Vol. 38 (2018)
No. 6

数 学 杂 志
J. of Math. (PRC)

CONSTACYCLIC CODES OF LENGTH 2^s OVER $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$

LIU Xiu-sheng, XU Xiao-fang, HU Peng
(*School of Mathematics and Physics, Hubei Polytechnic University, Huangshi 435003, China*)

Abstract: In this paper, we investigate all constacyclic codes of length 2^s over $R = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, where R is a local ring, but it is not a chain ring. First, by means of the Euclidean algorithm for polynomials over finite commutative local rings, we classify all cyclic and $(1+uv)$-constacyclic codes of length 2^s over R, and obtain their structure in each of those cyclic and $(1+uv)$-constacyclic codes. Second, by using $(x-1)^{2^s} = u$, we address the $(1+u)$-constacyclic codes of length 2^s over R, and get their classification and structure. Finally, by using similar discussion of $(1+u)$-constacyclic codes, we obtain the classification and the structure of $(1+v), (1+u+uv), (1+v+uv), (1+u+v), (1+u+v+uv)$-constacyclic codes of length 2^s over R.

Keywords: constacyclic codes; cyclic codes; local ring; repeated-root constacyclic codes
2010 MR Subject Classification: 94B05; 94B15
Document code: A **Article ID:** 0255-7797(2018)06-0975-15

1 Introduction

Codes over the ring $R = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ were introduced in [1]. The ring R is a characteristic 2 ring of size 16. It turns out to be a commutative, non-chain, and a local Frobenius ring constructed subject to $u^2 = v^2 = 0, uv = vu$. It can be viewed as a natural extension of the ring $\mathbb{F}_2+u\mathbb{F}_2$, which was studied quite extensively in [2] and [3]. In particalar, the ring $\mathbb{F}_2 + u\mathbb{F}_2$ is interesting because it shares some good properties of both $\mathbb{Z}_4$ and Galois field $\mathbb{F}_4$. $(1+u)$-constacyclic codes over $\mathbb{F}_2+u\mathbb{F}_2$ of odd length were first introduced by Qian et al. in [4], where it proved that the Gray image of a linear $(1+u)$-constacyclic code over $\mathbb{F}_2 + u\mathbb{F}_2$ of odd length is a binary distance invariant linear cyclic code. Recently, Yildiz and Karadeniz in [5, 6] studied constacyclic codes of odd length over R. They found some good binary codes as the Gray images of these cyclic codes. The authors in [7] considered the more general ring $\frac{\mathbb{F}_2[u_1,u_2,\ldots,u_k]}{\langle u_i^2,u_j^2,u_iu_j-u_ju_i\rangle}$, and studied the general properties of cyclic codes over these rings and characterized the nontrivial one-generator cyclic codes. Kemat et al. in [8] extended these studies to cyclic codes over the ring $\frac{\mathbb{Z}_p[u,v]}{\langle u^2,v^2,uv-vu\rangle} = \mathbb{Z}_p + u\mathbb{Z}_p + v\mathbb{Z}_p + uv\mathbb{Z}_p$, where $u^2 = 0, v^2 = 0, uv = vu$ and p is a prime number.

* **Received date:** 2017-02-28 **Accepted date:** 2017-10-18
Foundation item: Supported by Scientific Research Foundation of Hubei Provincial Education Department of China (D20144401; Q20174503) and the National Science Foundation of Hubei Polytechnic University of China (12xjz14A; 17xjz03A).

Biography: Liu Xiusheng (1960–), male, born at Daye, Hubei, professor, major in groups and algebraic coding, multiple linear algebra.

In this paper, we study repeated-root λ-constacyclic codes of length 2^s over R, where λ is unit of R. Although repeated-root λ-constacyclic codes over finite ring $\tilde{R}$ are known to be asymptotically bad, they are optimal in a few cases. They motivated the researchers to further study (see [9–15]).

The paper is organized as follows. In Section 2, we recall some notations and properties about constacyclic codes over finite local rings. In Section 3, we address the cyclic and $(1+uv)$-constacyclic codes of length 2^s over R. We classify all such cyclic and $(1+uv)$-constacyclic codes by categorizing the ideals of the local ring $R_1=\frac{R[x]}{\langle x^{2^s}-1\rangle}$ and $R_2=\frac{R[x]}{\langle x^{2^s}-(1+uv)\rangle}$ into 13 types. In the last section, we study the $(1+u)$-constacyclic codes of length 2^s over R. These $(1+u)$-constacyclic codes are the ideals of the ring $R_3=\frac{R[x]}{\langle x^{2^s}-(1+u)\rangle}$, which is a local ring with the maximal ideal $\langle x-1, v\rangle$. We classify all $(1+u)$-constacyclic codes by categorizing the ideals of the local ring R_3 into 4 type, and provide a detailed structure of ideal in each type. By using similar discussion of $(1+u)$-constacyclic codes, we obtain the classification and the structure of $(1+v), (1+u+uv), (1+v+uv), (1+u+v), (1+u+v+uv)$-constacyclic codes of length 2^s over R.

2 Basics

A code of length n over R is a nonempty subset of R^n, and a linear code C of length n over R is an R-submodule of R^n. If λ is a unit in R, a linear code C is called as λ-constacyclic if $(\lambda a_{n-1}, a_0, \cdots, a_{n-2})\in C$ for every $(a_0, a_1, \cdots, a_{n-1})\in C$. It is well known that a λ-constacyclic code of length n over R can be identified as an ideal in the residue ring $\frac{R[x]}{\langle x^n-\lambda\rangle}$ via the R-module isomorphism $\varphi: R^n\to\frac{R[x]}{\langle x^n-\lambda\rangle}$ given by

$$(a_0, a_1, \cdots, a_{n-1})\mapsto a_0+a_1x+\cdots+a_{n-1}x^{n-1}(\mathrm{mod}(x^n-\lambda)).$$

If $\lambda=1$, λ-constacyclic codes are just cyclic codes and if $\lambda=-1$, λ-constacyclic codes are known as negacyclic codes. A polynomial is said to be regular if it is not a zero divisor. The following version of the Euclidean algorithm holds true for polynomials over finite commutative local rings.

Proposition 2.1 (see [16, Example, III.6]) Let $\tilde{R}$ be a finite commutative local ring, and f, g be nonzero polynomials in $\tilde{R}[x]$. If g is regular, then there exist polynomials $q(x), r(x)\in\tilde{R}[x]$ such that $f(x)=q(x)g(x)+r(x)$ and $r(x)=0$ or $\deg(r(x))<\deg(g(x))$.

3 Cyclic and $(1+uv)$-Constacyclic Codes of Length 2^s Over R

Cyclic codes of length 2^s over R are ideals of the residue ring $R_1=\frac{R[x]}{\langle x^{2^s}-1\rangle}$, and the $(1+uv)$-constacyclic codes of length 2^s over R are ideals of the residue ring $R_2=\frac{R[x]}{\langle x^{2^s}-(1+uv)\rangle}$. It is easy to prove the following three lemmas.

Lemma 3.1 The following hold true in R_1:

(i) For any nonegative integer t, $(x-1)^{2^t}=x^{2^t}-1$.

(ii) $x-1$ is nilpotent with the nilpotency index 2^s.

Lemma 3.2 The following hold true in R_2.

