Consider

\[
\begin{align*}
A_0 &= \{g_0g_1, xg_0g_1, \ldots, x^{n-t_0-1}g_0g_1\}, \\
A_1 &= \{g_1, xg_1, \ldots, x^{t_0-t_1-1}g_1\}, \\
A_2 &= \{1, x, \ldots, x^{t_1-1}\}.
\end{align*}
\]

We show that \( \Delta = A_0 \cup uA_1 \cup u^2A_2 \) is a spanning set for \( C \) as an \( R_3 \)-module. Clearly, every element of \( \Delta \) is in \( C \). Suppose that \( \beta = \beta_{32} : S_3 \rightarrow S_2 \) is the epimorphism in Proposition 6.3. Since \( \deg (g_0g_1) < 2n \), by Lemma 4.1, \( \beta(C) \) is the ideal of \( S_2 \) generated by \( g_0g_1 \). By Proposition 6.3, the set

\[
\{g_0g_1, xg_0g_1, \ldots, x^{n-t_0-1}g_0g_1\} \cup \{vg_1, xv_1g_1, \ldots, x^{t_0-t_1-1}vg_1\}
\]

is a minimal spanning set for \( \beta(C) \). Also by Lemma 6.3, the set \( \{u^2, xu^2, \ldots, x^{n-1}u^2\} \) is a minimal spanning set for \( \ker \beta = < u^2 > \). Assume that \( c(x) \in C \). Hence

\[
c(x) = \sum_{i=0}^{n-t_0-1} r_i x^i g_0g_1 + \sum_{j=0}^{t_0-t_1-1} s_j x^j g_1 + \sum_{l=0}^{n-1} d_l x^l u^2,
\]

where \( r_i, s_j \in R_3, 0 \leq i \leq n - t_0 - 1, 0 \leq j \leq t_0 - t_1 - 1 \) and \( d_l \in F_q, 0 \leq l \leq n - 1 \). Now, we shall show that \( u^2x^r, t_1 \leq r \leq n - 1 \), are in the \( R_3 \)-module spanned by \( \Delta \). We have

\[
u^2x^{t_1} = u^2[g_1(x) + l(x)] = u^2g_1(x) + u^2l(x), \text{ where } l(x) \in F_q[x] \text{ and } \deg l < t_1.
\]

Thus \( u^2x^{t_1} \) is in the \( R_3 \)-module spanned by \( \Delta \). Since \( u^xg_1(x) \in \Delta \) for any \( i, 0 \leq i \leq t_0-t_1-1 \), inductively, for \( i, 0 \leq i \leq t_0-t_1-1, \ u^2x^{t_1+i} = u^2x^i g_1(x) + u^2x^i l(x) \) is generated by elements of \( \Delta \).

Now, by the division algorithm, there exist \( k(x) \in F_q[x] \) with \( \deg k < t_0 \) and \( b_0, b_1, \ldots, b_j \) in \( F_q \) such that

\[
u^2x^{t_0+j} = u^2[b_jx^j g_0(x) + b_{j-1}x^{j-1}g_0(x) + \cdots + b_0g_0(x) + k(x)],
\]

where \( 0 \leq j \leq n-t_0-1 \). We saw that \( u^2k(x) \) is in the \( R_3 \)-module generated by \( \Delta \). It is enough
to prove that $u^2x^ig_0(x)$, $0 \leq i \leq j$, is generated by the elements of $\Delta$. Clearly, $ux^ig_0(x) \in C$. Thus $\beta(ux^ig_0(x)) = vx^ig_0(x) \in \beta(C)$. Hence there exist $r'_i, s'_j \in R_3$, $0 \leq i \leq n - t_0 - 1$ and $0 \leq j \leq t_0 - t_1 - 1$ such that

$$ux^ig_0(x) - (\sum_{i=0}^{n-t_0-1} r'_ix^ig_0g_1 + \sum_{j=0}^{t_0-t_1-1} s'_jx^juq_1) \in \ker \beta = <u^2>.$$ 

