MDS and self-dual codes over rings

Kenza Guenda a, T. Aaron Gulliverb,∗

a Faculty of Mathematics, USTHB, University of Science and Technology of Algiers, Algeria
b Department of Electrical and Computer Engineering, University of Victoria, PO Box 3055, STN CSC, Victoria, BC, V8W 3P6, Canada

ABSTRACT

In this paper we give the structure of constacyclic codes over formal power series and chain rings. We also present necessary and sufficient conditions on the existence of MDS codes over principal ideal rings. These results allow for the construction of infinite families of MDS self-dual codes over finite chain rings, formal power series and principal ideal rings. We also define the Reed–Solomon codes over principal ideal rings.

© 2012 Elsevier Inc. All rights reserved.

1. Introduction

Although codes over rings are not new [3], they have attracted significant attention from the scientific community only since 1994, when Hammons et al. [16] established a fundamental connection between non-linear binary codes and linear codes over \( \mathbb{Z}_4 \). In [16], it was proven that some of the best non-linear codes, such as the Kerdock, Preparata, and Goethal codes can be viewed as linear codes over \( \mathbb{Z}_4 \) via the Gray map from \( \mathbb{Z}_4^n \) to \( \mathbb{F}_2^n \). The link between self-dual codes and unimodular lattices was given by Bonnecaze et al. [4] and Bannai et al. [1]. These results created a great deal of interest in self-dual codes over a variety of rings, see [24] and the references therein. Calderbank
and Sloane [6] gave the structure of cyclic codes over $\mathbb{Z}_{p^e}$. Dinh, Kanwar and Lopez-Permouth [18,7] presented the structure of cyclic and negacyclic codes over chain rings. Norton and Sălăgean [23,22] provided a different approach to the study of these codes, and they considered the problem of determining the minimum distance. Dougherty et al. [9,10] used the Chinese remainder theorem to generalize the structure of codes over principal ideal rings. They gave conditions on the existence of self-dual codes over principal ideal rings in [9], and conditions on the existence of MDS codes over these rings in [10]. Dougherty et al. [12,11] introduced the $\gamma$-adic codes over a formal power series ring and studied cyclic and negacyclic codes over these rings.

Dougherty [13] recently posed a number of problems concerning codes over rings. Several of these are answered in this paper. In particular, we give necessary and sufficient conditions on the existence of MDS codes over all the base fields. We also give the structure of constacyclic codes over formal power series and chain rings. The projection and the lift of these codes is described using a generalization of the Hensel Lift Lemma and the structure of the ideals of $R[x]/\langle x^e - \lambda \rangle$. Finally, infinite families of MDS self-dual codes are given over principal ideal rings, finite chain rings and formal power series.

We begin by reviewing and extending the necessary results on finite chain rings. The lift and projection of these rings are given in the references above. In Section 3, we give a necessary and sufficient condition on the existence of MDS codes over principal ideal rings. We also construct Reed–Solomon codes over these rings. In Section 4, constacyclic codes over finite chain rings and formal power series rings are examined. The structure of the ideals of $R[x]/\langle x^e - \lambda \rangle$ is given. We consider the free constacyclic codes and their lifts, and the number of such codes is determined. In the last section, two families of MDS self-dual codes over chain rings and principal ideal rings are constructed. These codes are derived from the MDS and self-dual codes given in [15]. A table of these codes is given which includes self-dual MDS codes derived from the codes in [2,19,15].

2. Codes over finite chain rings and formal power series rings

A finite chain ring is a local principal ideal ring with maximal ideal $\langle \gamma \rangle$, where $\gamma$ is a nilpotent element of $R$ with nilpotency index $e$. Hence the elements of $R \setminus \langle \gamma \rangle = R^*$ are units and the ideals of $R$ form the following chain

$$(0) = \langle \gamma^e \rangle \subset \langle \gamma^{e-1} \rangle \subset \cdots \subset \langle \gamma \rangle \subset R.$$

If we denote the field $R/\langle \gamma \rangle$ by $K$, then we have the following canonical ring morphism

$$- : R[x] \to K[x],$$

$$f \mapsto \bar{f} = f \pmod{\gamma}.$$ (1)

The following lemma is well known (see [11,12,22], for example).

**Lemma 2.1.** Let $R$ be a finite chain ring with maximal ideal $\langle \gamma \rangle$. Let $V \subseteq R$ be a set of representatives for the equivalence classes of $R$ under congruence modulo $\gamma$. Then

(i) for all $v \in R$ there exist unique $v_0, \ldots, v_{e-1} \in V$ such that $v = \sum_{i=0}^{e-1} v_i \gamma^i$;
(ii) $|V| = |K|$;
(iii) $|\langle \gamma^j \rangle| = |K|^{e-j}$ for $0 \leq j \leq e - 1$.

By Lemma 2.1, we can compute the cardinality of $R$ as follows

$$|R| = |K| \cdot |\langle \gamma \rangle| = |K| \cdot |K|^{e-1} = |K|^e = p^{er}.$$ (2)
A code $C$ of length $n$ over $R$ is a subset of $R^n$. If the code is a submodule we say that the code is linear. Here, all codes are assumed to be linear. If $n$ is the length of the code and $p$ is the characteristic of $K$ we also assume that $\gcd(n, p) = 1$.

We attach the standard inner product to the ambient space, i.e., $v \cdot w = \sum v_i w_i$. The dual code $C^\perp$ of $C$ is defined by $C^\perp = \{v \in R^n \mid v \cdot w = 0\text{ for all }w \in C\}$. If $C \subseteq C^\perp$, we say that the code is self-orthogonal, and if $C = C^\perp$ we say that the code is self-dual.

Let $R$ be a finite chain ring. From [6], any linear code over $R$ has a generator matrix in the following standard form

$$
\begin{pmatrix}
I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & \cdots & A_{0,e} \\
0 & \gamma I_{k_1} & \gamma A_{1,2} & \gamma A_{1,3} & \cdots & \cdots & \gamma A_{1,e} \\
0 & 0 & \gamma^2 I_{k_2} & \gamma^2 A_{2,3} & \cdots & \cdots & \gamma^2 A_{2,e} \\
\vdots & \vdots & 0 & \ddots & \ddots & \ddots & \vdots \\
\vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & \cdots & \gamma^{e-1} I_{k_{e-1}} & \gamma^{e-1} A_{e-1,e}
\end{pmatrix},
$$

where the columns are grouped into blocks of sizes $k_0, k_1, \ldots, k_{e-1}, n - \sum_{i=0}^{e-1} k_i$. We say that $C$ is of type $1^{k_0} \gamma^{k_1} \gamma^2 I_{k_2} \cdots (\gamma^{e-1})^{k_{e-1}}$. We have the following equalities

$$
|C| = |K|^{\sum_{i=0}^{e-1} (e-i)k_i},
$$

$$
|C||C^\perp| = q^{\sum (e-i)(k_i + k_j)} = q^n |R|^n,	ext{ and } (C^\perp)^\perp = C.
$$

The rank of $C$ is defined to be

$$
k(C) = \sum_{i=0}^{e-1} k_i.
$$

The free rank of $C$ is defined to be the maximum of the ranks of the free submodules of $C$. A linear code is said to be free if its free rank is equal to its rank. In this case, the code is a free $R$-submodule which is isomorphic as a module to $R^{k(C)}$, and has a basis of $k(C)$ elements. As for codes over finite fields, we denote by $d_H(C)$ or simply $d$ the minimum non-zero Hamming distance of $C$.

