Journal of Algebraic Structures and Their Applications
ISSN: 2382-9761
www.as.yazd.ac.ir

Algebraic Structures and Their Applications Vol. 6 No. 1 (2019) pp 65-82.

CONSTACYCLIC CODES OF ARBITRARY LENGTH OVER $F_q + uF_q + \cdots + u^{e-1}F_q$

MARZIYEH BEYGI, SHOHREH NAMAZI* AND HABIB SHARIF

Abstract. 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 [6], determined

DOI: 10.29252/as.2019.1355

MSC(2010): Primary:94B05, 94A55, 94B15, 58F15, 58F17.

Keywords: Linear code, constacyclic code, minimal spanning set, minimum Hamming distance.

Received: 07 July 2018, Accepted: 15 April 2019.

*Corresponding author

the structure of constacyclic codes of lengths p^s over $F_{p^k}+uF_{p^k}+\cdots+u^{m-1}F_{p^k}$, where $u^m=0$. In [7], Kai, Zhu and Li specify the structure of $(1+\lambda u)-$ Constacyclic codes over $\frac{F_p[u]}{<u^m>}$.

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 $\sum_{i=0}^{n-1}c_ix^i$. 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 $n=p^sm$, where $gcd(p,m)=1$, unless stated otherwise. Let a,b be non-zero elements in F_q and $\mathcal{S}=\frac{R[x]}{<x^n-(a+bu)>}$.

2. Some characterizations of $(a+bu)-$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 $k_i(x)\in F_q[x]$, $0\le i\le e-1$.
We have the following lemma whose proof is straightforward.

Lemma 2.1. *For any i, $0\le i\le e-1$, 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 $\mathcal{S}$. Then $k_0(x)=k_1(x)=\ldots=k_{e-1}(x)=0$ in $F_q[x]$.*

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

Consider the ring $T_e=\frac{F_q[x]}{<x^n-a>^e}$. 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* $k<en$ 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* $k_i<n$ ($0\le i\le e-1$).

In the ring $\mathcal{S}$ we have $u=b^{-1}(x^n-a)$. Now, applying Corollary 2.2, there exists an isomorphism ψ from $\mathcal{S}$ onto T_e which maps u to $b^{-1}(x^n-a)$. In fact, we have the following proposition.

Proposition 2.3. *Let $\psi : \mathcal{S} \to T_e$ be defined by*

$$\psi(\textstyle\sum_{i=0}^{e-1} u^i k_i(x)) = \sum_{i=0}^{e-1} b^{-i}(x^n - a)^i k_i(x),$$

where $k_i(x) \in F_q[x]$, for any i, $0 \leq i \leq e-1$ and deg $k_i < n$. Then ψ is a ring isomorphism as well as an $F_q[x]-$homomorphism.

Proof. Obviously, ψ 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 $\mathcal{S}$, 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,

$$\begin{aligned} k(x)l(x) &= \sum_{i=0}^{e-1} u^i (\sum_{j=0}^{i} k_j(x) l_{i-j}(x)) \\ &= \sum_{i=0}^{e-1}\sum_{j=0}^{i} u^i k_j(x) l_{i-j}(x). \end{aligned}$$

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 $\mathcal{S}$, $h_i(x) = buq_i(x) + s_i(x)$. Hence

$$\begin{aligned} k(x)l(x) &= \sum_{i=0}^{e-1} u^i (buq_i(x) + s_i(x)) \\ &= \sum_{i=0}^{e-1} bu^{i+1} q_i(x) + u^i s_i(x) \\ &= s_0(x) + \sum_{i=1}^{e-1} u^i (bq_{i-1}(x) + s_i(x)). \end{aligned}$$

Thus

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

Also,

$$\begin{aligned} \psi(k(x))\psi(l(x)) &= \sum_{i=0}^{e-1}\sum_{j=0}^{i} b^{-i}(x^n - a)^i k_j(x) l_{i-j}(x) \\ &= \sum_{i=0}^{e-1} b^{-i}(x^n - a)^i ((x^n - a)q_i(x) + s_i(x)) \\ &= \sum_{i=0}^{e-1} b^{-i}(x^n - a)^{i+1} q_i(x) + (x^n - a)^i s_i(x) \\ &= s_0(x) + \sum_{i=1}^{e-1} b^{-i}(x^n - a)^i (bq_{i-1}(x) + s_i(x)). \end{aligned}$$

Therefore $\psi(k(x)l(x)) = \psi(k(x))\psi(l(x))$. This show that ψ 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 $deg\ k_i < n$ ($0 \leq i \leq e-1$). We can see that $\psi(\sum_{i=0}^{e-1} b^i u^i k_i(x)) = k(x)$. Hence ψ is an epimorphism. The rest of the proof is straightforward. □

Remark 2.4. *i*) Since T_e is a principal ideal ring, $\mathcal{S}$ is too. We shall now determine the unique form of a generator of an ideal of $\mathcal{S}$.
ii) Note that, here $b \neq 0$. The reader should be careful that the ideals of $\mathcal{S}$ are different from the ideals of the ring $\frac{R[x]}{<x^n-a>}$(this ring is not a principal ideal ring).