(i) For any nonnegative integer t, $(x-1)^{2^t} = x^{2^t} - 1$. In particular, $(x-1)^{2^s} = uv$.

(ii) $x-1$ is nilpotent with the nilpotency index 2^{s+1}.

Lemma 3.3 Let $f(x) \in R_1$ or R_2. Then $f(x)$ can be uniquely expressed as

$$\begin{aligned} f(x) =& \sum_{j=0}^{2^s-1} a_{0j}(x-1)^j + u\sum_{j=0}^{2^s-1} a_{1j}(x-1)^j + v\sum_{j=0}^{2^s-1} a_{2j}(x-1)^j + uv\sum_{j=0}^{2^s-1} a_{3j}(x-1)^j \\ =& a_{00} + (x-1)\sum_{j=1}^{2^s-1} a_{0j}(x-1)^{j-1} + u\sum_{j=0}^{2^s-1} a_{1j}(x-1)^j + v\sum_{j=0}^{2^s-1} a_{2j}(x-1)^j \\ &+ uv\sum_{j=0}^{2^s-1} a_{3j}(x-1)^j, \end{aligned}$$

where $a_{0j}, a_{1j}, a_{2j}, a_{3j} \in \mathbb{F}_2$. Furthermore, $f(x)$ is invertible if and only if $a_{00} \neq 0$.

Proposition 3.4 The ring R_1 or R_2 is a local ring with the maximal ideal $\langle u, v, x-1\rangle$, but it is not a chain ring.

Proof By Lemma 3.3, the ideal $\langle u, v, x-1\rangle$ is the set of all non-invertible elements of R_1 or R_2. Hence R_1 or R_2 is a local ring with maximal ideal $\langle u, v, x-1\rangle$. Suppose $u \in \langle x-1\rangle$. Then there must exist $f_1(x)$ and $f_2(x) \in R[x]$ such that $u = (x-1)f_1(x) + (x^{2^s}-1)f_2(x)$ or $u = (x-1)f_1(x) + [x^{2^s} - (1+uv)]f_2(x)$. However, this is impossible because plugging in $x = 1$ yields $u = 0$ or $u = uv$. Hence, $u \notin \langle x-1\rangle$. Similarly, $v \notin \langle x-1\rangle$. Next we suppose $x-1 \in \langle u\rangle$ or $\langle v\rangle$. Then $(x-1)^2 = 0$, which is a contradiction with $s > 1$. Therefore, the maximal ideal $\langle u, v, x-1\rangle$ of R_1 or R_2 is not principal. It means R_1 or R_2 is not a chain ring.

Theorem 3.5 All of cyclic codes of length 2^s over R, i.e., ideals of the ring R_1 are the following:

- Type 1: $\langle 0\rangle, \langle 1\rangle$;
- Type 2: $I = \langle uv(x-1)^\sigma\rangle$, where $0 \le \sigma \le 2^s - 1$;
- Type 3: $I = \langle v(x-1)^t + uv\sum_{j=0}^{t} m_{1j}(x-1)^j\rangle$, where $0 \le t \le 2^s - 1$;
- Type 4: $I = \langle v(x-1)^t + uv\sum_{j=0}^{t-1} m_{1j}(x-1)^j, uv(x-1)^z\rangle$, where $1 \le t \le 2^s - 1, z < t$;
- Type 5: $I = \langle u(x-1)^l + v\sum_{j=0}^{2^s-1} h_{2j}(x-1)^j + uv\sum_{j=0}^{l} h_{3j}(x-1)^j\rangle$, where $0 \le l \le 2^s - 1$;
- Type 6: $I = \langle u(x-1)^l + v\sum_{j=0}^{2^s-1} h_{2j}(x-1)^j + uv\sum_{j=0}^{l-1} h_{3j}(x-1)^j, uv(x-1)^t\rangle$, where $1 \le l \le 2^s - 1, t < l$;
- Type 7: $I = \langle u(x-1)^l + v\sum_{j=0}^{2^s-1} h_{2j}(x-1)^j + uv\sum_{j=0}^{l} h_{3j}(x-1)^j, v(x-1)^z + uv\sum_{j=0}^{z} b_{3j}(x-1)^j\rangle$, where $0 \le l \le 2^s - 1, 0 \le z \le 2^s - 1$;

• Type 8: $I=\langle u(x-1)^l+v\sum\limits_{j=0}^{z-1}h_{2j}(x-1)^j+uv\sum\limits_{j=0}^{z-1}h_{3j}(x-1)^j, v(x-1)^z+uv\sum\limits_{j=0}^{z-1}b_{3j}(x-1)^j, uv(x-1)^w\rangle$, where $1\le l\le 2^s-1, 1\le z\le 2^s-1$, and $w<\min\{l,z\}$;

• Type 9: $I=\langle (x-1)^i+u\sum\limits_{j=0}^{i}a_{1j}(x-1)^j+v\sum\limits_{j=0}^{i}a_{2j}(x-1)^j+uv\sum\limits_{j=0}^{i}a_{3j}(x-1)^j\rangle$, where $0\le i\le 2^s-1$;

• Type 10: $I=\langle (x-1)^i+u\sum\limits_{j=0}^{i}a_{1j}(x-1)^j+v\sum\limits_{j=0}^{i}a_{2j}(x-1)^j+uv\sum\limits_{j=0}^{t}a_{3j}(x-1)^j, u(x-1)^l+v\sum\limits_{j=0}^{i}h_{2j}(x-1)^j+uv\sum\limits_{j=0}^{t}h_{3j}(x-1)^j\rangle$, where $0\le i\le 2^s-1, 0\le l\le 2^s-1$ and $t\le\min\{i,l\}$;

• Type 11: $I=\langle (x-1)^i+u\sum\limits_{j=0}^{i}a_{1j}(x)^j+v\sum\limits_{j=0}^{i}a_{2j}(x-1)^j+uv\sum\limits_{j=0}^{t}a_{3j}(x-1)^j, u(x-1)^l+v\sum\limits_{j=0}^{i}h_{2j}(x-1)^j+uv\sum\limits_{j=0}^{t}h_{3j}(x-1)^j, uv(x-1)^t\rangle$, where $0\le i\le 2^s-1, 0\le l\le 2^s-1$ and $t\le\min\{i,l\}$;

• Type 12: $I=\langle (x-1)^i+u\sum\limits_{j=0}^{i}a_{1j}(x-1)^j+v\sum\limits_{j=0}^{i}a_{2j}(x-1)^j+uv\sum\limits_{j=0}^{t}a_{3j}(x-1)^j, u(x-1)^l+v\sum\limits_{j=0}^{i}h_{2j}(x-1)^j+uv\sum\limits_{j=0}^{t}h_{3j}(x-1)^j, v(x-1)^z+uv\sum\limits_{j=0}^{t}b_{3j}(x-1)^j\rangle$, where $0\le i\le 2^s-1, 0\le l\le 2^s-1, 0\le z\le 2^s-1$ and $t\le\min\{i,l,z\}$;

• Type 13: $I=\langle (x-1)^i+u\sum\limits_{j=0}^{i}a_{1j}(x-1)^j+v\sum\limits_{j=0}^{i}a_{2j}(x-1)^j+uv\sum\limits_{j=0}^{w}a_{3j}(x-1)^j, u(x-1)^l+v\sum\limits_{j=0}^{i}h_{2j}(x-1)^j+uv\sum\limits_{j=0}^{w}h_{3j}(x-1)^j, v(x-1)^z+uv\sum\limits_{j=0}^{w}b_{3j}(x-1)^j, uv(x-1)^w\rangle$, where $0\le i\le 2^s-1, 0\le l\le 2^s-1, 0\le z\le 2^s-1$ and $w\le\min\{i,l,z\}$.