The well-known Singleton bound for codes over any alphabet of size $m$ (see [20]) gives that

$$
d_H(C) \leq n - \log_m(|C|) + 1.
$$

If a code meets this bound, it is called maximum distance separable (MDS). For codes over principal ideal rings we have the following bound [17]

$$
d_H(C) \leq n - k(C) + 1.
$$

This is a stronger bound in general unless the linear code is free, in which case the bounds coincide. If a code over $R$ meets the bound (8), then we say that $C$ is a Maximum Distance with respect to Rank (MDR) code. The submodule quotient of $C$ by $v \in R$ is the code

$$
(C : v) = \{x \in R^n \mid xv \in C\}.
$$

Thus we have the tower of linear codes over $R$,

$$
C = (C : \gamma) \subseteq \cdots \subseteq (C : \gamma^i) \subseteq \cdots \subseteq (C : \gamma^{e-1}).
$$
For \( i = 1, 2, \ldots, e - 1 \) the projections of \((C : \gamma^i)\) over the field \( K \) are denoted by \( \text{Tor}_i(C) = (\overline{C} : \gamma^i) \), and are called the torsion codes associated with the code \( C \). By a proof similar to that for [8, Theorem 5.1], one can obtain the following result

\[
|\text{Tor}_i(C)| = \prod_{j=0}^{i} q^{k_j}. \tag{10}
\]

Using (9), we obtain the following tower

\[
\text{Tor}_0(C) \subset \text{Tor}_1(C) \subset \cdots \subset \text{Tor}_{e-1}(C) \subset \text{Tor}_0(C)\perp. \tag{11}
\]

**Proposition 2.2.** Let \( R \) be a finite chain ring with maximal ideal \( \gamma \) and nilpotency index \( e \). Then the following hold:

(i) If \( C \) is a linear MDS code over \( R \) of rank \( k = k(C) \) and type \( \gamma^0 \gamma^{k_1} \gamma^{k_2} \cdots (\gamma^{e-1})^{k_{e-1}} \), we have that \( k_i = 0 \) for \( i > 0 \). Furthermore we have \( \text{Tor}_i(C) = \text{Tor}_0(C) \) for all \( 0 \leq i, j \leq e - 1 \), and it is an MDS code of length \( n \) and dimension \( k \) over the field \( K \).

(ii) If there exists an MDS code over \( R \), then \( \text{Tor}_{e-1}(C) \) is an MDS code over the field \( K \).

**Proof.** From (4) we have \( |C| < p^{ek} \). If \( k_i > 0 \) for any \( i > 0 \), then the code meets the bound given in (7), which prevents the code from meeting the bound given in (8). Thus \( C \) is a free code. From [10, Theorem 5.3] \( \text{Tor}_i(C) = \text{Tor}_{0}(C) \) for all \( 0 \leq i, j \leq e - 1 \), and \( \text{Tor}_i(C) \) is an MDS code. Part (ii) follows from [10, Theorem 5.4]. \( \square \)

From Lemma 2.1 we can deduce that any element \( a \) of \( R \) can be written uniquely as \( a = a_0 + a_1 \gamma + \cdots + a_{e-1} \gamma^{e-1} \), where \( a_i \in K \). Hence for integer \( i > 0 \), we define \( R_i \) as

\[
R_i = \{ a_0 + a_1 \gamma + \cdots + a_{i-1} \gamma^{i-1} \mid a_i \in K \}. \tag{12}
\]

Then the \( R_i \) are finite chain rings with \( R_1 = K \) and \( R_e = R \). \( R_i \) has index of nilpotency \( i \), maximal ideal \( \langle \gamma \rangle \), and set of units

\[
R_i^* = \left\{ \sum_{l=0}^{i-1} a_l \gamma^l \mid 0 \neq a_0 \in K \right\}. \tag{13}
\]

The ring of formal power series \( R_\infty \) is defined as

\[
R_\infty = K[[\gamma]] = \left\{ \sum_{l=0}^{\infty} a_l \gamma^l \mid a_l \in K \right\}. \tag{14}
\]

The following result is well known [5,11,26].

**Lemma 2.3.** Assume the notation given above. Then we have that

(i) \( R_\infty^* = \{ \sum_{l=0}^{\infty} a_l \gamma^l \mid a_0 \neq 0 \} \);

(ii) the ring \( R_\infty \) is a principal ideal domain with a unique maximal ideal \( \langle \gamma \rangle \).
Hence from Lemma 2.3, any non-zero element \( a \) of \( R_\infty \) can be written as

\[
a = \gamma^d,
\]

with \( d \) a unit in \( R_\infty \). The generator matrix of a linear code over \( R_\infty \) is given by the following lemma.

**Lemma 2.4.** (See [12, Lemma 3.3].) Let \( C \) be a non-zero linear code over \( R_\infty \) of length \( n \). Then any generator matrix of \( C \) is permutation equivalent to a matrix of the following form

\[
G = \begin{pmatrix}
\gamma^{m_0}I_{k_0} & \gamma^{m_0}A_{0,1} & \gamma^{m_0}A_{0,2} & \gamma^{m_0}A_{0,3} & \cdots & \gamma^{m_0}A_{0,r} \\
\gamma^{m_1}I_{k_1} & \gamma^{m_1}A_{1,2} & \gamma^{m_1}A_{1,3} & \cdots & \gamma^{m_1}A_{1,r} \\
\gamma^{m_2}I_{k_2} & \gamma^{m_2}A_{2,3} & \cdots & \gamma^{m_2}A_{2,r} \\
\vdots & \vdots & \ddots & \vdots \\
\gamma^{m_r}I_{k_{r-1}} & \gamma^{m_r}A_{r-1,2} & \gamma^{m_r}A_{r-1,3} & \cdots & \gamma^{m_r}A_{r-1,r}
\end{pmatrix},
\]

(16)

where \( 0 \leq m_0 < m_1 < \cdots < m_r-1 \) for some integer \( r \).

A code \( C \) with generator matrix of the form given in (16) is said to be of type

\[
\left( \gamma^{m_0} \right)^{k_0} \left( \gamma^{m_1} \right)^{k_1} \cdots \left( \gamma^{m_{r-1}} \right)^{k_{r-1}},
\]

where \( k = k_0 + k_1 + \cdots + k_{r-1} \) is called the rank, and is the rank of \( C \) as a module. A code \( C \) of length \( n \) with rank \( k \) over \( R_\infty \) is called a \( \gamma \)-adic \([n,k]\) code.

An MDR code over \( R_\infty \) is said to be MDS if it is of type \( 1^k \) for some \( k \). We have the following result.

**Lemma 2.5.** (See [12].) If \( C \) is a linear code over \( R_\infty \) then \( C^\perp \) has type \( 1^m \) for some \( m \). Furthermore, the following hold:

(i) \( C = (C^\perp)^\perp \) if and only if \( C \) has type \( 1^k \).

(ii) If \( C \) is an MDR or MDS code then \( C^\perp \) is an MDS code.

For two positive integers \( i < j \), we define a map as follows

\[
\Psi^j_i : R_j \to R_i,
\]

\[
\sum_{l=0}^{j-1} a_l \gamma^l \mapsto \sum_{l=0}^{i-1} a_l \gamma^l.
\]

(17)

(18)

If we replace \( R_j \) with \( R_\infty \) then we denote \( \Psi^\infty_i \) by \( \Psi_i \). It is easy to show that the maps \( \Psi^j_i \) and \( \Psi_i \) are ring morphisms.

**Definition 2.6.** An \([n,k]\) code \( \tilde{C} \) over \( R_j \) is said to be the lift of a code \( C \) over \( R_i \), with \( i \) and \( j \) integers such that \( 1 \leq i \leq j < \infty \), if \( \tilde{C} \) has a generator matrix \( \tilde{G} \) such that \( \Psi^j_i(\tilde{G}) \) is a generator matrix of \( C \).

Hence we have \( C = \Psi^j_i(\tilde{C}) \). If \( C \) is an \([n,k]\) \( \gamma \)-adic code, then for any \( i < \infty \) we call \( \Psi_i(C) \) a projection of \( C \). We denote \( \Psi_i(C) \) by \( C^i \).
Remark 2.7. The map $\Psi^j_i$ is the same map as that given in (1). Hence if $C$ is a cyclic code over $K$ generated by a polynomial $g$, then the code over $R_i$ generated by the lifted polynomial of $g$ is the lifted code $\bar{C}$ in the sense of the definition above.