Hence $u^2x^ig_0(x) = \sum_{i=0}^{n-t_0-1} ur'_ix^ig_0g_1 + \sum_{j=0}^{t_0-t_1-1} s'_jx^ju^2g_1$. Therefore, $\Delta$ is a spanning set for $C$. Consider $\overline{\Delta} = \bigcup_{i=0}^2 \bigcup_{j=1}^2 u^jA_i$. Since $\Delta$ is a spanning set for $C$ as an $R_3$-module, $\overline{\Delta}$ is a spanning set for $C$ as an $F_q$-module. Now $|\overline{\Delta}| = q^{3n-t_0-t_1}$ is equal to the dimension of $C$ as a vector space, by Proposition 3.10. So $\overline{\Delta}$ is a linearly independent set over $F_q$. Therefore, the result holds. □

**Notation.** Suppose that $g_i(x)$, $i = 0, 1, 2$, are monic polynomials in $F_q[x]$ such that $g_2(x) \mid g_1(x) \mid g_0(x) \mid x^n - a$ and $\deg g_i = t_i$. We set

- $A_0$, the underlying set for "$g_2(x) \mid g_1(x) \mid g_0(x) \mid x^n - a$",
- $A_1$, the underlying set for "$g_2(x) \mid g_1(x) \mid g_0(x)$" and $g_1(x)"$
- $A_2$, the underlying set for "$g_2(x) \mid g_1(x)$".

**Proposition 3.9.** Let $C = <g_0g_1g_2 >$ be an $(a + bu)$-constacyclic code over $R_3$. Then $\Gamma = \bigcup_{i=0}^2 \bigcup_{j=1}^2 u^jA_j$ is a minimal spanning set for $C$.

**Proof.** Suppose that $\deg g_i = t_i$, $0 \leq i \leq 2$. We shall show that $\overline{\Gamma} = \bigcup_{i=0}^2 \bigcup_{j=1}^2 u^jA_j$ is a linearly independent subset of $S_3$ over $F_q$. Assume that in $S_3$,

$$\sum_{i=0}^2 \sum_{j=1}^2 \sum_{k=0}^{t_i-1} \sum_{l=0}^{t_i-1} z_{ijkl}u^jx^i = 0,$$

where $t_i = n$ and $z_{ijkl} \in F_q$.

In $F_q[x]$, set $k_{ij} = \sum_{k=0}^{t_i-1} \sum_{l=0}^{t_i-1} z_{ijkl}x^i$. Hence in $S_3$,

$$k_0(x) + uk_0(x) + u^2k_0(x)g_0g_1g_2 + (k_{11}(x) + uk_{12}(x))ug_1g_2 + k_{22}(x)u^2g_2 = 0.$$ 

Thus there exist $h_0(x), h_1(x)$ and $h_2(x)$ in $F_q[x]$ such that

$$k_0(x)g_0g_1g_2 = (x^n - a)h_0(x),$$

$$k_0(x)g_0g_1g_2 + k_{11}(x)g_1g_2 = (x^n - a)h_1(x) - bh_0(x),$$

$$k_0(x)g_0g_1g_2 + k_{12}(x)g_1g_2 + k_{22}(x)g_2 = (x^n - a)h_2(x) - bh_1(x).$$

By the third equality, $g_2(x) \mid h_1(x)$ and by the second equality, $g_1(x)g_2(x) \mid h_0(x)$. Hence $(x^n - a) \mid k_0(x)g_0(x)$. Since $\deg k_0g_0 < n$, $k_0(x) = h_0(x) = 0$. So $k_{11}(x)g_0g_1g_2 + k_{11}(x)g_1g_2 = (x^n - a)h_1(x)$. Therefore, $k_{01}(x)g_0g_1 + k_{11}(x)g_1g_2 = (x^n - a)\frac{h_1(x)}{g_2}$. Now, in $S_3$, $u^2k_0(x)g_0g_1 + u^2k_{11}(x)g_1g_2 = 0$. By Proposition 3.8, $k_{01}(x) = k_{11}(x) = 0$. Hence $h_1(x) = 0$. So in the third equality, $g_1(x) \mid k_{22}(x)g_2(x)$. Since $\deg k_{22}g_2 < \deg g_1$, $k_{22}(x) = 0$. Hence $k_0(x)g_0g_1g_2 + k_{12}(x)g_1g_2 = (x^n - a)h_2(x)$. By the division algorithm in $F_q[x]$,

$$h_2(x) = g_2(x)q(x) + s(x),$$

where $\deg s < \deg g_2$. 