Proof Ideals of Type 1 are the trivial ideals. Consider an arbitrary nontrivial ideals of R_1.

Case 1 $I\subseteq\langle v\rangle$. Any element of I must have the form $v\sum\limits_{j=0}^{2^s-1}a_{0j}(x-1)^j+uv\sum\limits_{j=0}^{2^s-1}a_{1j}(x-1)^j$, where $a_{0j},a_{1j}\in\mathbb{F}_2$.

Let

$$M=\{v\sum_{j=0}^{2^s-1}a_{0j}(x-1)^j+uv\sum_{j=0}^{2^s-1}a_{1j}(x-1)^j\in I|\sum_{j=0}^{2^s-1}a_{0j}(x-1)^j\neq 0\}$$

and $N=\{uv\sum\limits_{j=0}^{2^s-1}a_{1j}(x-1)^j\in I\}$. Suppose $M=\Phi$. Then there exists the smallest integer σ such that $n(x)=uv(x-1)^\sigma n_1(x)$ for $n(x)\in N$, where $n_1(x)\in R_1$. It is easy to verify that $uv(x-1)^\sigma\in N$. Hence $I=\langle uv(x-1)^\sigma\rangle$, and I is in Type 2.

Suppose $M\neq\Phi$. Setting $\alpha=\min\{\deg(m(x))|m(x)\in M\}$. Then there is an element $m_1(x)=v\sum m_{0j}(x-1)^j+uv\sum m_{1j}(x-1)^j\in M$ with $\deg(m_1(x))=\alpha$. It has the smallest

t such that $m_{0t} \neq 0$. Hence we have

$$m_1(x) = v(x-1)^t[m_{0t} + \sum_{j=t+1}^{2^s-1} m_{0j}(x-1)^{j-t}] + uv \sum_{j=0}^{2^s-1} m_{1j}(x-1)^j \in I.$$

Let

$$m_2(x) = (x-1)^t[m_{0t} + \sum_{j=t+1}^{2^s-1} m_{0j}(x-1)^{j-t}] + u \sum_{j=0}^{2^s-1} m_{1j}(x-1)^j.$$

Then $m_1(t) = vm_2(t)$.

Now we have two subcases.

Case 1.1 $N \subseteq \langle m_1(x) \rangle$. For any $f(x) \in M$, obviously, $f(x)$ can be written as $f(x) = vf_1(x)$, where $f_1(x) = \sum_{j=0}^{2^s-1} a_{0j}(x-1)^j + u \sum_{j=0}^{2^s-1} a_{1j}(x-1)^j$. By Proposition 2.1, $f_1(x)$ can be written as $f_1(x) = q(x)m_2(x) + r(x)$, where $q(x), r(x) \in R_1$ and $r(x) = 0$ or $\deg(r(x)) < \deg(m_2(x)) = \deg(m_1(x))$. It implies that $f(x) = q(x)m_1(x) + vr(x)$. Suppose $vr(x) \notin N$. Then $vr(x) \neq 0$. Hence $vr(x) = f(x) - q(x)m_1(x) \in M$, which contradicts with the assumption of $m_1(x)$. Thus $vr(x) \in N$. Therefore, $I = \langle v(x-1)^t + uv \sum_{j=0}^{t} m_{1j}(x-1)^j \rangle$, $0 \leq t \leq 2^s - 1$. Thus I is in Type 3.

Case 1.2 $N \nsubseteq \langle m_1(x) \rangle$. Then there exists the smallest integer z such that $n(x) = uv(x-1)^z n_1(x)$ for every $n(x) \in N$, where $n_1(x) \in R_1$. It is easy to verify that $uv(x-1)^z \in N$, but $uv(x-1)^z \notin \langle m_1(x) \rangle$, and $z < t$. Hence

$$I = \langle v(x-1)^t + uv \sum_{j=0}^{t-1} m_{1j}(x-1)^j, uv(x-1)^z \rangle, 1 \leq t \leq 2^s - 1, 0 \leq z < t.$$

Therefore, I is in Type 4.

Case 2 $\langle v \rangle \subsetneq I \subseteq \langle u, v \rangle$. Any element of I must have the form

$$u \sum_{j=0}^{2^s-1} a_{1j}(x-1)^j + v \sum_{j=0}^{2^s-1} a_{2j}(x-1)^j + uv \sum_{j=0}^{2^s-1} a_{3j}(x-1)^j,$$

and there exists an element $u \sum_{j=0}^{2^s-1} b_{1j}(x-1)^j + v \sum_{j=0}^{2^s-1} b_{2j}(x-1)^j + uv \sum_{j=0}^{2^s-1} b_{3j}(x-1)^j$ in I such that $\sum_{j=0}^{2^s-1} b_{1j}(x-1)^j \neq 0$.

Let

$$\begin{aligned} M &= \{u \sum_{j=0}^{2^s-1} a_{1j}(x-1)^j + v \sum_{j=0}^{2^s-1} a_{2j}(x-1)^j + uv \sum_{j=0}^{2^s-1} a_{3j}(x-1)^j \in I \\ &\quad \mid \sum_{j=0}^{2^s-1} a_{1j}(x-1)^j \neq 0, a_{1j}, a_{2j}, a_{3j} \in \mathbb{F}_2\}, \end{aligned}$$

and let $N=\{v\sum\limits_{j=0}^{2^s-1}a_{2j}(x-1)^j+uv\sum\limits_{j=0}^{2^s-1}a_{3j}(x-1)^j\in I\mid a_{2j},a_{3j}\in\mathbb{F}_2\}$. Then there is an element $\tilde{h}_1(x)=u\sum\limits_{j=0}^{2^s-1}\tilde{h}_{1j}(x-1)^j+v\sum\limits_{j=0}^{2^s-1}\tilde{h}_{2j}(x-1)^j+uv\sum\limits_{j=0}^{2^s-1}\tilde{h}_{3j}(x-1)^j$ in M that has the smallest l such that $\tilde{h}_{1l}\neq 0$. Hence we have

$$\tilde{h}_1(x)=u(x-1)^l[\tilde{h}_{1l}+\sum_{j=l+1}^{2^s-1}\tilde{h}_{1j}(x-1)^{j-l}]+v\sum_{j=0}^{2^s-1}\tilde{h}_{2j}(x-1)^j+uv\sum_{j=0}^{2^s-1}\tilde{h}_{3j}(x-1)^j\in I.$$

Since $\tilde{h}_{1l}\neq 0$, $\tilde{h}_{1l}+\sum\limits_{j=l+1}^{2^s-1}\tilde{h}_{1j}(x-1)^{j-l}$ is invertible, and

$$h_2(x)=\tilde{h}_1(x)[\tilde{h}_{1l}+\sum_{j=l+1}^{2^s-1}\tilde{h}_{1j}(x-1)^{j-l}]^{-1}=u(x-1)^l+v\sum_{j=0}^{2^s-1}h_{2j}(x-1)^j+uv\sum_{j=0}^{2^s-1}h_{3j}(x-1)^j\in I.$$

