ARTICLE IN PRESS

Discrete Mathematics ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Complete classification of $(\delta + \alpha u^2)$-constacyclic codes over $\mathbb{F}_{2^m}[u]/\langle u^4\rangle$ of oddly even length

Yuan Cao, Yonglin Cao *, Fanghui Ma

School of Mathematics and Statistics, Shandong University of Technology, Zibo, Shandong 255091, China

ARTICLE INFO

Article history:
Received 2 January 2017
Received in revised form 6 June 2017
Accepted 2 August 2017
Available online xxxx

Keywords:
Constacyclic code
Linear code
Finite chain ring
Additive code

ABSTRACT

Let $\mathbb{F}_{2^m}$ be a finite field of cardinality 2^m, $R = \mathbb{F}_{2^m}[u]/\langle u^4\rangle$ and n be an odd positive integer. For any $\delta, \alpha \in \mathbb{F}_{2^m}^{\times}$, ideals of the ring $R[x]/\langle x^{2n} - (\delta + \alpha u^2)\rangle$ are identified as $(\delta+\alpha u^2)$-constacyclic codes of length $2n$ over R. In this paper, an explicit representation and enumeration for all distinct $(\delta+\alpha u^2)$-constacyclic codes of length $2n$ over R are presented.

1. Introduction

Algebraic coding theory deals with the design of error-correcting and error-detecting codes for the reliable transmission of information across noisy channel. The class of constacyclic codes plays a very significant role in the theory of error-correcting codes. It includes as a subclass the important class of cyclic codes, which has been well studied since the late 1950s. Constacyclic codes also have practical applications as they can be efficiently encoded with simple shift registers. This family of codes is thus interesting for both theoretical and practical reasons.

Let Γ be a commutative finite ring with identity $1 \neq 0$, and $\Gamma^{\times}$ be the multiplicative group of invertible elements of Γ. For any $a \in \Gamma$, we denote by $\langle a\rangle_{\Gamma}$, or $\langle a\rangle$ for simplicity, the ideal of Γ generated by a, i.e. $\langle a\rangle_{\Gamma} = a\Gamma = \{ab \mid b \in \Gamma\}$. For any ideal I of Γ, we will identify the element $a + I$ of the residue class ring Γ/I with $a \pmod I$ for any $a \in \Gamma$ in this paper.

A *code* of length N over Γ is a nonempty subset $\mathcal{C}$ of $\Gamma^N = \{(a_0, a_1, \ldots, a_{N-1}) \mid a_j \in \Gamma, j = 0, 1, \ldots, N-1\}$. The code $\mathcal{C}$ is said to be *linear* if $\mathcal{C}$ is a Γ-submodule of Γ^N. All codes in this paper are assumed to be linear. Let $\lambda \in \Gamma^{\times}$. A linear code $\mathcal{C}$ of length N over Γ is called a λ-*constacyclic code* if $(\lambda c_{N-1}, c_0, c_1, \ldots, c_{N-2}) \in \mathcal{C}$ for all $(c_0, c_1, \ldots, c_{N-1}) \in \mathcal{C}$. Particularly, $\mathcal{C}$ is called a *negacyclic code* if $\lambda = -1$, and $\mathcal{C}$ is called a *cyclic code* if $\lambda = 1$. For any $a = (a_0, a_1, \ldots, a_{N-1}) \in \Gamma^N$, let $a(x) = a_0 + a_1x + \cdots + a_{N-1}x^{N-1} \in \Gamma[x]/\langle x^N - \lambda\rangle$. We will identify a with $a(x)$ in this paper. Then $\mathcal{C}$ is a λ-constacyclic code of length N over Γ if and only if $\mathcal{C}$ is an ideal of the residue class ring $\Gamma[x]/\langle x^N - \lambda\rangle$ (cf. [11] Propositions 2.2).

Let $\mathbb{F}_q$ be a finite field of cardinality q, where q is power of a prime, and denote $R = \mathbb{F}_q[u]/\langle u^e\rangle = \mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{e-1}\mathbb{F}_q$ $(u^e = 0)$ where $e \geq 2$. Then R is a finite chain ring. When $e = 2$, there was a lot of literatures on linear codes, cyclic codes and constacyclic codes of length N over rings $\mathbb{F}_{p^m}[u]/\langle u^2\rangle = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ for various prime p and positive integers m and N. See [2,4,5,10–13,15] and [19], for example.