So in $S_3$, $uk_0(x)g_0g_1g_2 + uk_1(x)g_1g_2 = u^2g_2(x)q(x) + u^2s(x)$. Thus $u^2s(x) \in C$. Since $\deg s < \deg g_2$, by Proposition 2.14, $s(x) = 0$. Hence $k_0(x)g_0g_1g_2 + k_1(x)g_1g_2 = (x^n - a)g_2(x)q(x)$.

So $k_0(x)g_0g_1 + k_1(x)g_1 = (x^n - a)q(x)$. Now, in $S_3$, $u^2k_0(x)g_0g_1 + u^2k_1(x)g_1 = 0$. By Proposition 3.8, $k_0(x) = k_1(x) = 0$. Therefore, $\hat{\Gamma}$ is linearly independent over $F_q$. So $\Gamma$ is a minimal set over $R_3$. Since the number of elements of $\hat{\Gamma}$ is equal to the dimension of $C$, $\hat{\Gamma}$ is a basis for $C$ over $F_q$. Thus $\Gamma$ is a minimal spanning set for $C$ over $R_3$. 

Now, we shall determine the minimal spanning set for an $(a + bu)$–constacyclic code over $R = F_q + uF_q + \cdots + u^{e-1}F_q$, where $u^e = 0$.

Let $g_j$, $0 \leq i \leq e - 1$, be monic polynomials in $F_q[x]$ such that $g_{e-1} | \cdots | g_1 | g_0 | x^n - a$. According to (III), suppose that $A_0$ is the underlying set for "$g_{e-1} | \cdots | g_1 | g_0 | x^n - a"$ and each $A_j$, $1 \leq j \leq e - 1$ is the underlying set for "$g_{e-1} | \cdots | g_j | g_{j-1}"$. Then we prove the following result.

**Proposition 3.10.** Let $C = \langle g_0g_1 \ldots g_{e-1} \rangle$ be an $(a + bu)$–constacyclic code over $R$. Then $\Gamma = \bigcup_{j=0}^{e-1} u^j A_j$ is a minimal spanning set for $C$ as an $R$–module. Also, $|C| = q^{en - \sum_{j=0}^{e-1} t_j}$, where $\deg g_j = t_j$, $0 \leq j \leq e - 1$.

**Proof.** For $e = 2$, we have Proposition 2.14. Inductively, similar to the proof of Proposition 3.8, for polynomials $k_j(x)$, $0 \leq j \leq i - 2$ and $3 \leq i \leq e$, we can prove that in $S_i$, $k_0(x)g_0g_1 \ldots g_{i-2} + k_1(x)g_1g_1 \ldots g_{i-2} + \cdots + k_{i-2}(x)g_{i-2} = 0$ implies that $k_0(x) = k_1(x) = k_{i-2}(x) = 0$ in $F_q[x]$, and similar to the proof of Proposition 3.13, we are done. 

4. The minimum Hamming distance of constacyclic codes

In this section, we shall determine the minimum distance of an $(a + bu)$–constacyclic code over $R$. We correspond to any constacyclic code $C$ over $R$, an ideal $\text{Tor}(C)$ of $T_1$ with the same minimum Hamming distance of $C$.

**Lemma 4.1.** Let $h_1(x)$ and $h_2(x)$ be two elements of $F_q[x]$. Suppose that for some $i$, $0 \leq i \leq e - 1$, $u^i h_1(x) \equiv u^i h_2(x)$ (mod $(x^n - (a + bu)))$, in $R[x]$. Then $h_1(x) \equiv h_2(x)$ (mod $(x^n - a)$) in $F_q[x]$.