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

Lemma 2.5. *Let* $C =< \prod_{i=1}^{\eta} f_i^{\alpha_i} >$ *and* $D =< \prod_{i=1}^{\eta} f_i^{\beta_i} >$ *be two ideals of* T_e*, where* $0 \leq \alpha_i, \beta_i \leq ep^s$*. 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

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

Since $0 \leq \beta_i \leq ep^s$, $\prod_{i=1}^{\eta} f_i^{\beta_i} \mid (x^n - a)^e$ 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 ψ, $\mathcal{S}$, 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* $n = mp^s$ *over* R*. Then as an ideal of* $\mathcal{S}$*,* C *has a unique generator of the form* $\prod_{i=1}^{\eta} f_i^{\alpha_i}$*, where* $0 \leq \alpha_i \leq ep^s$ *and* f_i *are distinct monic irreducible divisors of* $x^m - a_0$ *in* $F_q[x]$*.*

Proof. Since $C \trianglelefteq \mathcal{S}$, $\psi(C) \trianglelefteq T_e$ (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 $0 \leq \alpha_i \leq ep^s$. 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 [7], Theotems 4.3, 4.5 and Corollary 4.7). Dinh et. al. [4] and also Guenda et. al. [5] seem to have used the uniqueness of the generators of constacyclic codes, implicitely, to calculate their numbers, although they have not pointed to it.

(ii) The authors of [4] and [5] have calculated $\mid C \mid$, 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 $x^m - a_0$ are greater than p^s, the equality does not hold). We shall find the exact number $\mid C \mid$, in the following corollary.

Corollary 2.8. (i) *Let* $C =< \prod_{i=1}^{\eta} f_i^{\alpha_i} >$ *and* $D =< \prod_{i=1}^{\eta} f_i^{\beta_i} >$ *be ideals of* $\mathcal{S}$*, 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* $C =< \prod_{i=1}^{\eta} f_i^{\alpha_i} >$ *is an* $(a+bu)-$*constacyclic code over* R*, then* $\mid C \mid = q^{en - \sum_{i=1}^{\eta} \alpha_i deg\ f_i}$*.*

Proof. (i) Soppose 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 2.5.
(ii) By the uniqueness of generators of these codes, the proof is straightforward.
(iii) Since $\mid C \mid = \mid \psi(C) \mid$ and $\psi(C)$ is an ideal of T_e, $\mid C \mid = q^{en - \sum_{i=1}^{\eta} \alpha_i deg\ f_i}$. □

Lemma 2.9. *Let* $C =< \prod_{i=1}^{\eta} f_i^{\alpha_i} >$ *be an ideal of* $\mathcal{S}$*,* $0 \leq \alpha_i \leq ep^s$*. 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 $< x^n - a >^l \subseteq < \prod_{i=1}^{\eta} f_i^{\alpha_i} >$ 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 2.5). □

Let $C =< \prod_{i=1}^{\eta} f_i^{\alpha_i} >$ 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

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

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 $0 =$

$s_0 \leq s_1 \leq \ldots \leq s_e = \eta$, $0 \leq \alpha_1, \alpha_2, \ldots, \alpha_{s_1} \leq p^s < \alpha_{s_1+1}, \ldots, \alpha_{s_2} \leq 2p^s < \ldots \leq (e-1)p^s < \alpha_{s_{e-1}+1}, \ldots, \alpha_{s_e} \leq ep^s$. Suppose that

$$\begin{aligned}
\alpha_{s_1+j_1} &= p^s + \beta_{s_1+j_1}, & 0 < \beta_{s_1+j_1} \leq p^s \\
\alpha_{s_2+j_2} &= 2p^s + \beta_{s_2+j_2}, & 0 < \beta_{s_2+j_2} \leq p^s \\
&\vdots \\
\alpha_{s_{e-1}+j_{e-1}} &= (e-1)p^s + \beta_{s_{e-1}+j_{e-1}}, & 0 < \beta_{s_{e-1}+j_{e-1}} \leq p^s.
\end{aligned}$$