When $e \geq 3$, for the case of $p = 2$ and $m = 1$ Abualrub and Siap [1] studied cyclic codes over the ring $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$ for arbitrary length N, then Al-Ashker and Hamoudeh [3] extended some of the results in [1], and studied

* Corresponding author.
E-mail addresses: yuancao@sdut.edu.cn (Y. Cao), ylcao@sdut.edu.cn (Y. Cao), 770619077@qq.com (F. Ma).

http://dx.doi.org/10.1016/j.disc.2017.08.002
0012-365X/

cyclic codes of an arbitrary length over the ring $\mathbb{Z}_2+u\mathbb{Z}_2+u^2\mathbb{Z}_2+\cdots+u^{k-1}\mathbb{Z}_2$ ($u^k=0$) for the rank and minimal spanning of this family of codes. For the case of $m=1$, Han et al. [14] studied cyclic codes over $R=\mathbb{F}_p+u\mathbb{F}_p+\cdots+u^{k-1}\mathbb{F}_p$ with length p^sn using discrete Fourier transform. Singh et al. [20] studied cyclic code over the ring $\mathbb{Z}_p[u]/\langle u^k\rangle=\mathbb{Z}_p+u\mathbb{Z}_p+u^2\mathbb{Z}_p+\cdots+u^{k-1}\mathbb{Z}_p$ for any prime integer p and positive integer N. A set of generators, the rank and the Hamming distance of these codes were investigated. Kai et al. [16] investigated $(1+\lambda u)$-constacyclic codes of arbitrary length over $\mathbb{F}_p[u]/\langle u^m\rangle$, where $\lambda\in\mathbb{F}_p^\times$. Cao [6] generalized these results to $(1+w\gamma)$-constacyclic codes of arbitrary length over an arbitrary finite chain ring R, where w is a unit of R and γ generates the unique maximal ideal of R. Sobhani et al. [22] showed that the Gray image of a $(1-u^{e-1})$-constacyclic code of length n is a length $p^{m(e-1)}n$ quasi-cyclic code of index $p^{m(e-1)-1}$.

Sobhani [21] determined the structure of $(\delta+\alpha u^2)$-constacyclic codes of length p^k over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$ completely, where $\delta,\alpha\in\mathbb{F}_{p^m}^\times$, and proposed some open problems and further research in this area: characterize $(\delta+\alpha u^2)$- constacyclic codes of length p^k over the finite chain ring $\mathbb{F}_{p^m}[u]/\langle u^e\rangle$ for $e\geq 4$. As a natural extension, the following problem is more worthy of study: characterize $(\delta+\alpha u^2)$- constacyclic codes of arbitrary length N over the finite chain ring $\mathbb{F}_{p^m}[u]/\langle u^e\rangle$ for $e\geq 4$, where $N=p^kn$, k is a positive integer and $n\in\mathbb{Z}^+$ satisfying $\gcd(p,n)=1$.

Recently, using the theory of modules over finite chain rings Cao et al. [7] provided a new way different from the methods used in [8], [16], [20] and [21] to determine the algebraic structures of $(\delta+\alpha u^2)$-constacyclic codes and their dual codes over the ring $\mathbb{F}_{3^m}[u]/\langle u^4\rangle$ of length $3n$ where n is an arbitrary positive integer satisfying $\gcd(3,n)=1$.

In this paper, using the main idea of [7], we study the latter problem for the special case of $p=2$, $k=1$, n is an odd positive integer and $e=4$. But the key results and techniques in [7] Lemma 3.5 and its proof cannot be applied to this situation directly. We have to solve this problem by developing new methods and techniques (see Lemma 3.5, Theorem 2.2 and its proof in Appendix of this paper).

From now on, we adopt the following notations.

Notation 1.1. Let $\delta,\alpha\in\mathbb{F}_{2^m}^\times$ and n be an odd positive integer. We denote

- $R=\mathbb{F}_{2^m}[u]/\langle u^4\rangle=\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}+u^2\mathbb{F}_{2^m}+u^3\mathbb{F}_{2^m}$ ($u^4=0$), which is a finite chain ring of 2^{4m} elements.
- $\mathcal{A}=\mathbb{F}_{2^m}[x]/\langle(x^{2n}-\delta)^2\rangle$, which is a principal ideal ring and $|\mathcal{A}|=2^{4mn}$.
- $\mathcal{A}[u]/\langle u^2-\alpha^{-1}(x^{2n}-\delta)\rangle=\mathcal{A}+u\mathcal{A}$ ($u^2=\alpha^{-1}(x^{2n}-\delta)$), where $\mathcal{A}+u\mathcal{A}=\{\xi_0+u\xi_1\mid\xi_0,\xi_1\in\mathcal{A}\}$ with operations defined by
  - $\diamond\ (\xi_0+u\xi_1)+(\eta_0+u\eta_1)=(\xi_0+\eta_0)+u(\xi_1+\eta_1)$,
  - $\diamond\ (\xi_0+u\xi_1)(\eta_0+u\eta_1)=\xi_0\eta_0+\alpha^{-1}(x^{2n}-\delta)\xi_1\eta_1+u(\xi_0\eta_1+\xi_1\eta_0)$,

for all $\xi_0,\xi_1,\eta_0,\eta_1\in\mathcal{A}$.