Lemma 2.8. (See [12, Theorem 2.11].) Let $C$ be a $\gamma$-adic code. Then the following results hold:

(i) the minimum Hamming distance $d_H(C^i)$ of $C^i$ is equal to $d = d_H(C^1)$ for all $i < \infty$;
(ii) the minimum Hamming distance $d_\infty = d_H(C)$ of $C$ is at least $d = d_H(C^1)$.

Theorem 2.9. Let $C$ be a linear code over $R_i$, and $\bar{C}$ be a lift code of $C$ over $R_j$, where $i < j \leq \infty$. Then the following hold:

(i) If $C$ is a free code over $R_i$ then $\bar{C}$ is a free code $R_j$.
(ii) If $C$ is an MDS code over $R_i$ then the code $\bar{C}$ is an MDS code over $R_j$ with the same minimum distance $d_H$.

Proof. If $C$ is a free code of rank $k(C)$ over $R_i$, then $C$ is isomorphic as a module to $R_i^{k(C)}$. Hence the $k$ rows of the generators matrix $G$ of $C$ are linearly independent. Since the map $\Psi^j_i$ is a morphism, the rows of $\bar{C}$ are also linearly independent, otherwise the rows of $G = \Psi^j_i(\bar{C})$ are not linearly independent, which is absurd. It then follows that the code $\bar{C}$ is also a free code over $R_j$.

For part (ii), assume that $C$ is an MDS linear code of length $n$ and dimension $k$, so that $d_H = n - k + 1$. Let $v$ be a codeword of $C$ of minimum Hamming weight. We have that $\bar{C}$ is a linear code over $R_i$ with length $n$ and rank $k$. The vector $v$ can be viewed as a codeword of $\bar{C}$ since we can write $v = (v_1, \ldots, v_n)$ where

$$v_1 = d_0^i + d_1^i \gamma + \cdots + d_{i-1}^i \gamma^{i-1} + 0 \gamma^i + \cdots + 0 \gamma^{j-1} + \cdots.$$ 

Let $w$ be any lifted codeword of $v$. Then we have that $w_H(w) \geq w_H(v)$. On the other hand, for any lifted codeword $w'$ of $v'$, where $v' \in C$, we also have that $w_H(w') \geq w_H(v') \geq w_H(v)$. Hence by Lemma 2.8 we obtain that the minimum Hamming weight of $\bar{C}$ is $d_H$, and this implies that $\bar{C}$ is an MDR code for all $j > i$. From Proposition 2.2 we have that an MDS code is a free code. Hence $C$ is a free code, and by part (i) the lifted code $\bar{C}$ is also free. Thus $\bar{C}$ is an MDS code. $\square$

3. Codes over principal ideal rings

Let $R$ be a finite principal ideal ring. Then from the Chinese remainder theorem there exists a canonical $R$-module isomorphism $\Psi : R^n \to \prod_{i=1}^s (R/m_i^n)$. The ideals $m_1, m_2, \ldots, m_s$ are the maximal ideals of $R$. The ring $R/m_i^n$ is a finite chain ring with nilpotency index $t_i$.

For $i = 1, \ldots, s$, let $C_i$ be a code over $R/m_i^n$ of length $n$, and let

$$C = CRT(C_1, C_2, \ldots, C_s) = \Psi^{-1}(C_1 \times \cdots \times C_s) = \{\Psi^{-1}(v_1, v_2, \ldots, v_s) \mid v_i \in C_i\}.$$ 

The code $C$ is called the Chinese product of codes $C_1, C_2, \ldots, C_s$ [10].

Theorem 3.1. (See [10].) With the above notation, let $C_1, C_2, \ldots, C_s$ be codes of length $n$ with $C_i$ a code over $R_i$, and let $C = CRT(C_1, C_2, \ldots, C_s)$. Then we have

(i) $|C| = \prod_{i=1}^s |C_i|$;
(ii) $rank(C) = \max\{rank(C_i) \mid 1 \leq i \leq s\}$;
(iii) $C$ is a free code if and only if each $C_i$ is a free code of the same rank;
(iv) $d_H(CRT(C_1, C_2, \ldots, C_s)) = \min\{d(C_i)\}$;
(v) $C_1, C_2, \ldots, C_s$ are self-dual codes if and only if $C$ is a self-dual code.
Theorem 3.2. With the notation above, let $C_1, C_2, \ldots, C_s$ be such that each $C_i$ is a code over $R_i$, and $C = CRT(C_1, \ldots, C_s)$. Then the following hold:

(i) If $C$ is an MDS code, then $C$ is a free code;
(ii) $C$ is an MDS code if and only if the $C_i$ are MDS and have the same rank for each $i$.

Proof. For part (i), the proof is the same as for part (i) of Proposition 2.2. For part (ii), suppose $C$ is MDS. Hence from part (i), $C$ is free, and from Theorem 3.1(iii), the $C_i$ are free and have the same rank $k$. By Theorem 3.1(iv) and the Singleton bound, the $C_i$ are MDS. If the $C_i$ are MDS and have the same rank, then they have the same minimum distance. Then from Theorem 3.1(iii) and (iv), we have that $C$ is MDS. □

Now combining Theorem 3.2, Proposition 2.2, and Theorem 2.9, the following result is obtained.

Theorem 3.3. With the notation above, there exists an MDS code $C = CRT(C_1, \ldots, C_s)$ with rank $k$ over $R$ if and only if there exists an MDS code with the same dimension $k$ over all of the residue fields $R/m_i$.

Shankar [25] introduced the Reed–Solomon (RS) codes over $\mathbb{Z}_{p^e_i}$ as the Hensel lift of RS codes over fields. In the following we define RS codes over $\mathbb{Z}_{m_i}$.

Definition 3.4. Let $m = \prod_{i=1}^{s} p_i^{e_i}$. Then the Reed–Solomon code of minimum distance $d$ over $\mathbb{Z}_m$ is the linear code $C = CRT(C_1, \ldots, C_s)$ such that for all $1 \leq i \leq s$, $C_i$ is a Reed–Solomon code over $\mathbb{Z}_{p_i^{e_i}}$ with minimum distance $d$.

Proposition 3.5. With the notation above, the Reed–Solomon code defined over $\mathbb{Z}_m$ is an MDS code with minimum distance $d$.

Proof. From Theorem 2.9 each lifted code over $\mathbb{Z}_{p_i^{e_i}}$ is MDS with minimum distance $d$. Hence the result follows from Theorem 3.3. □

Example 3.6. There exists an MDS code (actually an RS code) over $\mathbb{Z}_{65}$ with length 4 and minimum distance $d = 2$. There is also a non-trivial RS code of length 6 over $\mathbb{Z}_{91}$ with minimum distance $d = 4$, and an MDS RS code of length 10 over $\mathbb{Z}_{141}$.

Remark 3.7. Dougherty et al. [10, Theorem 6.5] proved that if $R$ is a finite principal ideal ring such that all residue fields satisfy

$$|R/m_i| > \binom{n-1}{n-k-1}$$

for some integers $n, k$ with $n - k - 1 > 0$, then there exists an MDS $[n, k, n-k+1]$ code over $R$. This is only a sufficient condition on the existence of MDS codes over a principal ideal ring. For example, the last two RS codes given in Example 3.6 are MDS but do not satisfy (19).