We have

$$\begin{aligned}
g_0(x) &= gcd(f(x), x^n - a) = (f_{s_0+1}^{\alpha_1} \ldots f_{s_1}^{\alpha_{s_1}})(\prod_{i=s_1+1}^{\eta} f_i^{p^s}) \\
g_1(x) &= gcd(\frac{f(x)}{g_0(x)}, g_0(x)) = (f_{s_1+1}^{\beta_{s_1+1}} \ldots f_{s_2}^{\beta_{s_2}})(\prod_{i=s_2+1}^{\eta} f_i^{p^s}) \\
&\vdots \\
g_{e-2}(x) &= gcd(\frac{f(x)}{g_0(x)g_1(x)\ldots g_{e-3}(x)}, g_{e-3}(x)) = (f_{s_{e-2}+1}^{\beta_{s_{e-2}+1}} \ldots f_{s_{e-1}}^{\beta_{s_{e-1}}})(\prod_{i=s_{e-1}+1}^{\eta} f_i^{p^s}) \\
g_{e-1}(x) &= gcd(\frac{f(x)}{g_0(x)g_1(x)\ldots g_{e-2}(x)}, g_{e-2}(x)) = (f_{s_{e-1}+1}^{\beta_{s_{e-1}+1}} \ldots f_{s_e}^{\beta_{s_e}}).
\end{aligned}$$

(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 $g_{e-1}(x) \mid \cdots \mid g_1(x) \mid g_0(x) \mid x^n - a$ 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 $C =< g_0 g_1 \ldots g_{e-1} >$, where g_i are monic polynomials in $F_q[x]$ such that $g_{e-1}(x) \mid \cdots \mid g_1(x) \mid g_0(x) \mid x^n - a$. Also $\mid C \mid = q^{en - \sum_{i=0}^{e-1} t_i}$ 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 $C =< g_0 g_1 \ldots g_{e-1} >$ be an $(a+bu)-$constacyclic code over R and l be a non-negative integer less than e. Then $< u^l > \subseteq C$ if and only if $g_l = g_{l+1} = \cdots = g_{e-1} = 1$.*

Proof. By Lemma 2.9, $< u^l > \subseteq C$ 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 disscussion preceding Proposition 2.10. □

Lemma 2.12. *Let $C =< g_0 g_1 \ldots g_{e-1} >$ 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 $g_0g_1\dots g_{e-1} \mid g_{e-1}(x^n-a)^{e-1}$. Thus $u^{e-1}g_{e-1} \in C$. By the division algorithm in $F_q[x]$,

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

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 ψ is the isomorphism in Proposition 2.3. So there exists $h(x) \in T_e$, where $deg\ h < en - \sum_{i=0}^{e-1} t_i$, such that $(x^n-a)^{e-1}f(x) = g_0g_1\dots g_{e-1}h(x)$. Since the degree of two sides of the above equality is lower than en, we can consider this equality in $F_q[x]$. Hence $(x^n-a)^{e-1} = g_0g_1\dots g_{e-2}g(x)h(x)$. Let $D =< g_0g_1\dots g_{e-2}g > \trianglelefteq \mathcal{S}$. Then $u^{e-1} = (x^n-a)^{e-1} \in D$ and $g(x) \mid g_{e-2}(x) \mid \cdots \mid g_1(x) \mid g_0(x) \mid x^n-a$. By Lemma 2.11 for D, $g(x) = 1$. Hence $f(x) = g_{e-1}$. □

Proposition 2.13. *Let $C =< g_0g_1\dots g_{e-1} >$ be an $(a+bu)-$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 $deg\ d_i < n$, $0 \le i \le e-1$. There exists the smallest non-negative integer j, $0 \le j \le e-1$, such that $deg\ d_j = deg\ d$. For any l, $0 \le l \le j-1$, $deg\ d_l < deg\ d$. Now, $u^{e-1}d_0(x) = u^{e-1}d(x) \in C$. Since $d(x)$ has the lowest degree in C and $deg\ d_0 = deg\ u^{e-1}d_0 < deg\ d$, $u^{e-1}d_0(x) = 0$ 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 $deg\ d_1 = deg\ u^{e-1}d_1 < deg\ d$, $d_1(x) = 0$. Similarly, $d_2(x) = \dots = d_{j-1}(x) = 0$. Now $u^{e-1}d_j(x) = u^{e-1-j}d(x) \in C$. Since $deg\ u^{e-1}d_j = deg\ d_j = deg\ d$, $u^{e-1}d_j(x)$ has the lowest degree in C. So by Lemma 2.12, $d_j(x) = g_{e-1}(x)$. Hence $deg\ d = deg\ d_j = deg\ g_{e-1} = deg\ u^{e-1}g_{e-1}$. 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 $(a+bu)-$constacyclic code over R. Let us define the following notations. If $h_j(x)$, $-1 \le j \le r$, are polynomials in $F_q[x]$ such that $deg\ h_j = t_j$ and

$$h_r(x) \mid \dots \mid h_0(x) \mid h_{-1}(x), \tag{1}$$

then we assign the underling set $\{f(x), xf(x), \dots, x^{t_{-1}-t_0-1}f(x) \mid f = \prod_{i=0}^{r} h_i\}$ for the property (1). If $t_{-1} = t_0$, then the empty set $\varnothing$ 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 $k(x) \in \mathcal{S}$, 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 $C =< g_0g_1 >$ 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*