The present paper is organized as follows. In Section 2, we sketch the basic theory of finite commutative chain rings and linear codes over finite commutative chain rings. In Section 3, we provide an explicit representation for each $(\delta+\alpha u^2)$-constacylic code over R of length $2n$ and give a formula to count the number of codewords in each code. As a corollary, we obtain a formula to count the number of all such codes. Finally, we list all 258741 distinct $(1+u^2)$-constacylic codes of length 14 over $\mathbb{F}_2[u]/\langle u^4\rangle$ in Section 4.

2. Preliminaries

In this section, we sketch the basic theory of finite commutative chain rings and linear codes over finite commutative chain rings needed in this paper.

Now, let $\mathcal{K}$ be an arbitrary commutative finite chain ring with $1\neq 0$, π be a fixed generator of the maximal ideal of $\mathcal{K}$ with nilpotency index 4, and F the residue field of $\mathcal{K}$ modulo its ideal $\langle\pi\rangle=\pi\mathcal{K}$, i.e. $F=\mathcal{K}/\langle\pi\rangle$. It is known that $|F|$ is a power of a prime number, and there is a unit ξ of $\mathcal{K}$ with multiplicative order $|F|-1$ such that every element $a\in\mathcal{K}$ has a unique *π-adic expansion*: $a_0+\pi a_1+\pi^2a_2+\pi^3a_3$, $a_0,a_1,a_2,a_3\in\mathcal{T}$, where $\mathcal{T}=\{0,1,\xi,\ldots,\xi^{|F|-2}\}$ is the Teichmüller set of $\mathcal{K}$ (cf. Nechaev [17]). Hence $|\mathcal{K}|=|F|^4$. If $a\neq 0$, the *π-degree* of a is defined as the least index $j\in\{0,1,2,3\}$ for which $a_j\neq 0$ and written for $\|a\|_\pi=j$. If $a=0$ we write $\|a\|_\pi=4$. It is clear that $a\in\mathcal{K}^\times$ if and only if $a_0\neq 0$, i.e. $\|a\|_\pi=0$. Hence $|\mathcal{K}^\times|=(|F|-1)|F|^3$. Moreover, we have $\mathcal{K}/\langle\pi^0\rangle=\{0\}$ and $\mathcal{K}/\langle\pi^l\rangle=\{\sum_{i=0}^{l-1}\pi^ia_i\mid a_0,\ldots,a_{l-1}\in\mathcal{T}\}$ with $|\mathcal{K}/\langle\pi^l\rangle|=|F|^l$, $1\leq l\leq 3$.

Let L be a positive integer and $\mathcal{K}^L=\{(\alpha_1,\ldots,\alpha_L)\mid\alpha_1,\ldots,\alpha_L\in\mathcal{K}\}$ the free $\mathcal{K}$-module under componentwise addition and scalar multiplication with elements from $\mathcal{K}$. Then $\mathcal{K}$-submodules of $\mathcal{K}^L$ are linear codes of length L over $\mathcal{K}$. Let C be a linear code over $\mathcal{K}$ of length L. By [18] Definition 3.1, a matrix G is called a *generator matrix* for C if the rows of G span C and none of them can be written as a $\mathcal{K}$-linear combination of the other rows of G. Furthermore, a generator matrix G is said to be *in standard form* if there is a suitable permutation matrix U of size $L\times L$ such that

$$G=\begin{pmatrix}\pi^0I_{k_0} & M_{0,1} & M_{0,2} & M_{0,3} & M_{0,4}\\ 0 & \pi I_{k_1} & \pi M_{1,2} & \pi M_{1,3} & \pi M_{1,4}\\ 0 & 0 & \pi^2I_{k_2} & \pi^2M_{2,3} & \pi^2M_{2,4}\\ 0 & 0 & 0 & \pi^3I_{k_3} & \pi^3M_{3,4}\end{pmatrix}U \tag{1}$$

where the columns are grouped into blocks of sizes k_0,k_1,k_2,k_3,k with $k_i\geq 0$ and $k=L-(k_0+k_1+k_2+k_3)$. Of course, if $k_i=0$, the matrices $\pi^iI_{k_i}$ and $\pi^iM_{i,j}$ ($i<j$) are suppressed in G. From [18] Proposition 3.2 and Theorem 3.5, we deduce the following.

Please cite this article in press as: Y. Cao, et al., Complete classification of $(\delta+\alpha u^2)$-constacyclic codes over $\mathbb{F}_{2^m}[u]/\langle u^4\rangle$ of oddly even length, Discrete Mathematics (2017), http://dx.doi.org/10.1016/j.disc.2017.08.002.