4. Constacyclic codes over finite chain rings and formal power series

In this section, constacyclic codes are considered. Let $R$ be a finite chain ring and $R_i, i \leq \infty$ the corresponding lifts. For a given unit $\lambda_i \in R_i$, a code $C$ is said to be constacyclic, or more generally, $\lambda_i$-constacyclic, if $(\lambda_i c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$ whenever $(c_0, c_1, \ldots, c_{n-1}) \in C$. Cyclic and negacyclic codes correspond to $\lambda_i = 1$ and $-1$, respectively. When $i < \infty$ it is well known that the $\lambda_i$-constacyclic codes over $R_i$ correspond to ideals in $R_i[x]/(x^n - \lambda)$. We will prove that the same holds for codes
over $R_\infty$. For this, the maps $\Psi_1^i$ and $\Psi_i$ in (17) can be extended to maps from $R_i[x]$ to $R_i[x]$ and from $R_\infty[x]$ to $R_i[x]$, respectively. In particular, for $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R_i[x]$, we have $\Psi_i^1(f(x)) = \Psi_i^1(a_0) + \Psi_i^1(a_1)x + \cdots + h_i(a_n)x^n$, and $\Psi_i(f(x)) = \Psi_i(a_0) + \Psi_i(a_1)x + \cdots + \Psi_i(a_n)x^n$. In this way, the map defined in (1) is the same as $\Psi_i^1$ in the finite case and $\Psi_1$ in the infinite case.

Lemma 4.1. Let $\lambda_j$ be an arbitrary unit of $R_j$, $j \leq \infty$. Then $\Psi_i^1(\lambda_j)$ is a unit of $R_i$.

Proof. Follows from (13) and Lemma 2.3. □

For clarity of notation, we denote $\Psi_i^1(\lambda_j)$ by $\lambda_i$ and also $\Psi_i(\lambda_\infty)$ by $\lambda_i$ when there is no ambiguity.

Consider now the following ring

$$R_\infty[x]/\langle x^n - \lambda_\infty \rangle = \{ f(x) + \langle x^n - \lambda_\infty \rangle \mid f(x) \in R_\infty[x] \}.$$ 

Since $R_\infty$ is a domain, we have that

$$R_\infty[x]/\langle x^n - \lambda_\infty \rangle = \{ f(x) + \langle x^n - \lambda_\infty \rangle \mid \operatorname{deg} f(x) < n \text{ or } f(x) = 0 \}. \quad (20)$$

Define the map $P_{\lambda_\infty}$ as follows

$$P_{\lambda_\infty} : R_\infty^n \to R_\infty[x]/\langle x^n - \lambda_\infty \rangle,$$

$$(a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + \langle x^n - \lambda_\infty \rangle. \quad (21)$$

Let $C$ be an arbitrary subset of $R_\infty^n$ and $P_{\lambda_\infty}(C)$ the image of $C$ under the map $P_{\lambda_\infty}$. Then we have

$$P_{\lambda_\infty}(C) = \{ (c_0 + c_1x + \cdots + c_{n-1}x^{n-1} + \langle x^n - \lambda_\infty \rangle \mid (c_0, c_1, \ldots, c_{n-1}) \in C \}. \quad (22)$$

Hence we obtain from (20) and (21) that a linear code $C$ of length $n$ over $R_\infty$ is a $\lambda_\infty$-constacyclic code if and only if $P_{\lambda_\infty}(C)$ is an ideal of $R_\infty[x]/\langle x^n - \lambda_\infty \rangle$.

Let $P_1 \subseteq R_i$, $i \leq \infty$ be a non-zero ideal. Then $P_1$ is called a prime ideal (resp. primary ideal), if it satisfies $ab \in P_1 \Rightarrow a \in P_1$ or $b \in P_1$ (resp. $ab \in P_1 \Rightarrow a \in P_1$ or $b^k \in P_1$), for some positive integer $k$.

A polynomial $f(x)$ over a chain ring $R_i$ is said to be basic irreducible if $\Psi_i^1(f)$ is irreducible in $K[x]$, where $K$ is the residue field of $R_i$. A polynomial in $R_i[x]$ is called regular if it is not a zero divisor. Hence from (13) we have that $f \in R_i[x]$ is regular if and only if $\Psi_i^1(f) \neq 0$.

Lemma 4.2 (Hensel’s Lemma). (See [21, Theorem XIII.7].) Let $i < \infty$ and $f$ be a polynomial over $R_i$. Assume $\Psi_i^1(f) = g_1g_2 \cdots g_r$ where $g_1, g_2, \ldots, g_r$ are pairwise coprime polynomials over $K$. Then there exist pairwise coprime polynomials $f_1, f_2, \ldots, f_r$ over $R_i$ such that $f = f_1f_2 \cdots f_r$ and $\Psi_i^1(f_j) = g_j$ for $j = 1, 2, \ldots, r$.

Theorem 4.3. Let $R_i$ be a finite chain ring with characteristic $p$ and $\lambda_i$ a unit of $R_i$. When $\gcd(n, p) = 1$, the polynomial $x^n - \lambda_i$ factors uniquely as a product of monic basic irreducible pairwise coprime polynomials over $R_i[x]$. Furthermore, there is a one-to-one correspondence between the set of basic irreducible polynomial divisors of $x^n - \lambda_i$ in $R_i[x]$ and the set of irreducible divisors of $\Psi_i^1(x^n - \lambda_i)$ in $K$.

Proof. Assuming $\gcd(n, p) = 1$, it must be that the componentwise reduction modulo $\gamma$ of $x^n - \lambda_i$, which is $\Psi_i^1(x^n - \lambda_i)$, is square free in $K[x]$. Hence by [7, Proposition 2.7] the polynomial $x^n - \lambda_i$ factors uniquely as a product of monic basic irreducible pairwise coprime polynomials $f_1 \cdots f_s$ over $R_i[x]$. Since $K$ is a field and hence $K[x]$ is a unique factorization domain, $\Psi_i^1(x^n - \lambda_i)$ has a unique factorization $h_1h_2 \cdots h_k$ into irreducible polynomials over $K$. These are pairwise coprime since $\gcd(n, p) = 1$. By Lemma 4.2, there exist polynomials $h_j$ in $R_i[x]$ such that $\Psi_i^1(h_j) = h_j$, and $x^n - \lambda_i = h_1 \cdots h_k$. Hence
the \( h_j \) are basic irreducible. From the fact that the decomposition of \( x^n - \lambda_j \) over \( R_i[x] \) is unique, we obtain that \( h_j = f_j \) and \( k = s \). \( \square \)

In the following we focus on constacyclic codes over \( R_\infty \) and the projections of these codes. Let

\[
\Psi_i : R_\infty[x]/(x^n - \lambda_\infty) \rightarrow R_i[x]/(x^n - \lambda_i),
\]

\[
f(x) \mapsto \Psi_i(f(x)).
\]

The map in (23) is a ring homomorphism. Thus if \( I \) is an ideal of \( R_\infty[x]/(x^n - \lambda_\infty) \), then \( \Psi_i(I) \) is an ideal of \( R_i[x]/(x^n - \lambda_i) \). This gives the following commutative diagram

\[
\begin{array}{ccc}
R_\infty^n & \xrightarrow{P_{\lambda_\infty}} & R_\infty[x]/(x^n - \lambda_\infty) \\
\downarrow{\Psi_i} & & \downarrow{\Psi_i} \\
R_i^n & \xrightarrow{P_{\lambda_i}} & R_i[x]/(x^n - \lambda_i).
\end{array}
\]

Hence we have the following theorem.

**Theorem 4.4.** The projection code \( \Psi_i(C) \) of a \( \lambda_\infty \)-constacyclic code \( C \) of \( R_\infty \) is a \( \lambda_i \)-constacyclic code over \( R_i \) for all \( i < \infty \).