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

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

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

$$\sum_{i=0}^{n-t_0-1} (k_i + uk'_i)x^i g_0g_1 + \sum_{j=0}^{t_0-t_1-1} d_j x^j ug_1 = 0, \tag{2}$$

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 $k(x) = \sum_{i=0}^{n-t_0-1} k_i x^i$, $k'(x) = \sum_{i=0}^{n-t_0-1} k'_i x^i$ and $d(x) = \sum_{j=0}^{t_0-t_1-1} d_j x^j$. We show that $k(x)$, $k'(x)$ and $d(x)$ are zero. In $\mathcal{S}$, $g_1(x)[k(x)g_0(x) + uk'(x)g_0(x) + ud(x)] = 0$. 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 (2),

$$uk'(x)g_0(x)g_1(x) + ud(x)g_1(x) = 0, \tag{3}$$

in $\mathcal{S}$. 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 $g_0(x) \mid q(x)$. Assume that $q(x) = g_0(x)q'(x)$, *deg* $q' \leq n - t_0 - 1$. Hence in $\mathcal{S}$, $k'(x)g_0(x)g_1(x) = bus(x) + g_0(x)q'(x)$. 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 $g_0(x) \mid d(x)g_1(x)$. 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 2.13, $ug_1(x)$ 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, $\mid \widehat{\Delta} \mid = 2n - t_0 - t_1$ is equal to the dimension of C as a vector space over F_q (by Corollary 2.8, part (iii)). So $\widehat{\Delta}$ is an spanning set for C as an F_q-module. Hence Δ generate C as an $R-$module. Also since $\widehat{\Delta}$ is linearly independent, Δ is a minimal spanning set for C. □

In the following lemma, we determine the minimal spanning set for the constacyclic code $C =< u^k g(x) >$ 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 2.9). This lemma is used in the proof of Proposition 3.8.

Lemma 3.3. *Let $C =< u^k g(x) >$ be an $(a+bu)-$constacyclic code over R, where $g(x) \mid x^n - a$, $0 \le k \le e-1$ 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 $0 \le k \le e-2$ and $\varnothing$, if $k = e-1$. Then $\Omega = u^k B_0 \bigcup u^{k+1} B_1$ is a minimal spanning set for C as an R-module. Also, $\mid C \mid = q^{(e-k)n-t}$.*

Proof. First, we show that Ω 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 $deg\ l \le n-t-1$, then we are done. Suppose that $deg\ l \ge n-t$. In $R[x]$,

$l(x) = (\frac{x^n - a}{g(x)}) q(x) + s(x)$, where $deg\ s \le n-t-1$ and $deg\ q \le t-1$.

Now in $\mathcal{S}$,

$$\begin{aligned} c(x) &= u^k g(x)((\frac{x^n - a}{g(x)}) q(x) + s(x)) \\ &= u^k q(x)(x^n - a) + u^k g(x) s(x) \\ &= b u^{k+1} q(x) + u^k g(x) s(x). \end{aligned}$$

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

$$\Omega = \{u^k g, x u^k g, \ldots, x^{n-t-1} u^k g, u^{k+1}, x u^{k+1}, \ldots, x^{t-1} u^{k+1}\}$$

is a spanning set for C if $0 \le k \le e-2$. Also if $k = e-1$, then

$$\Omega = \{u^{e-1} g, x u^{e-1} g, \ldots, x^{n-t-1} u^{e-1} g\}$$

is a spanning set for C. We claim that Ω is a minimal spanning set. For, it is enough to show that

$$\textstyle\sum_{i=0}^{n-t-1} (\sum_{j=0}^{e-k-1} l_{ji} u^j) x^i u^k g + \sum_{i'=0}^{t-1} (\sum_{j'=0}^{e-k-2} d_{j'i'} u^{j'}) x^{i'} u^{k+1} = 0,$$

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

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

Since the degree of all polynomials in the above equality is lower than n, by applying Lemma 2.1, we have,

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

Since $g(x) \neq 0$, $l_0(x) = 0$. Also $deg\ (l_j g) > deg\ d_{j-1}$ implies that $l_j(x) = d_{j-1}(x) = 0$.
To prove the last statement of the lemma, note that $\psi(C) =< (x^n - a)^k g(x) >$ and $\mid \psi(C) \mid = q^{en-kn-t}$. Hence $\mid C \mid = q^{(e-k)n-t}$. $\square$