Because $vh_2(x)=uv(x-1)^l\in I$, we have

$$h_1(x)=u(x-1)^l+v\sum_{j=0}^{2^s-1}h_{2j}(x-1)^j+uv\sum_{j=0}^{l-1}h_{3j}(x-1)^j\in I.$$

For any $m(x)\in M$, obviously, $m(x)$ can be written as

$$m(x)=u(x-1)^l\sum_{j=l}^{2^s-1}a_{1j}(x-1)^{j-l}+v\sum_{j=0}^{2^s-1}a_{2j}(x-1)^j+uv\sum_{j=0}^{2^s-1}a_{3j}(x-1)^j,$$

where $a_{1j},a_{2j},a_{3j}\in\mathbb{F}_2$. Thus we can assume that

$$m(x)-h_1(x)\sum_{j=l}^{2^s-1}a_{1j}(x-1)^{j-l}=v\sum_{j=0}^{2^s-1}a_{2j}(x-1)^j+uv\sum_{j=0}^{2^s-1}a_{3j}(x-1)^j\in N.$$

Now we have two subcases.

Case 2.1 $N=\{0\}$. Then $I=\langle u(x-1)^l+v\sum\limits_{j=0}^{2^s-1}h_{2j}(x-1)^j+uv\sum\limits_{j=0}^{l}h_{3j}(x-1)^j\rangle$, where $0\leq l\leq 2^s-1$. Thus, I is in Type 5.

Case 2.2 $N\neq\{0\}$. We denote

$$N_1=\{v\sum_{j=0}^{2^s-1}a_{2j}(x-1)^j+uv\sum_{j=0}^{2^s-1}a_{3j}(x-1)^j\in N\mid\sum_{j=0}^{2^s-1}a_{2j}(x-1)^j\neq 0,a_{2j},a_{3j}\in\mathbb{F}_2\},$$

and $N_2=\{uv\sum\limits_{j=0}^{2^s-1}a_{3j}(x-1)^j\in N\mid a_{3j}\in\mathbb{F}_2\}$ in the following.

Again we have two subcases.

Case 2.2.1 $N_1 = \Phi$. Then $N_2 \neq \{0\}$. Therefore, there exists the smallest integer t such that $n_2(x) = uv(x-1)^t q(x)$ for every $n_2(x) \in N_2 = N$, where $q(x) \in R_1$. It is easy to verify that $uv(x-1)^t \in N_2 = N$. Hence,

$$I = \langle u(x-1)^l + v\sum_{j=0}^{2^s-1} h_{2j}(x-1)^j + uv\sum_{j=0}^{l-1} h_{3j}(x-1)^j, uv(x-1)^t\rangle.$$

Suppose that $t \geq l$. Then

$$uv(x-1)^t = v(x-1)^{t-l}[u(x-1)^l + v\sum_{j=0}^{2^s-1} h_{2j}(x-1)^j + uv\sum_{j=0}^{l-1} h_{3j}(x-1)^j].$$

Thus, $I = \langle u(x-1)^l + v\sum\limits_{j=0}^{2^s-1} h_{2j}(x-1)^j + uv\sum\limits_{j=0}^{l-1} h_{3j}(x-1)^j\rangle$, it is in Type 5. We can assume without loss of generality that $t < l$, and thus

$$I = \langle u(x-1)^l + v\sum_{j=0}^{2^s-1} h_{2j}(x-1)^j + uv\sum_{j=0}^{l-1} h_{3j}(x-1)^j, uv(x-1)^t\rangle,$$

where $1 \leq l \leq 2^s - 1$. Therefore, I is in Type 6.

Case 2.2.2 $N_1 \neq \Phi$. Then there is an element

$$\tilde{a}_1(x) = v\sum_{j=0}^{2^s-1} \tilde{a}_{2j}(x-1)^j + uv\sum_{j=0}^{2^s-1} \tilde{a}_{3j}(x-1)^j$$

in N_1 that has smallest z such that $\tilde{a}_{2z} \neq 0$. Hence we have

$$\tilde{b}_1(x) = v(x-1)^z[\tilde{b}_{2z} + \sum_{j=z+1}^{2^s-1} \tilde{b}_{2j}(x-1)^{j-z}] + uv\sum_{j=0}^{2^s-1} \tilde{b}_{3j}(x-1)^j \in N_1.$$

Thus $b_1(x) = \tilde{b}_1(x)[\tilde{b}_{2z} + \sum\limits_{j=z+1}^{2^s-1} \tilde{b}_{2j}(x-1)^{j-z}]^{-1} \in I$ and $b_1(x)$ can be expressed as $b_1(x) = v(x-1)^z + uv\sum\limits_{j=0}^{z-1} b_{3j}(x-1)^j$.

For any $n_1(x) \in N_1$, obviously, $n_1(x)$ can be written as

$$n_1(x) = v(x-1)^z\sum_{j=z}^{2^s-1} a_{2j}(x-1)^{j-z} + uv\sum_{j=0}^{2^s-1} a_{3j}(x-1)^j,$$

where $a_{2j}, a_{3j} \in \mathbb{F}_2$. Thus, we can assume that

$$n_1(x) - b_1(x)\sum_{j=z}^{2^s-1} a_{2j}(x-1)^{j-z} = uv\sum_{j=0}^{2^s-1} a_{3j}(x-1)^j \in I.$$

If $N_2 = \{0\}$, then

$$I = \langle u(x-1)^l + v\sum_{j=0}^{2^s-1} h_{2j}(x-1)^j + uv\sum_{j=0}^{l} h_{3j}(x-1)^j, v(x-1)^z + uv\sum_{j=0}^{l} b_{3j}(x-1)^j\rangle,$$

where $0 \le l \le 2^s-1, 0 \le z \le 2^s-1$. Thus, I is in Type 7.

If $N_2 \ne \{0\}$. Then there exists the smallest integer w such that $n_2(x) = uv(x-1)^w q(x)$ for every $n_2(x) \in N_2$, where $q(x) \in R_1$. It is easy to verify that $uv(x-1)^w \in I$. Hence,

$$I = \langle u(x-1)^l + v\sum_{j=0}^{z-1} h_{2j}(x-1)^j + uv\sum_{j=0}^{z-1} h_{3j}(x-1)^j, v(x-1)^z + uv\sum_{j=0}^{z-1} b_{3j}(x-1)^j, uv(x-1)^w\rangle,$$

where $1 \le l \le 2^s-1, 1 \le z \le 2^s-1$, and $w < \min\{l, z\}$. Thus, I is in Type 8.