**Proof.** Assume that \( C \) is a \( \lambda_\infty \)-constacyclic code over \( R_\infty \). Then \( P_{\lambda_\infty}(C) \) is an ideal of \( R_\infty[x]/(x^n - \lambda_\infty) \). By the homomorphism in (23) and the commutative diagram above, \( \Psi_i(P_{\lambda_\infty}(C)) = P_{\lambda_i}(\Psi_i(C)) \) is an ideal of \( R_i[x]/(x^n - \lambda_i) \). This implies that \( \Psi_i(C) \) is a \( \lambda_i \)-constacyclic code over \( R_i \) for all \( i < \infty \). \( \square \)

**Lemma 4.5.** Let \( C \) be a \( \lambda_j \)-constacyclic code over \( R_j \), \( j \leq \infty \), and \( C^\perp \) the dual code of \( C \). Then the code \( C^\perp \) is a \( \lambda_j^{-1} \)-constacyclic code over \( R_j \).

**Proof.** We have that \( \lambda_j \), \( j \leq \infty \), is a unit. Furthermore since \( i < \infty \) we have that \( R_i \) is a finite chain ring. From Lemma 2.3, \( R_\infty \) is a principal ideal domain. Hence the ideals of \( R_j \) are principal. The result then follows by a proof similar to that for constacyclic codes over a finite field. \( \square \)

**Theorem 4.6.** Let \( C \) be a \( \lambda_\infty \)-constacyclic code over \( R_\infty \) and \( C^\perp \) the dual code of \( C \). Then the code \( \Psi_i(C^\perp) \) is a \( \lambda_i^{-1} \)-constacyclic code, and if \( (C^\perp)^\perp = C \) then \( \Psi_i((C^\perp)^\perp) = \Psi_i(C^\perp) \) for all \( i < \infty \).

**Proof.** From Lemma 4.5 we have that \( C^\perp \) is a \( \lambda_\infty^{-1} \)-constacyclic code over \( R_\infty \). Hence from Theorem 4.4, the code \( \Psi_i((C^\perp)^\perp) \) is a \( \Psi_i(\lambda_i^{-1}) \)-constacyclic code for all \( i < \infty \). Then since \( \Psi_i \) is a ring homomorphism and the rings are with unity, we have \( \Psi_i(\lambda_i^{-1}) = \lambda_i^{-1} \). Hence the result follows. We next prove that \( \Psi_i(C^\perp) = \Psi_i(C_i)^{\perp} \) for all \( i < \infty \).

Let \( \nu \in \Psi_i(C^\perp) \) and let \( \omega \) be an arbitrary element of \( \Psi_i(C) \). Then there exist \( \nu' \in C^\perp \) and \( \omega' \in C \) such that \( \nu = \Psi_i(\nu') \) and \( \omega = \Psi_i(\omega') \). We have that \( \nu \cdot \omega = \Psi_i(\nu') \cdot \Psi_i(\omega') = \Psi_i(\nu' \cdot \omega') = \Psi_i(0) = 0 \). This implies that \( \Psi_i(C^\perp) \subseteq \Psi_i(C)^\perp \). By Lemma 2.5, \( C^\perp \) has type \( 1^{n-k} \). Since \( C = (C^\perp)^\perp \), by Lemma 2.5, this implies that \( C \) has type \( 1^k \). Hence \( \Psi_i(C) \) has type \( 1^{n-k} \) and \( \Psi_i(C)^\perp \) has type \( 1^{n-k} \). It was proven already that \( \Psi_i(C^\perp) \subseteq \Psi_i(C_i)^\perp \), and thus \( \Psi_i(C_i)^{\perp} = \Psi_i(C^\perp) \). \( \square \)

**Lemma 4.7.** Assume the notation given above and let \( P_i \) be an arbitrary prime ideal of \( R_i[x]/(x^n - \lambda_i) \), for \( i < \infty \). Then we have \( \gamma \in P_i \).
**Proof.** Let \( j \) be the least integer such that \( \gamma^j \not\in \mathcal{P}_1 \). Hence \( \gamma^{j-1} \in \mathcal{P}_1 \). Since \( \mathcal{P}_1 \) is prime, the hypothesis on \( j \) gives that \( \gamma^s \in \mathcal{P}_1 \) for all \( s \leq j-1 \), and so \( \gamma \in \mathcal{P}_1 \). \( \square \)

**Theorem 4.8.** Assume the notation given above. Then the prime ideals in \( R_i[x]/(x^\lambda - \lambda_i) \) are \( \langle \pi_i(x), \gamma \rangle \), where \( \pi_i(x) \) is a monic basic irreducible polynomial divisor of \( x^\lambda - \lambda_i \) over \( R_i \). If \( i = \infty \), then the ideals \( \langle \pi_1(x), \gamma \rangle \), where \( i \geq 1, i \in \mathbb{N} \), are also prime ideals of \( R_\infty[x]/(x^\lambda - \lambda_\infty) \).

**Proof.** For the finite case, let \( \mathcal{P}_1 \) be an arbitrary prime ideal in \( R_i[x]/(x^\lambda - \lambda_i) \). Since \( \Psi_i^1 \) is a ring homomorphism, \( \Psi_i^1(\mathcal{P}_1) \) is also a prime ideal in \( K[x]/(x^\lambda - \lambda_1) \). Since \( K \) is a field, any prime ideal in \( K[x]/(x^\lambda - \lambda_1) \) over \( K \) is of the form \( \langle \pi_1(x) \rangle \) [14, Theorem 3.10], where \( \pi_1(x) \) is a monic irreducible divisor of \( x^\lambda - \lambda_1 \) over \( K \). Hence \( \Psi_i^1(\mathcal{P}_1) = \langle \pi_1(x) \rangle \), and \( \pi_1(x) \in \langle \pi_i(x), \gamma \rangle = \mathcal{P}_i \). By Lemma 4.2, there exists \( \pi_i(x) \in \mathcal{P}_1 \) such that \( \Psi_i^1(\pi_1(x)) = \pi_1(x) \), where \( \pi_1(x) \) is a monic basic irreducible divisor of \( x^\lambda - \lambda_i \) over \( R_i \). Since \( i < \infty \), by Lemma 4.7 we have that \( \gamma \in \mathcal{P}_1 \). This implies that \( \langle \pi_i(x), \gamma \rangle \subseteq \mathcal{P}_1 \).

For \( i = \infty \) and \( \gamma \not\in \mathcal{P}_1 \), the only possibility is \( \mathcal{P}_1 = \langle \pi_1(x) \rangle \). \( \square \)

**Theorem 4.9.** Every prime ideal \( \mathcal{P}_1 = \langle \pi_1(x), \gamma \rangle \) in \( R_i[x]/(x^\lambda - \lambda_i) \) contains an idempotent \( e_i(x) \) with \( e_i(x)^2 = e_i(x) \), and \( \mathcal{P}_1 = \langle e_i(x), \gamma \rangle \). Furthermore if \( i = \infty \), then every prime ideal \( \mathcal{P}_1 = \langle \pi_\infty(x) \rangle \) of \( R_\infty[x]/(x^\lambda - \lambda_\infty) \) has an idempotent generator.

**Proof.** We establish the first assertion by induction. Let \( K \) be the residue field of characteristic \( p \) of \( R_i \). Then since we can apply the Euclidean algorithm over \( K[x] \), by a proof similar to that for the cyclic case in [20, Ch. 8, Theorem 1], we have that every ideal \( \mathcal{P}_1 \) in \( K[x]/(x^\lambda - \lambda_1) \) contains an idempotent \( e_1 \) such that \( \mathcal{P}_1 = \langle e_1 \rangle \). Let \( \langle \Psi_i^1(\pi_1(x)), \gamma \rangle \) be the projection of \( \mathcal{P}_1 = \langle \pi_1(x), \gamma \rangle \) onto \( R_i[x]/(x^\lambda - \lambda_i) \). Suppose \( e_1(x) \in \langle \Psi_i^1(\pi_1(x)), \gamma \rangle \) is an idempotent element with \( \langle e_1(x), \gamma \rangle = \langle \Psi_i^1(\pi_1(x)), \gamma \rangle \). Then we have that \( e_1^2(x) = e_1(x) + \gamma^l h(x) \) in \( R_{i+1}[x]/(x^\lambda - \lambda_{i+1}) \) for some \( h(x) \in R_{i+1}[x]/(x^\lambda - \lambda_{i+1}) \).