For every positive integer j, set $T_j = \frac{F_q[x]}{<x^n - a>^j}$. If $i \le j$, then clearly T_i is a homomorphic image of T_j. Consider the natural ring epimorphism $\pi_{ji} : T_j \longrightarrow T_i$ with $ker \pi_{ji} = \frac{<x^n - a>^i}{<x^n - a>^j}$. Note that for polynomials $h_1(x)$ and $h_2(x)$ in $F_q[x]$, if $h_1(x) \equiv h_2(x) \pmod{(x^n - a)^j}$, then

$\pi_{ji}(h_1(x)) \equiv \pi_{ji}(h_2(x)) \pmod{(x^n-a)^i}$. Obviously, every $h(x) \in T_j$ has a unique representation $h(x) = \sum_{l=0}^{j-1} h_l(x)(x^n-a)^l$, 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

$$\begin{aligned}\pi_{ji}(h(x)) &= \pi_{ji}(\sum_{l=0}^{j-1} h_l(x)(x^n-a)^l) \\ &= \sum_{l=0}^{i-1} h_l(x)(x^n-a)^l.\end{aligned}$$

For $j \geq 2$, consider the finite chain ring $R_j = F_q + u_jF_q + \cdots + u_j^{j-1}F_q$, where $u_j^j = 0$ 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_i is a homomorphic image of S_j.

Proposition 3.4. *Let i and j be two integers such that $1 < i \leq j$. Then there exists an epimorphism $\beta_{ji} : S_j \longrightarrow S_i$ 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 2.3, consider $\psi_j : S_j \to T_j$ by

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

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 β_{ji} is an epimorphism and $ker\beta_{ji} = \psi_j^{-1}(ker\pi_{ji})$. Hence $ker\beta_{ji} =< u_j^i >$. Furthermore, $\beta_{ji}(u_j) = u_i$. 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 $C =< \prod_{l=1}^{\eta} f_l^{\alpha_l} >$ be an $(a+bu)-$constacyclic code over R_j, where $0 \leq \alpha_l \leq jp^s$. If $i \leq j$ and $< u_j^i > \subseteq C$, then $\beta_{ji}(C)$ as an ideal of S_i generated by $\prod_{l=1}^{\eta} f_l^{\alpha_l}$.*

Proof. Since $< u_j^i >\subseteq C$, by Lemma 2.9, $0 \leq \alpha_l \leq ip^s$ for any l, $1 \leq l \leq \eta$. Hence $deg\ (\prod_{l=1}^{\eta} f_l^{\alpha_l}) < ni$. So $\beta_{ji}(\prod_{l=1}^{\eta} f_l^{\alpha_l}) = \prod_{l=1}^{\eta} f_l^{\alpha_l}$, by Lemma 3.6. Since C contains $ker\beta_{ji}$, we can see that $\beta_{ji}(C)$ is an ideal of S_i generated by $\beta_{ji}(\prod_{l=1}^{\eta} f_l^{\alpha_l})$. □

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 $S_2 = \frac{R_2[x]}{<x^n-(a+bv)>}$.

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,*

$$u^2k_0(x)g_0g_1 + u^2k_1(x)g_1 = 0,$$

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 2.1. Let $g_0(x) \neq x^n - a$ and $C =< g_0g_1 >$ be the $(a + bu)-$constacyclic code over R_3. Consider

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

We show that $\Delta = A_0 \bigcup uA_1 \bigcup u^2A_2$ is a spanning set for C as an R_3-module. Clearly, every element of Δ is in C. Suppose that $\beta = \beta_{32} : S_3 \longrightarrow S_2$ is the epimorphism in Proposition 3.4. Since $deg\ (g_0g_1) < 2n$, by Lemma 3.7, $\beta(C)$ is the ideal of S_2 generated by g_0g_1. By Proposition 3.2, the set

$$\{g_0g_1, xg_0g_1, \ldots, x^{n-t_0-1}g_0g_1\} \bigcup \{vg_1, xvg_1, \ldots, x^{t_0-t_1-1}vg_1\}$$

is a minimal spanning set for $\beta(C)$. Also by Lemma 3.3, 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

$$c(x) = \sum_{i=0}^{n-t_0-1} r_ix^ig_0g_1 + \sum_{j=0}^{t_0-t_1-1} s_jx^jug_1 + \sum_{l=0}^{n-1} d_lx^lu^2,$$

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 Δ. 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 Δ. Since $ux^ig_1(x) \in \Delta$ for any i, $0 \leq i \leq t_0-t_1-1$, inductively, for i, $0 \leq i \leq t_0 - t_1 - 1$, $u^2x^{t_1+i} = u^2x^ig_1(x) + u^2x^il(x)$ is generated by elements of Δ.