Case 3 $I \nsubseteq \langle u, v\rangle$. Let $I_{u,v} = \{f(x) \in \frac{\mathbb{F}_2[x]}{\langle x^{2^s}-1\rangle} \mid$ there are $g(x), h(x), m(x) \in \mathbb{F}_2[x]/\langle x^{2^s}-1\rangle$ such that $f(x) + ug(x) + vh(x) + uvm(x) \in R_1\}$. Then $I_{u,v}$ is a nonzero ideal of the ring $\frac{\mathbb{F}_2[x]}{\langle x^{2^s}-1\rangle}$. It is a chain ring with ideals $\langle (x-1)^j\rangle$, where $0 \le j \le 2^s$. Hence there is an integer $i \in \{0, 1, \cdots, 2^s-1\}$ such that $I_{u,v} = \langle (x-1)^i\rangle \subseteq \frac{\mathbb{F}_2[x]}{\langle x^{2^s}-1\rangle}$. Therefore, there are three elements

$$c_i(x) = \sum_{j=0}^{2^s-1} c_{0j}^{(i)}(x-1)^j + u\sum_{j=0}^{2^s-1} c_{1j}^{(i)}(x-1)^j + v\sum_{j=0}^{2^s-1} c_{2j}^{(i)}(x-1)^j + uv\sum_{j=0}^{2^s-1} c_{3j}^{(i)}(x-1)^j \in R_1$$

for $i = 1, 2, 3$ such that $(x-1)^i + uc_1(x) + vc_2(x) + uvc_3(x) \in I$, where $c_{0j}^{(i)}, c_{1j}^{(i)}, c_{2j}^{(i)}, c_{3j}^{(i)} \in \mathbb{F}_2$. Because

$$\begin{aligned}
&(x-1)^i + uc_1(x) + vc_2(x) + uvc_3(x)\\
=&(x-1)^i + u\sum_{j=0}^{2^s-1} c_{0j}^{(1)}(x-1)^j + v\sum_{j=0}^{2^s-1} c_{0j}^{(2)}(x-1)^j + uv\sum_{j=0}^{2^s-1}(c_{2j}^{(1)} + c_{1j}^{(2)} + c_{0j}^{(3)})(x-1)^j\\
=& (x-1)^i + u\sum_{j=0}^{2^s-1} a_{1j}(x-1)^j + v\sum_{j=0}^{2^s-1} a_{2j}(x-1)^j + uv\sum_{j=0}^{2^s-1} a_{3j}(x-1)^j,
\end{aligned}$$

where $a_{1j} = c_{0j}^{(1)}, a_{2j} = c_{0j}^{(2)}, a_{3j} = c_{2j}^{(1)} + c_{1j}^{(2)} + c_{0j}^{(3)}$, and for all l with $i \le l \le 2^s-1$,

$$uv(x-1)^l = uv[(x-1)^i + u\sum_{j=0}^{2^s-1} a_{1j}(x-1)^j + v\sum_{j=0}^{2^s-1} a_{2j}(x-1)^j + uv\sum_{j=0}^{2^s-1} a_{3j}(x-1)^j](x-1)^{l-i} \in I.$$

It follows that

$$(x-1)^i + u\sum_{j=0}^{2^s-1} a_{1j}(x-1)^j + v\sum_{j=0}^{2^s-1} a_{2j}(x-1)^j + uv\sum_{j=0}^{l-1} a_{3j}(x-1)^j \in I.$$

Hence it can be assumed without loss of generality that

$$a(x) = (x-1)^i + u\sum_{j=0}^{i} a_{1j}(x-1)^j + v\sum_{j=0}^{i} a_{2j}(x-1)^j + uv\sum_{j=0}^{i} a_{3j}(x-1)^j \in I.$$

Now we have two subcases.

Case 3.1 $I=\langle (x-1)^i+u\sum_{j=0}^{i}a_{1j}(x-1)^j+v\sum_{j=0}^{i}a_{2j}(x-1)^j+uv\sum_{j=0}^{i}a_{3j}(x-1)^j\rangle$, where $0\le i\le 2^s-1$. Then I is in Type 9.

Case 3.2 $\langle (x-1)^i+u\sum_{j=0}^{i}a_{1j}(x-1)^j+v\sum_{j=0}^{i}a_{2j}(x-1)^j+uv\sum_{j=0}^{i}a_{3j}(x-1)^j\rangle \subsetneq I$. For every $f(x)\in I\backslash\langle (x-1)^i+u\sum_{j=0}^{i}a_{1j}(x-1)^j+v\sum_{j=0}^{i}a_{2j}(x-1)^j+uv\sum_{j=0}^{i}a_{3j}(x-1)^j\rangle$, there is an element $g(x)\in R_1$ such that

$$0\neq b_f(x)=f(x)-g(x)[(x-1)^i+u\sum_{j=0}^{i}a_{1j}(x-1)^j+v\sum_{j=0}^{i}a_{2j}(x-1)^j+uv\sum_{j=0}^{i}a_{3j}(x-1)^j]\in I,$$

and $b_f(x)$ can be expressed as

$$b_f(x)=\sum_{j=0}^{i}b_{0j}(x-1)^j+u\sum_{j=0}^{i}b_{1j}(x-1)^j+v\sum_{j=0}^{i}b_{2j}(x-1)^j+uv\sum_{j=0}^{i}b_{3j}(x-1)^j\in I,$$

where $b_{0j},b_{1j},b_{2j},b_{3j}\in\mathbb{F}_2$. Now, by the definition of $I_{u,v}$, we have

$$\sum_{j=0}^{i}b_{0j}(x-1)^j\in I_{u,v}=\langle (x-1)^i\rangle.$$

It implies that b_{0j} for all $0\le j\le i$, i.e.,

$$b_f(x)=u\sum_{j=0}^{i}b_{1j}(x-1)^j+v\sum_{j=0}^{i}b_{2j}(x-1)^j+uv\sum_{j=0}^{i}b_{3j}(x-1)^j\in I.$$

Similarly with Case 2, we have

$$\begin{aligned}I=&\langle (x-1)^i+u\sum_{j=0}^{i}a_{1j}(x-1)^j+v\sum_{j=0}^{i}a_{2j}(x-1)^j+uv\sum_{j=0}^{t}a_{3j}(x-1)^j,\\&u(x-1)^l+v\sum_{j=0}^{i}h_{2j}(x-1)^j+uv\sum_{j=0}^{t}h_{3j}(x-1)^j\rangle,\end{aligned}$$

where $0\le i\le 2^s-1, 0\le l\le 2^s-1$ and $t\le\min\{i,l\}$. Therefore, I is in Type 10.

$$\begin{aligned}I=&\langle (x-1)^i+u\sum_{j=0}^{i}a_{1j}(x-1)^j+v\sum_{j=0}^{i}a_{2j}(x-1)^j+uv\sum_{j=0}^{t}a_{3j}(x-1)^j,u(x-1)^l\\&+v\sum_{j=0}^{i}h_{2j}(x-1)^j+uv\sum_{j=0}^{t}h_{3j}(x-1)^j,uv(x-1)^t\rangle,\end{aligned}$$

where $0 \le i \le 2^s - 1, 0 \le l \le 2^s - 1$ and $t \le \min\{i, l\}$. Thus, I is in Type 11.

$$I = \langle (x-1)^i + u\sum_{j=0}^{i} a_{1j}(x-1)^j + v\sum_{j=0}^{i} a_{2j}(x-1)^j + uv\sum_{j=0}^{t} a_{3j}(x-1)^j,$$
$$u(x-1)^l + v\sum_{j=0}^{i} h_{2j}(x-1)^j + uv\sum_{j=0}^{t} h_{3j}(x-1)^j, v(x-1)^z + uv\sum_{j=0}^{t} b_{3j}(x-1)^j \rangle,$$

where $0 \le i \le 2^s - 1, 0 \le l \le 2^s - 1, 0 \le z \le 2^s - 1$ and $t \le \min\{i, l, z\}$. Thus, I is in Type 12.

$$I = \langle (x-1)^i + u\sum_{j=0}^{i} a_{1j}(x-1)^j + v\sum_{j=0}^{i} a_{2j}(x-1)^j + uv\sum_{j=0}^{w} a_{3j}(x-1)^j, u(x-1)^l$$
$$+ v\sum_{j=0}^{i} h_{2j}(x-1)^j + uv\sum_{j=0}^{w} h_{3j}(x-1)^j, v(x-1)^z + uv\sum_{j=0}^{w} b_{3j}(x-1)^j, uv(x-1)^w \rangle,$$

where $0 \le i \le 2^s - 1, 0 \le l \le 2^s - 1, 0 \le z \le 2^s - 1$ and $w \le \min\{i, l, z\}$. Thus, I is in Type 13.