**Proof.** In $R[x]$,

$$u^i(h_1(x) - h_2(x)) = (x^n - (a + bu))(k_0(x) + uk_1(x) + \cdots + u^{e-1}k_{e-1}(x)),$$
where \( k_j(x) \in F_q[x] \) (\( 0 \leq j \leq e - 1 \)). Hence in \( F_q[x] \),

\[
0 = (x^n - a)k_0(x) \\
0 = (x^n - a)k_1(x) - bk_0(x) \\
\vdots \\
0 = (x^n - a)k_{i-1}(x) - bk_{i-2}(x) \\
h_1(x) - h_2(x) = (x^n - a)k_i(x) - bk_{i-1}(x).
\]

By the first \( i \) relations, we deduce that \( k_0(x) = k_1(x) = \ldots = k_{i-1}(x) = 0 \). So \( h_1(x) - h_2(x) = (x^n - a)k_i(x) \) for \( i, 0 \leq i \leq e - 1 \). Hence \( h_1(x) \equiv h_2(x) \pmod{(x^n - a)} \) in \( F_q[x] \). \( \square \)

**Lemma 4.2.** Let \( h_1(x) \) and \( h_2(x) \) be two elements of \( F_q[x] \). Then \( h_1(x) \equiv h_2(x) \pmod{(x^n - a)} \) in \( F_q[x] \) if and only if \( u^{e-1}h_1(x) \equiv u^{e-1}h_2(x) \pmod{(x^n - (a + bu))} \) in \( R[x] \).

**Proof.** \( \Rightarrow \) Assume that \( h_1(x) \equiv h_2(x) \pmod{(x^n - a)} \) in \( F_q[x] \). Hence there exists \( k(x) \in F_q[x] \) such that \( h_1(x) - h_2(x) = (x^n - a)k(x) \). So in \( R[x] \), \( u^{e-1}h_1(x) - u^{e-1}h_2(x) = u^{e-1}(x^n - a)k(x) \).

Since \( x^n - a \equiv bu \pmod{(x^n - (a + bu))} \), \( u^{e-1}h_1(x) \equiv u^{e-1}h_2(x) \pmod{(x^n - (a + bu))} \).

\( \Leftarrow \) The proof follows by Lemma 4.2. \( \square \)

Suppose that \( C \) is an \((a + bu)\)-constacyclic code over \( R \). Regarding Lemma 4.2, let \( Tor(C) \) be the set of all polynomials \( h(x) \) in \( T_1 \) such that \( u^{e-1}h(x) \in C \). Clearly \( Tor(C) \) is an ideal of \( T_1 \). Hence \( Tor(C) \) is generated by a unique monic divisor \( k(x) \) of \( x^n - a \) in \( F_q[x] \). In fact, \( Tor(C) \) is an \( a \)-constacyclic code over \( F_q \). If we consider \( C \) as an \( R \)-submodule of \( R^n \), we can write

\[
Tor(C) = \{ h = (h_0, h_1, \ldots, h_{n-1}) \in F_q^n \mid u^{e-1}h \in C \}.
\]

Recall that the Hamming weight of \( \mathbf{v} \in R^n \), is defined to be the number of non-zero components of \( \mathbf{v} \). We denote by \( d_H(C) \), the minimum Hamming distance of a code \( C \). We shall show that \( d_H(C) = d_H(Tor(C)) \).

**Lemma 4.3.** Let \( C \) be an \((a + bu)\)-constacyclic code over \( R \). Then \( d_H(C) = d_H(Tor(C)) \).

**Proof.** Since \( u^{e-1}Tor(C) \subseteq C \), \( d_H(C) \leq d_H(u^{e-1}Tor(C)) \). Clearly \( d_H(Tor(C)) = d_H(u^{e-1}Tor(C)) \). Therefore \( d_H(C) \leq d_H(Tor(C)) \). Assume that

\[
\mathbf{v} = (\sum_{i=0}^{e-1} v_0u^i, \sum_{i=0}^{e-1} v_1u^i, \ldots, \sum_{i=0}^{e-1} v_{n-1}u^i).
\]
is a non-zero element of \( C \), \( v_{ji} \in F_q \), \( 0 \leq j \leq n - 1 \) and \( 0 \leq i \leq e - 1 \). Obviously, we can write \( v = \sum_{i=0}^{e-1}(v_{0i}, v_{1i}, \ldots, v_{n-1,i})u^i \). Suppose that \( l \) is the lowest integer such that \( w_l = (v_{0i}, v_{1i}, \ldots, v_{n-1,i}) \neq 0 \). Hence \( u^{e-1-l}v = u^{e-1}w_l \). Since \( u^{e-1-l}v \in C \), \( u^{e-1}w_l \in C \). So \( w_l \in \text{Tor}(C) \). Thus \( wt_H(w_l) \geq d_H(\text{Tor}(C)) \). Therefore, 
\[
wt_H(v) \geq wt_H(u^{e-1-l}v) = wt_H(u^{e-1}w_l) = wt_H(w_l) \geq d_H(\text{Tor}(C)).
\]
This shows that \( d_H(C) \geq d_H(\text{Tor}(C)) \). \( \square \)