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

$$u^2x^{t_0+j} = u^2[b_jx^jg_0(x) + b_{j-1}x^{j-1}g_0(x) + \cdots + b_0g_0(x) + k(x)],$$

where $0 \leq j \leq n-t_0-1$. We saw that $u^2k(x)$ is in the R_3-module generated by Δ. It is enough to prove that $u^2x^ig_0(x)$, $0 \leq i \leq j$, is generated by the elements of Δ. 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

$$ux^ig_0(x) - (\sum_{i=0}^{n-t_0-1} r'_ix^ig_0g_1 + \sum_{j=0}^{t_0-t_1-1} s'_jx^jug_1) \in ker\beta =< u^2 >.$$

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, Δ is a spanning set for C. Consider $\widehat{\Delta} = \bigcup_{l=0}^{2}\bigcup_{j=l}^{2} u^jA_l$. Since Δ is a spanning set for C as an R_3-module, $\widehat{\Delta}$ is a spanning set for C as an F_q-module. Now $\mid \widehat{\Delta} \mid= q^{3n-t_0-t_1}$ is equal to the dimension of C as a vector space, by Proposition 2.10. So $\widehat{\Delta}$ 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`

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 $\Gamma = \bigcup_{j=0}^{2} u^jA_j$ is a minimal spanning set for C.*

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

$$\sum_{l=0}^{2}\sum_{j=l}^{2}\sum_{i=0}^{t_{l-1}-t_l-1} z_{lji}u^jx^i\prod_{r=l}^{2} g_r = 0, \text{ where } t_{-1} = n \text{ and } z_{lji} \in F_q.$$

In $F_q[x]$, set $k_{lj} = \sum_{i=0}^{t_{l-1}-t_l-1} z_{lji}x^i$. Hence in S_3,

$$(k_{00}(x) + uk_{01}(x) + u^2k_{02}(x))g_0g_1g_2 + (k_{11}(x) + uk_{12}(x))ug_1g_2 + k_{22}(x)u^2g_2 = 0.$$

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

$$\begin{aligned} k_{00}(x)g_0g_1g_2 &= (x^n - a)h_0(x) \\ k_{01}(x)g_0g_1g_2 + k_{11}(x)g_1g_2 &= (x^n - a)h_1(x) - bh_0(x) \\ k_{02}(x)g_0g_1g_2 + k_{12}(x)g_1g_2 + k_{22}(x)g_2 &= (x^n - a)h_2(x) - bh_1(x). \end{aligned}$$

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 $(x^n-a) \mid k_{00}(x)g_0(x)$. Since $deg\ k_{00}g_0 < n$, $k_{00}(x) = h_0(x) = 0$. So $k_{01}(x)g_0g_1g_2+k_{11}(x)g_1g_2 = (x^n - a)h_1(x)$. Therefore, $k_{01}(x)g_0g_1 + k_{11}(x)g_1 = (x^n - a)\frac{h_1(x)}{g_2}$. Now, in S_3, $u^2k_{01}(x)g_0g_1 + u^2k_{11}(x)g_1 = 0$. 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 $k_{02}(x)g_0g_1g_2 + k_{12}(x)g_1g_2 = (x^n - a)h_2(x)$. By the division algorithm in $F_q[x]$,

$$h_2(x) = g_2(x)q(x) + s(x), \text{ where } deg\ s < deg\ g_2.$$

So in S_3, $uk_{02}(x)g_0g_1g_2+uk_{12}(x)g_1g_2 = u^2g_2(x)q(x)+u^2s(x)$. Thus $u^2s(x) \in C$. Since $deg\ s < deg\ g_2$, by Proposition 2.13, $s(x) = 0$. Hence $k_{02}(x)g_0g_1g_2 + k_{12}(x)g_1g_2 = (x^n - a)g_2(x)q(x)$. So $k_{02}(x)g_0g_1 + k_{12}(x)g_1 = (x^n - a)q(x)$. Now, in S_3, $u^2k_{02}(x)g_0g_1 + u^2k_{12}(x)g_1 = 0$. By Proposition 3.8, $k_{02}(x) = k_{12}(x) = 0$. Therefore, $\widehat{\Gamma}$ is linearly independent over F_q. So Γ is a minimal set over R_3. Since the number of elements of $\widehat{\Gamma}$ is equal to the dimension of C, $\widehat{\Gamma}$ is a basis for C over F_q. Thus Γ is a minimal spanning set for C over R_3. $\square$

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

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

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

Proof. For $e = 2$, we have Proposition 3.2. 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 3.9, we are done. $\square$