Similar to discussion in Theorem 3.5, and note that $(x-1)^{2^s} = uv$, we have following theorem.

Theorem 3.6 $(1 + uv)$-constacyclic codes of length 2^s over R, i.e., ideals of the ring R_2 are

- Type 1: $\langle 0 \rangle, \langle 1 \rangle$;
- Type 2: $I = \langle uv(x-1)^\sigma \rangle$, where $0 \le \sigma \le 2^s - 1$;
- Type 3: $I = \langle v(x-1)^t + uv\sum_{j=0}^{t} m_{1j}(x-1)^j \rangle$, where $0 \le t \le 2^s - 1$;
- Type 4: $I = \langle v(x-1)^t + uv\sum_{j=0}^{t-1} m_{1j}(x-1)^j, uv(x-1)^z \rangle$, where $1 \le t \le 2^s - 1, z < t$;
- Type 5: $I = \langle u(x-1)^l + v\sum_{j=0}^{2^s-1} h_{2j}(x-1)^j + uv\sum_{j=0}^{l} h_{3j}(x-1)^j \rangle$, where $0 \le l \le 2^s - 1$;
- Type 6: $I = \langle u(x-1)^l + v\sum_{j=0}^{2^s-1} h_{2j}(x-1)^j + uv\sum_{j=0}^{l-1} h_{3j}(x-1)^j, uv(x-1)^t \rangle$, where $1 \le l \le 2^s - 1, t < l$;
- Type 7: $I = \langle u(x-1)^l + v\sum_{j=0}^{2^s-1} h_{2j}(x-1)^j + uv\sum_{j=0}^{l} h_{3j}(x-1)^j, v(x-1)^z + uv\sum_{j=0}^{z} b_{3j}(x-1)^j \rangle$, where $0 \le l \le 2^s - 1, 0 \le z \le 2^s - 1$;
- Type 8: $I = \langle u(x-1)^l + v\sum_{j=0}^{z-1} h_{2j}(x-1)^j + uv\sum_{j=0}^{z-1} h_{3j}(x-1)^j, v(x-1)^z + uv\sum_{j=0}^{z-1} b_{3j}(x-1)^j, uv(x-1)^w \rangle$, where $1 \le l \le 2^s - 1, 1 \le z \le 2^s - 1$, and $w < \min\{l, z\}$;
- Type 9: $I = \langle (x-1)^i + u\sum_{j=0}^{i} a_{1j}(x-1)^j + v\sum_{j=0}^{i} a_{2j}(x-1)^j + uv\sum_{j=0}^{i} a_{3j}(x-1)^j \rangle$, where $0 \le i \le 2^s - 1$;

• Type 10: $I=\langle (x-1)^i+u\sum_{j=0}^{i}a_{1j}(x-1)^j+v\sum_{j=0}^{i}a_{2j}(x-1)^j+uv\sum_{j=0}^{t}a_{3j}(x-1)^j, u(x-1)^l+v\sum_{j=0}^{i}h_{2j}(x-1)^j+uv\sum_{j=0}^{t}h_{3j}(x-1)^j\rangle$, where $0\le i\le 2^s-1, 0\le l\le 2^s-1$ and $t\le \min\{i,l\}$;

• Type 11: $I=\langle (x-1)^i+u\sum_{j=0}^{i}a_{1j}(x-1)^j+v\sum_{j=0}^{i}a_{2j}(x-1)^j+uv\sum_{j=0}^{t}a_{3j}(x-1)^j, u(x-1)^l+v\sum_{j=0}^{i}h_{2j}(x-1)^j+uv\sum_{j=0}^{t}h_{3j}(x-1)^j, uv(x-1)^t\rangle$, where $0\le i\le 2^s-1, 0\le l\le 2^s-1$ and $t\le \min\{i,l\}$;

• Type 12: $I=\langle (x-1)^i+u\sum_{j=0}^{i}a_{1j}(x-1)^j+v\sum_{j=0}^{i}a_{2j}(x-1)^j+uv\sum_{j=0}^{t}a_{3j}(x-1)^j, u(x-1)^l+v\sum_{j=0}^{i}h_{2j}(x-1)^j+uv\sum_{j=0}^{t}h_{3j}(x-1)^j, v(x-1)^z+uv\sum_{j=0}^{t}b_{3j}(x-1)^j\rangle$, where $0\le i\le 2^s-1, 0\le l\le 2^s-1, 0\le z\le 2^s-1$ and $t\le \min\{i,l,z\}$;

• Type 13: $I=\langle (x-1)^i+u\sum_{j=0}^{i}a_{1j}(x-1)^j+v\sum_{j=0}^{i}a_{2j}(x-1)^j+uv\sum_{j=0}^{w}a_{3j}(x-1)^j, u(x-1)^l+v\sum_{j=0}^{i}h_{2j}(x-1)^j+uv\sum_{j=0}^{w}h_{3j}(x-1)^j, v(x-1)^z+uv\sum_{j=0}^{w}b_{3j}(x-1)^j, uv(x-1)^w\rangle$, where $0\le i\le 2^s-1, 0\le l\le 2^s-1, 0\le z\le 2^s-1$ and $w\le \min\{i,l,z\}$.

4 Constacyclic Codes of Length 2^s over R

In this section, we discuss the λ-constacyclic codes, where

$$\lambda=1+u, 1+v, 1+u+uv, 1+v+uv, 1+u+v, 1+u+v+uv.$$

First, we study the structure of the $(1+u)$-constacyclic codes of length 2^s over R. Obviously, $(1+u)$-constacyclic codes of length 2^s over R are ideals of the residue ring $R_3=\frac{R[x]}{\langle x^{2^s}-(1+u)\rangle}$. It is easy to verify the following lemmas.

Lemma 4.1 The following hold true in R_3.

(i) For any nonnegative integer t, $(x-1)^{2^t}=x^{2^t}-1$. In particular, $(x-1)^{2^s}=u$.

(ii) $x-1$ is nilpotent with the nilpotency index 2^{s+1}.