In the following, we show that \( e_{i+1}(x) = e_i(x) + \gamma^l \theta(x) \) is an idempotent element by choosing a suitable \( \theta(x) \). We have that

\[
e_{i+1}^2(x) \equiv (e_i(x) + \gamma^l \theta(x))^2 = e_i^2(x) + 2\gamma^l \theta(x)e_i(x) \pmod{\gamma^{i+1}}
\]

\[
= e_i(x) + \gamma^l h(x) + 2\gamma^l \theta(x)e_i(x) \pmod{\gamma^{i+1}}
\]

\[
= e_{i+1}(x) - \gamma^l \theta(x) + \gamma^l h(x) + 2\gamma^l \theta(x)e_i(x) \pmod{\gamma^{i+1}}
\]

\[
= e_{i+1}(x) + \gamma^l (h(x) - \theta(x)(1 - 2e_i(x))) \pmod{\gamma^{i+1}}.
\]

If \( p = 2 \), we can choose \( \theta(x) = h(x) \), and \( e_{i+1}(x) \) is an idempotent element. If \( p \neq 2 \), then \( (1 - 2e_i(x))^2 = 1 + 4\gamma^l h(x) \). This gives that \( (1 - 2e_i(x))^\infty \) is a unit. Then by choosing \( \theta(x) = h(x)(1 - 2e_i(x))^{-1} \), we get that \( e_{i+1}(x) \) is an idempotent element in \( R_{i+1}[x]/(x^\lambda - \lambda_{i+1}) \), and then \( \langle e_{i+1}(x), \gamma \rangle = \langle \pi_{i+1}(x), \gamma \rangle \).

Since \( \pi_\infty(x) \) and \( (x^\lambda - \lambda_\infty)/\pi_\infty(x) \) are relatively prime, there exist \( h(x), h'(x) \in R_\infty[x] \) such that

\[
h(x)\pi_\infty(x) + h'(x) \cdot (x^\lambda - \lambda_\infty)/\pi_\infty(x) = 1.
\]

This means that

\[
(h(x)\pi_\infty(x))^2 = h(x)\pi_\infty(x) - h'(x)h(x) \cdot (x^\lambda - \lambda_\infty),
\]

and hence

\[
(h(x)\pi_\infty(x))^2 \equiv h(x)\pi_\infty(x) \pmod{x^\lambda - \lambda_\infty}.
\]

Then \( h(x)\pi_\infty(x) \) is an idempotent element in \( R_\infty[x]/(x^\lambda - \lambda_\infty) \). \( \square \)
Theorem 4.10. Assume the notation given above. Then for \( i \leq \infty \), the primary ideals in \( R_i[x]/(x^\ell - \lambda_i) \) are \((0), (1), (\pi_i(x)), (\pi_i(x), \gamma^l)\), where \( \pi_i(x) \) is a basic irreducible divisor of \( x^\ell - \lambda_i \) over \( R_i \) and \( 1 \leq l < i \).

Proof. Let \( \mathcal{P}_i \) be a prime ideal of \( R_i[x]/(x^\ell - \lambda_i) \). Hence by Theorem 4.8, \( \mathcal{P}_i = (\pi_i(x), \gamma) \) and if \( i = \infty \), there is another case \( \mathcal{P}_i = (\pi_i(x)) \). It is obvious that these prime ideals are primary. Then the first class of primary ideals of \( R_i[x]/(x^\ell - \lambda_i) \) is the class of prime ideals given in Theorem 4.8. From the fact that \( (\gamma) \) is maximal in \( R_i, \mathcal{P}_i = (\pi_i(x), \gamma) \) is maximal in \( R_i[x]/(x^\ell - \lambda_i) \), but \( \mathcal{P}_i = (\pi_i(x)) \) is not maximal. By [26, Corollary 2, p. 153], we have that the powers of the maximal ideals are primary ideals. Let \( \mathcal{Q}_i \) be a primary ideal associated with the prime ideal \( \mathcal{P}_i = (\pi_i(x), \gamma) \). Then by [26, Ex. 2, p. 200], there is an integer \( k \) such that \( \mathcal{P}_i^k \subset \mathcal{Q}_i \subset \mathcal{P}_i \). From this, we obtain \( \mathcal{Q}_i = \mathcal{P}_i^l \), for some \( l \). Hence the primary ideals of \( R_i[x]/(x^\ell - \lambda_i) \) are \(( (\pi_i(x), \gamma)^l, (\pi_i(x)) \) from Theorem 4.9, we have that \( \mathcal{P}_i = (\pi_i(x), \gamma) = (e_i(x), \gamma), \) and \( e_i(x) \) is an idempotent of \( R_i[x]/(x^\ell - \lambda_i) \), so that \( \mathcal{P}_i^l = ( (\pi_i(x), \gamma)^l = (e_i(x), \gamma)^l \). Let \( a \in (e_i(x), \gamma)^l \), then there exist \( g_{l,i}(x), h_{l,i}(x) \in R_i[x], \) such that \( a = \prod_{l=1}^l e_i(x)g_{l,i}(x) + \gamma h_{l,i}(x) \). Since \( e_i(x)^2 = e_i(x), \) then \( a = e_i(x)G_i(x) + \gamma H_i(x) \) for some \( G_i(x), H_i(x) \in R_i[x] \). Hence the non-trivial primary ideals of \( R_i[x]/(x^\ell - \lambda_i) \) are \((\pi_i(x), \gamma^l)\). □

Theorem 4.11. Let \( \pi_i(x), 1 \leq l \leq b, i \in \mathbb{N}, \) denote the distinct monic irreducible divisors of \( x^\ell - \lambda_i \) over \( R_i \), with \( i \leq \infty \). Then any ideal in \( R_i[x]/(x^\ell - \lambda_i) \) can be written in a unique way as follows

\[
I = \prod_{l=1}^b (\pi_i^l(x), \gamma^{m_l}),
\]

where \( 0 \leq m_l \leq l \). In particular, if \( i \) is finite, then there are \((i + 1)^b\) distinct ideals.

Proof. Since \( R_i[x]/(x^\ell - \lambda_i) \) is Noetherian, from the Lasker–Noether decomposition Theorem [26, p. 209] any ideal in \( R_i[x]/(x^\ell - \lambda_i) \) has a representation as a product of primary ideals. From Theorem 4.10, we have that the primary ideals of \( R_i[x]/(x^\ell - \lambda_i) \) are \((\pi_i^l(x), \gamma^{m_l})\). Hence the result follows. In addition, if \( i \) is finite then there are \((i + 1)^b\) distinct ideals in \( R_i \). □

The following lemma is a generalization of Hensel’s Lemma.

Lemma 4.12. Let \( \lambda_i \) be a unit in a chain ring, \( i \leq \infty \). If \( h_1(x) \in K[x] \) is a monic irreducible divisor of \( x^\ell - \lambda_i \) such that \( K \) is the residue field of \( R_i \), then there is a unique monic irreducible polynomial \( h_1(x) \) which divides \((\psi_i^{-1}(x^\ell - \lambda_i) \) over \( R_i \) and is congruent to \( h_1(x) \) (mod \( \gamma \).