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 $Tor(C)$ 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, $0 \leq i \leq e-1$, $u^ih_1(x) \equiv u^ih_2(x)$ (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 $F_q[x]$,

$$\begin{aligned}
0 &= (x^n - a)k_0(x) \\
0 &= (x^n - a)k_1(x) - bk_0(x) \\
&\vdots \\
0 &= (x^n - a)k_{i-1}(x) - bk_{i-2}(x) \\
h_1(x) - h_2(x) &= (x^n - a)k_i(x) - bk_{i-1}(x).
\end{aligned}$$

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 $F_q[x]$. □

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 4.1. □

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

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

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

$$\mathbf{v} = (\textstyle\sum_{i=0}^{e-1} v_{0i}u^i, \sum_{i=0}^{e-1} v_{1i}u^i, \ldots, \sum_{i=0}^{e-1} v_{n-1,i}u^i)$$

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 $\mathbf{v} = \sum_{i=0}^{e-1}(v_{0i}, v_{1i}, \ldots, v_{n-1,i})u^i$. Suppose that l is the lowest integer such that $\mathbf{w}_l = (v_{0l}, v_{1l}, \ldots, v_{n-1,l}) \neq 0$. Hence $u^{e-1-l}\mathbf{v} = u^{e-1}\mathbf{w}_l$. Since $u^{e-1-l}\mathbf{v} \in C$, $u^{e-1}\mathbf{w}_l \in C$. So $\mathbf{w}_l \in Tor(C)$. Thus $wt_H(\mathbf{w}_l) \geq d_H(Tor(C))$. Therefore,

$$wt_H(\mathbf{v}) \geq wt_H(u^{e-1-l}\mathbf{v}) = wt_H(u^{e-1}\mathbf{w}_l) = wt_H(\mathbf{w}_l) \geq d_H(Tor(C)).$$

This shows that $d_H(C) \geq d_H(Tor(C))$. □

Proposition 4.4. *Let $C =< g_0 g_1 \ldots g_{e-1} >$ be an $(a+bu)-$constacyclic code over R. Then $Tor(C)$ 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 $Tor(C)$. Thus $h(x)$ is a generator of $Tor(C)$ as an ideal of T_1. Since $u^{e-1}h(x) \in C$, $h(x) = g_{e-1}(x)$ by Lemma 2.12. □

Example 4.5. Let $R = F_2 + uF_2 + u^2F_2$, where $u^3 = 0$ and $\mathcal{S} = \frac{R[x]}{<x^{15}-(1+u)>}$. In $F_2[x]$, $x^{15}-1 = f_1 f_2 f_3 f_4 f_5$, 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 $C =< f_1^2 f_2 f_4^3 >$. We can see that $\mid C \mid = 2^{19}$ and with the notations of Proposition 2.10, $g_0 = f_1 f_2 f_4$, $g_1 = f_1 f_4$ and $g_2 = f_4$. Since $Tor(C)$ is an ideal of $\frac{F_2[x]}{<x^{15}-1>}$, it is the cyclic Hamming code generated by f_4 over F_2. Therefore, $d_H(C) = d_H(Tor(C)) = 3$.

With the previous notations, we see that $d_H(C) = d_H(Tor(C))$. 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 $f(x) = a_{i_1}x^{i_1} + a_{i_2}x^{i_2} + \cdots + ai_l x^{i_l}$, where for any r, $1 \leq r \leq l$, $a_{i_r} \neq 0$. We have

$$k(x) = \sum_{j=0}^{t} \tbinom{t}{j} c^{t-j}(a_{i_1}x^{i_1+jmp^{s-1}} + a_{i_2}x^{i_2+jmp^{s-1}} + \cdots + a_{i_l}x^{i_l+jmp^{s-1}}). \quad (4)$$

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 $\binom{t}{j}$ is a non-zero element of F_q. Hence $\binom{t}{j}c^{t-j} \neq 0$. Also, in the righthand side of (4) the powers of x are different. So $wt[k(x)] = (t+1).wt[f(x)]$.
□

Assume that $k(x) = f_1^{\alpha_1} f_2^{\alpha_2} \dots f_\eta^{\alpha_\eta}, (0 \leq \alpha_j \leq p^s)$ and a has an $n-$th root $a_1 \in F_q^*$. Suppose that r is a positive integer such that

$i)$ For any j, $1 \leq j \leq r$, $\alpha_j = (p-1)p^{s-1} + d_j$ and $0 < d_j \leq p^{s-1}$,

$ii)$ For any j, $r+1 \leq j < \eta$, $\alpha_j \leq (p-1)p^{s-1}$.

Then we have the following proposition.