**Proposition 4.4.** Let \( C = \langle g_0 g_1 \ldots g_{e-1} \rangle \) be an \((a + bu)\)-constacyclic code over \( R \). Then \( \text{Tor}(C) \) is the ideal of \( T_1 \) generated by \( g_{e-1} \).

**Proof.** Assume that \( h(x) \) is the monic polynomial of the lowest degree in \( \text{Tor}(C) \). Thus \( h(x) \) is a generator of \( \text{Tor}(C) \) as an ideal of \( T_1 \). Since \( u^{e-1}h(x) \in C \), \( h(x) = g_{e-1}(x) \) by Lemma 4.4. \( \square \)

**Example 4.5.** Let \( R = F_2 + uF_2 + u^2F_2 \), where \( u^3 = 0 \) and \( S = \frac{R[x]}{<x^{19} - (1 + u)>} \). In \( F_2[x] \), 
\[
x^{19} - 1 = f_1 f_2 f_3 f_4 f_5,
\]
where \( f_1 = x + 1 \), \( f_2 = x^2 + x + 1 \), \( f_3 = x^4 + x^3 + x^2 + x + 1 \), \( f_4 = x^4 + x^3 + 1 \) and \( f_5 = x^4 + x + 1 \) are irreducible polynomials. Now, consider the \((1 + u)\)-constacyclic code \( C = \langle f_1^2 f_2 f_3^4 \rangle \). We can see that \( |C| = 2^{19} \) and with the notations of Proposition 4.4, \( g_0 = f_1 f_2 f_4 \), \( g_1 = f_1 f_4 \) and \( g_2 = f_4 \). Since \( \text{Tor}(C) \) is an ideal of \( \frac{F_2[x]}{<x^{19} - 1>} \), it is the cyclic Hamming code generated by \( f_4 \) over \( F_2 \). Therefore, \( d_H(C) = d_H(\text{Tor}(C)) = 3 \).

With the previous notations, we see that \( d_H(C) = d_H(\text{Tor}(C)) \). Then we examine the \( a \)-constacyclic codes over \( F_q \). Recall that, for a polynomial \( f(x) \in F_q[x] \), the number of non-zero coefficients of \( f(x) \) in \( F_q[x] \) is called the weight of \( f(x) \) and is denoted by \( wt[f(x)] \).

**Lemma 4.6.** Suppose that \( n = mp^s \) and \( k(x) = f(x)(x^{mp^s-1} - c)^t \), where \( c \in F_q^* \), \( f(x) \in F_q[x] \) and \( \deg f < mp^s - 1 \). If \( t \leq p - 1 \), then \( wt[k(x)] = (t + 1).wt[f(x)] \) and \( \deg k < n \).

**Proof.** Suppose that \( wt[f(x)] = l \) and \( f(x) = a_{i_1} x^{i_1} + a_{i_2} x^{i_2} + \cdots + a_{i_r} x^{i_r} \), where for any \( r, 1 \leq r \leq l, a_{i_r} \neq 0 \). We have
\[
k(x) = \sum_{j=0}^{l} (\binom{l}{j})c^{l-j}(a_{i_1} x^{i_1 + jmp^{s-1}} + a_{i_2} x^{i_2 + jmp^{s-1}} + \cdots + a_{i_r} x^{i_r + jmp^{s-1}}).
\]
Since for any \( r, 1 \leq r \leq l, i_r \leq \deg f < mp^{s-1} \),
\[
i_r + jmp^{s-1} < mp^{s-1} + jmp^{s-1} = (1 + j)mp^{s-1} \leq mp^s = n.
\]
So \( \deg k < n \). Now, \( t \leq p - 1 \) implies that \( \binom{l}{j} \) is a non-zero element of \( F_q \). Hence \( (\binom{l}{j})c^{l-j} \neq 0 \).