Lemma 4.2 Let $f(x)\in R_3$. Then $f(x)$ can be uniquely expressed as

$$f(x)=\sum_{j=0}^{2^{s+1}-1}a_{0j}(x-1)^j+v\sum_{j=0}^{2^{s+1}-1}a_{1j}(x-1)^j,$$

where $a_{0j}, a_{1j}\in\mathbb{F}_2$. Furthermore, $f(x)$ is invertible if and only if $a_{00}\neq 0$

Proof Since each element $r\in R$ has a unique presentation $r=r_1+ur_2+vr_3+uvr_4$, where $r_1, r_2, r_3, r_4\in\mathbb{F}_2$, each element $f(x)$ over R_3 can be uniquely represented as

$$f(x)=\sum_{j=0}^{2^{s+1}-1}b_{0j}(x-1)^j+u\sum_{j=0}^{2^{s+1}-1}b_{1j}(x-1)^j+v\sum_{j=0}^{2^{s+1}-1}b_{2j}(x-1)^j+uv\sum_{j=0}^{2^{s+1}-1}b_{3j}(x-1)^j.$$

Because $(x-1)^{2^s}=u$ in R_3, it can be uniquely represented without loss of generality that $f(x)=\sum\limits_{j=0}^{2^{s+1}-1}a_{0j}(x-1)^j+v\sum\limits_{j=0}^{2^{s+1}-1}a_{1j}(x-1)^j$, where $a_{0j},a_{1j}\in\mathbb{F}_2$. The last assertion follows from the fact that v and $x-1$ are both nilpotent in R_3.

Similar to the discussions in Proposition 3.3, we have the following proposition.

Proposition 4.3 The ring R_3 is a local ring with the maximal ideals $\langle v,x-1\rangle$, but it is not a chain ring.

Following the proposition and lemmas above, we can list all $(1+u)$-constacyclic codes of length 2^s over R_3 as follows.

Theorem 4.4 $(1+u)$-constacyclic codes of length 2^s over R, i.e., ideals of the ring R_3 are

- Type 1: $\langle 0\rangle,\langle 1\rangle$;
- Type 2: $I=\langle v(x-1)^k\rangle$, where $0\le k\le 2^s-1$;
- Type 3: $I=\langle (x-1)^l+v\sum\limits_{j=0}^{l-1}c_{1j}(x-1)^j\rangle$, where $1\le l\le 2^{s+1}-1$;
- Type 4: $I=\langle (x-1)^l+v\sum\limits_{j=0}^{w-1}c_{1j}(x-1)^j, v(x-1)^w\rangle$, where $1\le l\le 2^{s+1}-1,\ w\le l$.

Proof Ideals of Type 1 are the trivial ideals. Consider an arbitrary nontrivial ideal of R_3.

Case 1 $I\subseteq\langle v\rangle$. Any element of I must have the form $v\sum\limits_{j=0}^{2^{s+1}-1}a_{0j}(x-1)^j$, where $a_{0j}\in\mathbb{F}_2$. Let $b(x)\in I$ be an element that has the smallest k such that $a_{0k}\neq 0$. Hence all element $a(x)\in I$ have the form

$$a(x)=v(x-1)^k\sum_{j=k}^{2^{s+1}-1}a_{0j}(x-1)^{j-k},$$

which implies $I\subseteq\langle u(x-1)^k\rangle$.

On the other hand, we have $b(x)\in I$ with

$$b(x)=v(x-1)^k[a_{0k}+\sum_{j=k+1}^{2^{s+1}-1}a_{0j}(x-1)^{j-k}].$$

As $a_{0k}\neq 0$, $a_{0k}+\sum\limits_{j=k+1}^{2^{s+1}-1}a_{0j}(x-1)^{j-k}$ is invertible, and $v(x-1)^k\in I$. That is to say, the ideal of R_3 contained in $\langle v\rangle$ are $\langle v(x-1)^k\rangle, 0\le k\le 2^{s+1}-1$. It means that I is in Type 2.

Case 2 $I\nsubseteq\langle v\rangle$. Any element of I must have the form

$$\sum_{j=0}^{2^{s+1}-1}a_{0j}(x-1)^j+v\sum_{j=0}^{2^{s+1}-1}a_{1j}(x-1)^j,$$

and there exists a polynomial

$$\sum_{j=0}^{2^{s+1}-1}b_{0j}(x-1)^j+v\sum_{j=0}^{2^{s+1}-1}b_{1j}(x-1)^j$$

in I such that $\sum\limits_{j=0}^{2^{s+1}-1} b_{0j}(x-1)^j \neq 0$. Let

$$M = \{ \sum_{j=0}^{2^{s+1}-1} a_{0j}(x-1)^j + v \sum_{j=0}^{2^{s+1}-1} a_{1j}(x-1)^j \in I \mid \sum_{j=0}^{2^{s+1}-1} a_{0j}(x-1)^j \neq 0, a_{0j}, a_{1j} \in \mathbb{F}_2\}$$

and $N = \{v \sum\limits_{j=0}^{2^{s+1}-1} a_{1j}(x-1)^j \in I \mid a_{1j} \in \mathbb{F}_2\}$. Setting $\delta = \min\{\deg(m(x)) \mid m(x) \in M\}$. Suppose that $H = \{h(x) \in M \mid \deg(h(x)) = \delta\}$. Then there is an element

$$h_1(x) = \sum_{j=0}^{2^{s+1}-1} h_{0j}(x-1)^j + v \sum_{j=0}^{2^{s+1}-1} h_{1j}(x-1)^j$$

in H that has the smallest l such that $h_{0l} \neq 0$. Hence we have

$$h_1(x) = (x-1)^l[h_{0l} + \sum_{j=l+1}^{2^{s+1}-1} h_{0j}(x-1)^{j-l}] + v \sum_{j=0}^{2^{s+1}-1} h_{1j}(x-1)^j \in M \subset I.$$

Now, we have two subcases.

Case 2.1 $N \subseteq \langle h_1(x)\rangle$. For any $f(x) \in M$, by Proposition 2.1, $f(x)$ can be written as $f(x) = q(x)h_1(x) + r(x)$, where $q(x), r(x) \in R_3$, and $r(x) = 0$ or $\deg(r(x)) < \deg(h_1(x))$. Suppose $r(x) \notin N$. Then $r(x) \neq 0$. Hence $r(x) = f(x) - q(x)h_1(x) \in M$, which contradicts with the assumption of $h_1(x)$. Thus $r(x) \in N$. Therefore, $I = \langle h_1(x)\rangle$. Because $vh_1(x) = v(x-1)^l[h_{0l} + \sum\limits_{j=l+1}^{2^{s+1}-1} h_{1j}(x-1)^{j-t}] \in I$ and $h_{0l} + \sum\limits_{j=l+1}^{2^{s+1}-1} h_{0j}(x-1)^{j-t}$ is an invertible element in R_3, $v(x-1)^l \in I$, it follows that

$$\tilde{h}_1(x) = (x-1)^l[h_{0l} + \sum_{j=l+1}^{2^{s+1}-1} h_{0j}(x-1)^{j-l}] + v \sum_{j=0}^{l-1} h_{1j}(x-1)^j \in I.$$

Thus

$$c(x) = \tilde{h}_1(x)[h_{0l} + \sum_{j=l+1}^{2^{s+1}-1} h_{0j}(x-1)^{j-l}]^{-1} \in I$$

and $c(x)$ can be expressed as $c(x) = (x-1)^l + v \sum\limits_{j=0}^{l-1} c_{1j}(x-1)^j$, where $c_{1j} \in \mathbb{F}_2$. Therefore,

$$I = \langle (x-1)^l + v \sum_{j=0}^{l-1} c_{1j}(x-1)^j \rangle,$$

where $1 \leq l \leq 2^{s+1} - 1$. Hence I is in Type 3.