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

$$d_H(D) \leq p.wt[f_1^{d_1} f_2^{d_2} \dots f_r^{d_r}].$$

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

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

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

$$\begin{aligned} h(x) &= l(x)(x^{mp^{s-1}} - a_1^{mp^{s-1}})^{p-1} \\ &= l(x)(f_1 f_2 \dots f_\eta)^{(p-1)p^{s-1}} \\ &= (f_1^{(p-1)p^{s-1}+d_1} \dots f_r^{(p-1)p^{s-1}+d_r} f_{r+1}^{\alpha_{r+1}} \dots f_\eta^{\alpha_\eta})(f_{r+1}^{(p-1)p^{s-1}-\alpha_{r+1}} \dots f_\eta^{(p-1)p^{s-1}-\alpha_\eta}) \\ &= k(x)(f_{r+1}^{(p-1)p^{s-1}-\alpha_{r+1}} \dots f_\eta^{(p-1)p^{s-1}-\alpha_\eta}) \in D. \end{aligned}$$

By Lemma 4.6, $wt[h(x)] = p.wt[l(x)]$. So $d_H(D) \leq p.wt[l(x)]$. □

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

Proof. The proof is straightforward. □

Proposition 4.9. [8, 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,*

$$wt[p(x)(x^n - c)^N] \geq wt[(x^n - c)^N].wt[p(x)\ \mathtt{mod}\ (x^n - c)].$$

□

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

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

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 $wt[k(x)l(x)]$ in $F_q[x]$ and by Proposition 4.9, we have

$$\begin{aligned} wt[k(x)l(x)] &= wt[(x-a_1)^{i+j}\frac{k(x)l(x)}{(x-a_1)^{i+j}}] \\ &\geq wt[(x-a_1)^{i+j}].wt[\frac{k(x)l(x)}{(x-a_1)^{i+j}} mod(x-a_1)] \\ &\geq wt[(x-a_1)^{i+j}]. \end{aligned}$$

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

Example 4.11. Consider $C =< u(x-1)^2 >$ 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, $Tor(C)$ is the cyclic code of length 6 over F_3 generated by $(x-1)^2$. By Proposition 4.10, $d_H(Tor(C)) \geq min\{wt[(x-1)^\alpha] \mid 2 \leq \alpha < 6\}$. So, $d_H(C) = d_H(Tor(C)) \geq 2$. Also $x^3 - 1$ is a codeword in $Tor(C)$ 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 $D =< f_1^{\alpha_1} f_2^{\alpha_2} \ldots f_\eta^{\alpha_\eta} >$, 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

$$\begin{aligned} (x^{mp^{s-1}} - a_1^{mp^{s-1}})^t &= ((x^m - a_1^m)^{p^{s-1}})^t \\ &= ((f_1 f_2 \ldots f_\eta)^{p^{s-1}})^t \\ &= (f_1^{tp^{s-1}} f_2^{tp^{s-1}} \ldots f_\eta^{tp^{s-1}}) \\ &= (f_1^{\alpha_1} f_2^{\alpha_2} \ldots f_\eta^{\alpha_\eta})(f_1^{tp^{s-1}-\alpha_1} f_2^{tp^{s-1}-\alpha_2} \ldots f_\eta^{tp^{s-1}-\alpha_\eta}) \in D, \end{aligned}$$

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

5. Acknowledgments

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

References

[1] T. G. K. Bakshi and M. Raka, A class of constacyclic codes over a finite field, *Finite Field Appl.*, **18**(2012), 362-377.

[2] B. Chen, Y. Fan, L. Lin and H. Liu, Constacyclic codes over finite fields, *Finite Field Appl.*, **18**(2012), 1217-1231.

[3] H. Q. Dinh, Constacyclic codes of length p^s over $F_{p^m} + uF_{p^m}$, *J. Algebra*, **324**(2010), 940-950.

[4] H. Q. Dinh and H. D. T. Nguyen, On some classes of Constacyclic codes over polynomial residue rings, *Advances in Math. of comm.*, **6**(2)(2012), 175-191.

[5] K.Guenda and T. A. Gulliver, Repeated root Constacyclic codes of length mp^s over $F_{p^r} + uF_{p^r} + \ldots + u^{e-1}F_{p^r}$, *J. Algebra and its Appl.*, **14**(1)(2015), 1450081(12 pages).

[6] S. Jitman and P. Udomkavanich, On the structure of constacyclic codes of length p^s over $F_{p^k} + uF_{p^k} + \cdots + u^{m-1}F_{p^k}$, *Int. J. Algebra*, **4**(11)(2010), 507-516.

[7] X.Kai, S. Zhu and P. Li, $(1 + \lambda u)-$ Constacyclic codes over $\frac{F_p[u]}{<u^m>}$, *J. Franklin Institute*, **347**(2010), 751-762.

[8] J. L. Massey, D. J. Costello and J. Justesen, Polynomial weights and code constructions, *IEEE Trans. Inform. Theory*, **19**(1)(1973), 101-1

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