Also, in the right-hand side of (2) the powers of \( x \) are different. So \( wt[k(x)] = (t + 1).wt[f(x)] \).
\( \square \)
Assume that \( k(x) = f_1^{α_1} f_2^{α_2} \cdots f_η^{α_η}, (0 ≤ α_j ≤ p^s) \) and \( a \) has an \( n \)-th root \( a_1 ∈ F_q^*. \) Suppose that \( r \) is a positive integer such that

\[ \text{i) For any } j, 1 ≤ j ≤ r, \text{ } α_j = (p - 1)p^{s-1} + d_j \text{ and } 0 < d_j ≤ p^{s-1}, \]

\[ \text{ii) For any } j, r + 1 ≤ j < η, \text{ } α_j ≤ (p - 1)p^{s-1}. \]

Then we have the following proposition.

**Proposition 4.7.** By the above notations, consider the \( a \)-constacyclic code \( D =< k(x) > \triangleleft T_1. \) Then

\[ d_H(D) ≤ p \cdot \text{wt}[f_1^{d_1} f_2^{d_2} \cdots f_r^{d_r}]. \]

**Proof.** Let \( D \neq 0 \) and \( l(x) = f_1^{d_1} f_2^{d_2} \cdots f_r^{d_r}. \) We have \( \deg l < mp^{s-1}. \) Thus

\[ \deg (l(x)(x^{mp^{s-1} - a_1^{mp^{s-1}}})^{p-1}) < mp^{s-1} + mp^{s-1}(p - 1) ≤ mp^s = n. \]

If \( h(x) = l(x)(x^{mp^{s-1} - a_1^{mp^{s-1}}})^{p-1}, \) then \( \text{wt}[h(x)] \) in \( F_q[x] \) is equal to the weight of \( h(x) \) in \( T_1. \) Now,

\[
\begin{align*}
h(x) &= l(x)(x^{mp^{s-1} - a_1^{mp^{s-1}}})^{p-1} \\
&= l(x)(f_1^{p-1} f_2^{p-1} \cdots f_η^{p-1})^{p-1} \\
&= (f_1^{(p-1)p^{s-1}+d_1} \cdots f_η^{(p-1)p^{s-1}+d_η})^{p-1} f_1^{α_1} \cdots f_η^{α_η} \\
&= k(x)(f_1^{(p-1)p^{s-1}+d_1} \cdots f_η^{(p-1)p^{s-1}+d_η})^{p-1} f_1^{α_1} \cdots f_η^{α_η} \in D.
\end{align*}
\]

By Lemma 4.8, \( \text{wt}[h(x)] = p \cdot \text{wt}[l(x)]. \) So \( d_H(D) ≤ p \cdot \text{wt}[l(x)]. \)

**Lemma 4.8.** Suppose that \( D =< k(x) > \) is an \( a \)-constacyclic code over \( F_q, \) where \( k(x) | x^n - a. \) If \( f(x) \) is a non-zero element of \( D, \) then there exists \( h(x) ∈ F_q[x] \) with \( \deg h < n - \deg k \) such that \( p(x) ≡ h(x)k(x) \pmod (x^n - a). \)

**Proof.** The proof is straightforward.

**Proposition 4.9.** [2] Theorem 6.3] For any polynomial \( p(x) \) over \( GF(p^r), \) the Galois field of order \( p^r, \) any non-zero element \( c \) of \( GF(p^r), \) and any non-negative integers \( n \) and \( N, \)

\[ \text{wt}[p(x)(x^n - c)^N] ≥ \text{wt}[(x^n - c)^N], \text{wt}[p(x) \pmod (x^n - c)]. \]