Case 2.2 $N \nsubseteq \langle h_1(x)\rangle = \langle c(x)\rangle$. Then there exists the smallest integer w such that $n(x) = v(x-1)^w n_1(x)$ for every $n(x) \in N$, where $n_1(x) \in R_3$. Obviously, $v(x-1)^w \in N$, but $v(x-1)^w \notin \langle h_1(x)\rangle = \langle c(x)\rangle$. Hence $I = \langle (x-1)^l + v \sum\limits_{j=0}^{l-1} c_{1j}(x-1)^j, v(x-1)^w\rangle$.

Suppose that $w > l$. Then

$$v(x-1)^w = v(x-1)^{w-l}[(x-1)^l + v\sum_{j=0}^{l-1} c_{1j}(x-1)^j] \in \langle c(x)\rangle.$$

It is impossible. Thus

$$I = \langle (x-1)^l + v\sum_{j=0}^{w-1} c_{1j}(x-1)^j, v(x-1)^w\rangle,$$

where $1 \le l \le 2^{s+1}-1,\ w \le l$. Therefore, I is in Type 4.

Next we study the structure of $(1+v), (1+u+uv), (1+v+uv), (1+u+v), (1+u+v+uv)$-constacyclic codes of length 2^s over R. Similar to the discussion in Theorem 4.4, we have the following theorems.

Theorem 4.5 $(1+u+uv), (1+u+v), (1+u+v+uv)$-constacyclic codes over R are

- Type 1: $\langle 0\rangle, \langle 1\rangle$;
- Type 2: $I = \langle v(x-1)^k\rangle$, where $0 \le k \le 2^{s+1}-1$;
- Type 3: $I = \langle (x-1)^l + v\sum\limits_{j=0}^{l-1} c_{1j}(x-1)^j\rangle$, where $1 \le l \le 2^{s+1}-1$;
- Type 4: $I = \langle (x-1)^l + v\sum\limits_{j=0}^{l-1} c_{1j}(x-1)^j, v(x-1)^w\rangle$, where $1 \le l \le 2^{s+1}-1,\ w \le l$.

Proof

$$f(x) = \sum_{j=0}^{2^{s+1}-1} a_{0j}(x-1)^j + v\sum_{j=0}^{2^{s+1}-1} a_{1j}(x-1)^j,$$

where $a_{0j}, a_{1j} \in \mathbb{F}_2$. Furthermore, $f(x)$ is invertible if and only if $a_{00} \ne 0$.

Now, Similar to the discussion in Theorem 4.4, we can complete the proof of statement.

Theorem 4.6 $(1+v), (1+v+uv)$-constacyclic codes over R are

- Type 1: $\langle 0\rangle, \langle 1\rangle$;
- Type 2: $I = \langle u(x-1)^k\rangle$, where $0 \le k \le 2^{s+1}-1$;
- Type 3: $I = \langle (x-1)^l + u\sum\limits_{j=0}^{l-1} c_{1j}(x-1)^j\rangle$, where $1 \le l \le 2^{s+1}-1$;
- Type 4: $I = \langle (x-1)^l + u\sum\limits_{j=0}^{l-1} c_{1j}(x-1)^j, u(x-1)^w\rangle$, where $1 \le l \le 2^{s+1}-1, w \le l$.

Proof $f(x) = \sum\limits_{j=0}^{2^{s+1}-1} a_{0j}(x-1)^j + u\sum\limits_{j=0}^{2^{s+1}-1} a_{1j}(x-1)^j$, where $a_{0j}, a_{1j} \in \mathbb{F}_2$. Furthermore, $f(x)$ is invertible if and only if $a_{00} \ne 0$.

Now, in the proof of Theorem 4.4, we replace each v by u and get our statement.

References

[1] Yildiz B, Karedemiz S. Linear codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$[J]. Des. Codes Cryptogr., 2010, 54: 61–81.

[2] Bonnecaza A, Udaya P. Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$[J]. IEEE Trans. Inform. Theory, 1999, 45: 1250–1255.

[3] Dougherty S T, Gaborit P, Harada M, Solé P. Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$[J]. IEEE Trans. Inform. Theory, 1999, 45: 32–45.

[4] Qian J F, Zhang L N, Zhu S X. $(1-u)$-constacyclic and cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2$[J]. Applied Math. Lett., 2006, 19: 820–823

[5] Yildiz B, Karedemiz S. Cyclia codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$[J]. Des. Codes Cryptoger., 2011, 58: 221–234.

[6] Karedemiz S, Yildiz B. $(1+v)$-constacyclic codes over $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$[J]. J. Franklin Institute, 2011, 348: 2625–2632.

[7] Dougherty S T, Karadeniz S, Yildiz B. Cyclic codes over R_k[J]. Des. Codes Cryptogr., 2012, 63(1): 113–126.

[8] KumarKewat P, Ghosh B, Pattanayak S. Cyclic codes over the ring $\frac{\mathbb{Z}_p[u,v]}{\langle u^2,v^2,uv-vu\rangle}$[J]. Finite Field Appl., 2015, 34: 161–175.

[9] Dinh H Q. Negacyclic codes of length 2^s over Galois rings[J]. IEEE Trans. Inform. Theory, 2005, 511: 4252–4262.

[10] Dinh H Q. López-Permouth S R. Cyclic and negacyclic codes over finite chain rings[J]. IEEE Trans. Inform. Theory, 2004, 50: 1728–1744.

[11] Dinh H Q. Constacyclic codes of length 2^s over Galois exlension rings of $\mathbb{F}_2 + u\mathbb{F}_2$[J]. IEEE Trans. Inform. Theory, 2009, 55: 1730–1740.

[12] Dinh H Q. Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$[J]. J. Alg., 2010, 324: 940–950.

[13] Norton G H, Sălăgean A. On the struture of linear and cyclic codes over a finite chain ring[J]. AAECC, 2000, 10: 489–506.

[14] Sălăgean A. Repelated-root cyclic and negacyclic codes over finite chain rings[J]. Disc. Appl. Math., 2006, 154: 413–419.

[15] Ling S, Niederreiter H, Solé P. On the algebraic structure of quasi-cyclic codes, IV, repeated root[J]. Des. Codes Crypt., 2006, 38: 337–361.

[16] McDonald B R. Finite ring with indentity[M]. New York: Marce Dekker, 1974.

环 $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ 上长度为 2^s 的常循环码

刘修生, 许小芳, 胡 鹏

(湖北理工学院数理学院, 湖北 黄石 435003)

摘要: 本文研究了环$R = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ 上长度为 2^s 的常循环码的分类和结构, 这个环是一个局部环, 但不是链环. 首先, 借助有限交换局部环中多项式的欧几里德算法, 得到了长为2^s的循环码与$(1+uv)$-常循环码分类, 且给出了每一类的结构. 其次, 利用$(x-1)^{2^s} = u$, 得到了长为2^s的$(1+u)$-常循环码分类和每一类的结构. 最后, 利用类似于长为2^s的$(1+u)$-常循环码的讨论方法, 给出了$(1+v), (1+u+uv), (1+v+uv), (1+u+v), (1+u+v+uv)$-常循环码分类和每一类的结构.

关键词: 常循环码; 循环码; 局部环; 重根循环码

MR(2010)**主题分类号**: 94B05; 94B15 **中图分类号**: O157.4