Proof. Let \( f(x) \) be the lift of \( h_1(x) \) over \( R_\infty \). If \( f(x) \) is reducible over \( R_\infty \) then there exist polynomials \( g(x), h(x) \) such that \( f(x) = g(x)h(x) \) and \( 0 \leq \deg(g(x)), \deg(h(x)) < \deg(f(x)) \). This implies that

\[
\psi_i(f(x)) = \psi_i(g(x)h(x)) = \psi_i(g(x))\psi_i(h(x)) = h_1(x).
\]

Since \( f(x) \) is monic, we have that \( 0 < \deg(\psi_i(g(x))), \deg(\psi_i(h(x))) < \deg(\psi_i(f(x))) = \deg(h_1(x)) \). This is a contradiction. Since \( f(x) \) is irreducible, \( f(x) \) is a prime ideal of \( R_\infty \). In addition, \( f(x) \) must be a divisor of \( \psi_i^{-1}(x^\ell - \lambda_i) \), otherwise \( \psi_i(f(x)) = h_1 \) is not a divisor of \( x^\ell - \lambda_i \). Since \( f(x) \) is maximal in \( R_\infty[x]/(\psi_i^{-1}(x^\ell - \lambda_i)) \), \( f(x) \) is unique. If \( i < \infty \) the result follows from Theorem 4.3. □

Theorem 4.13. Let \( R_i \) be a chain ring \( i \leq \infty \), and \( C \) be a constacyclic code of length \( n \) over \( R_i[x]/(x^\ell - \lambda_i) \).

(i) If \( i < \infty \), then \( C \) is equal to

\[
\langle g_0(x), \gamma g_1(x), \ldots, \gamma^{i-1}g_{i-1}(x) \rangle,
\]

where the \( g_i(x) \) are divisors of \( x^\ell - \lambda_i \) and \( g_{i-1}(x) | \ldots | g_1(x) | g_0(x) \).
(ii) If $i = \infty$, then $C$ is equal to
\[
\{ y^{t_0} g_0(x), y^{t_1} g_1(x), \ldots, y^{t_{i-1}} g_{i-1}(x) \},
\]
where $0 \leq t_0 < t_1 < \cdots < t_{i-1}$ for some $l$ and $g_{l-1}(x) | \ldots | g_1(x) | g_0(x)$.

**Proof.** The results follow by expanding the products in Theorems 4.10 and 4.11. □

**Theorem 4.14.** Let $C$ be a constacyclic code over $R_i[x]$. If $i < \infty$, then there exists a unique family of pairwise coprime polynomials $F_0, \ldots, F_i$ in $R_i[x]$ such that $F_0 \cdots F_i = x^n - \lambda_i$ and $C = \langle \hat{F}_1 + y \hat{F}_2 + \cdots + y^i \hat{F}_i \rangle$, where $\hat{F}_j = x^{r - \lambda_i}$, for $0 < j < i$. Moreover
\[
|C| = |K| \sum_{j=0}^{i-1} (i-j) \deg F_{j+1}.
\]

**Proof.** The proof is similar to that for the cyclic case [7, Theorem 3.8]. □

**Corollary 4.15.** With the above notation, for $i \leq \infty$, every ideal in $R_i[x]/(x^n - \lambda_i)$ is principal.

**Proof.** For $i < \infty$, the result is given by Theorem 4.14.

For $i = \infty$, let $I$ be an ideal in $R_\infty[x]/(x^n - \lambda_\infty)$, with $\lambda_\infty$ a unit in $R_\infty$. Then $\Psi_j(I)$ is a principal ideal $\langle g_j \rangle$ of $R_j[x]/(x^n - \lambda_j)$ for all $0 < j < \infty$ from the first case. Using (15), we can define a $\gamma$-adic metric, since $R$ is finite. Hence by Tychonoff’s theorem [27], $R_\infty$ is compact and then $R_\infty[x]/(x^n - \lambda_\infty)$ is also compact with respect to this metric. Hence the sequence $\{g_j\}$ has a subsequence which converges to a limit $g$, which gives the result. □

Now we consider free constacyclic codes as free linear codes over the finite chain rings defined in Section 2.

**Theorem 4.16.** Let $C$ be a $\lambda_i$-constacyclic code of length $n$ over a finite chain ring $R_i$, with characteristic $p$ such that $\gcd(p, n) = 1$. Then $C$ is a free constacyclic code with rank $k$ if and only if there is a polynomial $f(x)$ such that $f(x)/(x^n - \lambda_i)$ generates $C$. In this case, we have $k = n - \deg(f)$.

**Proof.** Let $f(x)$ be a polynomial of degree $r$ such that $f(x)/(x^n - \lambda_i)$, and $C = \langle f(x) \rangle$ be the constacyclic code generated by $f(x)$ such that $\deg f = r$. Assume that $f_0$ and $f_r$ are the constant and leading coefficients of $f$, respectively. Then $f_0$ and $f_r$ are units in $R_i$, since $x^n - \lambda_i$ is monic and $\lambda_i$ is a unit. Let $B = \{ f(x), xf(x), \ldots, x^{n-r-1}f(x) \}$. We will prove that $B$ is a basis for $C$. First, it is established that the vectors are independent. Suppose
\[
\alpha_0 f(x) + \cdots + \alpha_{n-r-1} x^{n-r-1} f(x) = 0,
\]
where $\alpha_0, \ldots, \alpha_{n-r-1} \in R$. By comparing coefficients, we have $\alpha_0 f_0 = 0$, but since $f_0$ is a unit, we obtain that $\alpha_0 = 0$. Hence (29) becomes
\[
\alpha_1 f(x) + \cdots + \alpha_{n-r-1} x^{n-r-1} f(x) = 0.
\]
Again by comparing the coefficients we obtain $\alpha_1 f_0 = 0$, which gives that $\alpha_1 = 0$. We finally obtain $\alpha_0 = \cdots = \alpha_{n-r-1} = 0$, and therefore the vectors of $B$ are linearly independent.

Now we prove that $B$ spans $C$. Let $c(x) \in \langle f(x) \rangle$. Then there is a polynomial $g(x) \in R[x]$ such that $c(x) = g(x) f(x)$, where $\deg g \leq n - 1$. If $\deg g(x) \leq n - r - 1$, then $c(x) \in \text{span}(B)$. Otherwise, since $f$ is a regular polynomial (divisor of $x^n - \lambda_i$ with $\gcd(n, p) = 1$), then by [21, Exercise XIII.6] there are polynomials $p(x), q(x)$ such that
\[ g(x) = \frac{x^n - \lambda_i}{f(x)} p(x) + q(x), \]  

where \( \deg q(x) \leq n - r - 1 \). Now multiplying (31) by \( g(x) \) gives

\[ f(x)g(x) = f(x)q(x). \]

Hence \( c(x) \in \text{span}(B) \), which gives that the code \( C \) is a free \( R \) module.

In order to prove the converse, suppose that \( C = (\hat{F}_1 + \gamma \hat{F}_2 + \cdots + \gamma^{i-1} \hat{F}_i) \) is a free code of rank \( k \). Hence \( C \) has a basis of cardinality \( k \). Consider now the polynomial \( F = \hat{F}_1 + \gamma \hat{F}_2 + \cdots + \gamma^{i-1} \hat{F}_i \). We prove that \( \deg F = n - k \). Let \( s = n - \deg F \) and \( \Psi_1(C) = \text{Tor}_0(C) \). Then from (10) we have that \( |\Psi_1(C)| = p^r \). On the other hand, the image \( \Psi_1(F) \) of \( F \) modulo \( \gamma \) is a generator of \( \Psi_1(C) \). This implies that \( x^s \Psi_1(F(x)) \), and any power \( x^i \Psi_1(F(x)) \), \( l \geq s \), can be written as a linear combination of \( \{\Psi_1(F(x)), x\Psi_1(F(x)), \ldots, x^{s-1}\Psi_1(F(x))\} \). This set is also independent and hence is a basis of \( \Psi_1(C) \), which gives that \( |\Psi_1(C)| = p^s \), so that \( k = s = n - \deg F \). By equating (4) and (28), we have that each \( k_j = \deg \hat{F}_{j+1} \) for some \( j_i \in (0, i - 1) \). Hence from (6) we have \( k = \sum k_j = \sum \deg \hat{F}_{j+1} = n = n - \deg F \), which is possible if and only if \( k_j = 0 \) for \( i > 0 \), so that \( k = k_0 = n - \deg F \). \( \square \)

**Theorem 4.17.** Let \( R_i \), \( i \leq \infty \), be a chain ring and \( K \) its residue field. Let \( C \) be a \( \lambda_1 \)-constacyclic MDS code of length \( n \) over \( K \). Then there is a unique MDS code \( \tilde{C} \) over \( R_i \) which is the lifted code of \( C \) over \( R_i \). \( \tilde{C} \) is a free constacyclic code with generator polynomial \( (\Psi_1^{-1}(g), a \text{ monic polynomial divisor of } (\Psi_1^{-1}(x^n - \lambda_1)) \), and \( d_H(\tilde{C}) = d_H(C) \).