**Proposition 4.10.** Let \( D =< k(x) > \) be an \( a \)-constacyclic code over \( F_q, \) where \( k(x) \) divides \( x^n - a. \) If \( a_1 \) is an \( n \)-th root of \( a \) in \( F_q \) and \( i \) is the largest non-negative integer such that \( (x-a_1)^i | k(x) \), then

\[ d_H(D) ≥ \min\{\text{wt}[(x - a_1)^{i+j}] | 0 ≤ j < n - \deg k\}. \]
Proof. Assume that $f(x)$ is a non-zero element of $D$. Thus there exists $l(x) \in F_q[x]$ with $\deg l < n - \deg k$ such that $f(x) \equiv l(x)k(x) \pmod{(x^n - a)}$ by Lemma 4.8. Let $j$ be the largest non-negative integer such that $(x - a_1)^j \mid l(x)$. Now the weight of $f(x)$ in $T_1$ is equal to $\text{wt}[k(x)l(x)]$ in $F_q[x]$ and by Proposition 4.3, we have

$$\text{wt}[k(x)l(x)] = \text{wt}[(x - a_1)^{i+j}k(x)l(x)] = \text{wt}[(x - a_1)^{i+j}] + \text{wt}[k(x)l(x)] \mod (x - a_1)] \\ \geq \text{wt}[(x - a_1)^{i+j}].$$

So $d_H(D) \geq \min\{\text{wt}[(x - a_1)^{i+j}] \mid 0 \leq j < n - \deg k\}$. \(\square\)

Example 4.11. Consider $C = \langle u(x-1)^2 \rangle$ as an $(1+u)$–constacyclic code over $R = F_3 + uF_3$ ($u^2 = 0$) of length 6 ($C \lhd \frac{R[x]}{<x^6 - (1+u)>}$). We shall show that $d_H(C) = 2$. Obviously, $\text{Tor}(C)$ is the cyclic code of length 6 over $F_3$ generated by $(x - 1)^2$. By Proposition 4.10, $d_H(\text{Tor}(C)) \geq \min\{\text{wt}[(x - 1)^\alpha] \mid 2 \leq \alpha < 6\}$. So, $d_H(C) = d_H(\text{Tor}(C)) \geq 2$. Also $x^3 - 1$ is a codeword in $\text{Tor}(C)$ of weight 2. So the equality does hold.

Proposition 4.12. Suppose that $a_1 \in F_q^*$ is an $n$–th root of $a$. Let $D = \langle f_1^{\alpha_1}f_2^{\alpha_2} \ldots f_\eta^{\alpha_\eta} \rangle$, be an $a$–constacyclic code over $F_q$, where $f_1, f_2, \ldots, f_\eta$ are the monic irreducible divisors of $x^m - a_0$. If there exists $t$ such that $t \leq p - 1$ and $\alpha_j \leq tp^{s-1}$ for any $j$, then $d_H(D) \leq t + 1$.

Proof. We have

$$(x^{mp^{s-1}} - a_1^{mp^{s-1}})^t = ((x^m - a_1^m)^{p^{s-1}})^t = ((f_1 f_2 \ldots f_\eta)^{p^{s-1}})^t = (f_1^{tp^{s-1}} f_2^{tp^{s-1}} \ldots f_\eta^{tp^{s-1}}) \in D,$$

$$\text{wt}[(x^{mp^{s-1}} - a_1^{mp^{s-1}})^t] \leq t + 1 \text{ and } \deg (x^{mp^{s-1}} - a_1^{mp^{s-1}})^t < n. \text{ So } d_H(D) \leq t + 1. \square$$

5. Acknowledgments

The authors wish to sincerely thank the referees for several useful comments.
References


[7] X. Kai, S. Zhu and P. Li, $(1+u)$- Constacyclic codes over $\frac{F_{p^m}[u]}{\langle u^m \rangle}$, J. Franklin Institute, 347(2010), 751-762.


Marziyeh Beygi
Department of Mathematics, College of Sciences, Shiraz University, Shiraz, 71467-13565, Iran.
m.beygi@shirazu.ac.ir

Shohreh Namazi
Department of Mathematics, College of Sciences, Shiraz University, Shiraz, 71467-13565, Iran.
namazi@shirazu.ac.ir

Habib Sharif
Department of Mathematics, College of Sciences, Shiraz University, Shiraz, 71467-13565, Iran.
sharif@susc.ac.ir