**Proof.** By Theorem 2.9, the code \( \tilde{C} \) is MDS. Hence from Theorem 2.2 we have that the code is a free code, and from Theorem 4.16 \( \tilde{C} \) is generated by \( (\Psi_1^{-1}(g)) \), a divisor of \( (\Psi_1^{-1}(x^n - \lambda_1)) \). From Lemma 4.12, we have that \( (\Psi_1^{-1}(g)) \) is monic and unique. Furthermore, Theorem 2.9 and Lemma 2.8 give that \( d_H(\tilde{C}) = d_H(C) \). \( \square \)

**Theorem 4.18.** Let \( R_i \) be a finite chain ring with nilpotence index \( i \). Let \( C_{rp}(n) \) be the number of \( rp \)-cyclotomic classes modulo \( n \) with \( \gcd(n, pr) = 1 \). Further, let \( \lambda_i \) be a unit in \( R_i \) such that \( \lambda_i^r = 1 \). Then the following hold:

(i) the number of constacyclic codes over \( R_i \) is equal to \( (i + 1)^{C_{rp}(n)} \);

(ii) the number of free constacyclic codes over \( R_i \) is equal to \( 2^{C_{rp}(n)} \).

**Proof.** It follows from Theorem 4.11 that the number of constacyclic codes over \( R_i \) is equal to \( (i + 1)^s \). By Theorem 4.3, the number \( s \) is equal to the number of irreducible polynomials in the factorization of \( x^n - \lambda_1 \) over \( K \), which is also equal to the number of \( rp \)-cyclotomic classes modulo \( n \). Part (ii) follows from Theorem 4.16 and part (i). \( \square \)

5. MDS self-dual codes from cyclic and negacyclic codes

The following result was given in [15, Theorems 11, 12].

**Lemma 5.1.** Let \( n \) be an even integer and \( q \) an odd prime power. Then there exist MDS negacyclic codes over \( \mathbb{F}_q \) which are self-dual codes in the following cases:

(i) \( n = 2n' \) with \( n' \) odd \( q \equiv 1 \) (mod 4), and \( n|q + 1 \);

(ii) \( n = 2^a n' \) with \( n' \) odd, \( q \equiv 1 \) (mod \( 2^{a+1}n' \)), and \( n|q - 1 \).

Let \( q = p \) be an odd prime and \( n \) an even integer as in Lemma 5.1. Then there exists a negacyclic MDS self-dual code of length \( n \) over \( \mathbb{Z}_p \). Assume now that \( K \) is a finite field such that \( |K| = p \). Then codes exist which are isomorphic to those given by Lemma 5.1. From Theorem 4.17, these codes
Table 1
Some self-dual MDS codes of length \( n \) over \( \mathbb{Z}_m \).

<table>
<thead>
<tr>
<th>( n )</th>
<th>( m )</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>3, 7, 13, 17, 21, 23, 39, 49, 91</td>
</tr>
<tr>
<td>6</td>
<td>5, 5², 13, 41, 65, 13², 205</td>
</tr>
<tr>
<td>8</td>
<td>5, 7, 11, 13, 17, 25, 49, 65, 77, 91, 11²</td>
</tr>
<tr>
<td>10</td>
<td>9, 13, 17, 81, 89, 117, 13²</td>
</tr>
<tr>
<td>12</td>
<td>11, 19, 23, 29, 11², 67, 209, 19², 261</td>
</tr>
<tr>
<td>14</td>
<td>13, 13², 377</td>
</tr>
<tr>
<td>16</td>
<td>11, 17, 23, 11², 143, 187</td>
</tr>
<tr>
<td>18</td>
<td>17, 19, 53, 137, 17², 323, 19²</td>
</tr>
<tr>
<td>20</td>
<td>19, 41, 19², 779</td>
</tr>
</tbody>
</table>

are lifted to MDS negacyclic codes over \( R_i \) if \( i < \infty \). For \( i = \infty \), the lifted codes are also MDS by Theorem 2.9 and negacyclic by Lemma 4.12. From [12], these lifted codes are also self-dual. Hence we have the following result.

**Theorem 5.2.** Let \( n \) be an even integer and \( p \) an odd prime such that \( \gcd(n, p) = 1 \). Let \( R_i, i \leq \infty \), be a chain ring with residue field \( K \) such that \( |K| = p \). Then there exists an infinite family of negacyclic codes over \( R_i \) which are MDS and self-dual in the following cases:

- (i) \( n = 2n' \) with \( n' \) odd, \( p \equiv 1 \pmod{4} \), and \( n|p + 1 \);
- (ii) \( n = 2^a n' \) with \( n' \) odd, \( p \equiv 1 \pmod{2^a + 1} \), and \( n|p - 1 \).

In [15, Theorem 7], the following existence results for MDS self-dual codes over \( \mathbb{F}_q \) were given.

**Lemma 5.3.** There exist \( [n + 1, \frac{n+1}{2}, \frac{n+3}{2}] \) MDS self-dual codes which are extended odd-like duadic codes \( \tilde{D}_i \) in the following cases:

- (i) \( q = r^t \) with \( r \equiv 3 \pmod{4} \), \( t \) odd and \( n = p^m \), with \( p \) a prime such that \( p \equiv 3 \pmod{4} \) and \( m \) odd;
- (ii) \( q = r^t \) with \( t \) odd, \( p \) a prime such that \( r \equiv p \equiv 1 \pmod{4} \) and \( n = p^m \).

Now we prove the existence of an infinite family of MDS self-dual codes over \( \mathbb{Z}_m \).

**Theorem 5.4.** Let \( n \) be an even integer, \( m = \prod_{i=1}^{s} p_i^{e_i} \), and \( p_i \) such that \( n \) divides \( p_i - 1 \) for all \( 1 \leq i \leq s \). Then there exist MDS self-dual codes over \( \mathbb{Z}_m \) derived from the extended duadic codes over \( \mathbb{Z}_{p_i} \) in the following cases:

- (i) \( n \equiv 0 \pmod{4} \) and \( p_i \equiv 3 \pmod{4} \), for all \( 1 \leq i \leq s \);
- (ii) \( n \equiv 2 \pmod{4} \) and \( p_i \equiv 1 \pmod{4} \), for all \( 1 \leq i \leq s \).

**Proof.** From the above conditions and Lemma 5.3, we have the existence of MDS self-dual codes over \( \mathbb{Z}_{p_i} \) for all \( 1 \leq i \leq s \). Hence from Theorem 2.9, these MDS codes over \( \mathbb{Z}_{p_i} \) can be lifted to MDS codes over \( \mathbb{Z}_{p_i^j}, j > 1 \). Theorem 3.2 proves that MDS codes exist over \( \mathbb{Z}_m \). From [12] the lift of a self-dual code is also self-dual, thus from Theorem 3.1 these codes are also self-dual. \( \square \)

In Table 1, we give examples of self-dual MDS codes over \( \mathbb{Z}_m \) obtained using the results above. Codes over fields from [2,15,19] were also used to obtain these codes. This table shows that there exist many MDS self-dual codes which do not satisfy the inequality (19).
Acknowledgments

The authors would like to thank Steven Dougherty for his helpful comments, in particular for motivating the results in Section 4, and also the reviewers for useful comments which improved the paper considerably.

References