Lifted codes and lattices from codes over finite chain rings

Reguia Lamia Bouzara1 · Kenza Guenda1 · Edgar Martínez-Moro2

Received: 11 July 2020 / Accepted: 11 February 2022 / Published online: 25 March 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
In this paper we give the generalization of lifted codes over any finite chain ring. This has been done by using the construction of finite chain rings from \( p \)-adic fields. Further we propose a lattice construction from linear codes over finite chain rings using lifted codes.

Keywords Codes over rings · Lifted codes · Lattices

Mathematics Subject Classification 94B05 · 06B05

1 Introduction

Codes over finite rings have received significant attention in recent decades. Several authors have studied these codes due to their relationship with lattices construction, among other properties. The class of \( p \)-adic codes was introduced in [1]. Calderbank and Sloane investigated codes over \( p \)-adic integers and studied lifts of codes over \( \mathbb{F}_p \) and \( \mathbb{Z}_p^r \).

Lifted codes over finite chain rings were studied in [3], however this study was restricted to the finite chain rings of the form \( \mathbb{F}_q[t]/\langle t^k \rangle \) as pointed out by the reviewer in [13]. Later, Young Ho generalized the construction of cyclic lifted codes for arbitrary finite fields to codes over Galois rings \( GR(p^e, r) \) in [11].

In [13], the reviewer stated that a unified treatment valid for all chain rings would certainly be desirable. Therefore, this study investigates the structure of finite chain rings as non-trivial quotient of ring integers of \( p \)-adic fields to generalize the construction in [3].

E. Martínez-Moro was supported in part by Grant PGC2018-096446-B-C21 funded by MCIN/AEI/10.13039/501100011033 and by “ERDF A way of making Europe”.

Edgar Martínez-Moro
edgar.martinez@uva.es

Reguia Lamia Bouzara
rbouzara@usthb.dz

Kenza Guenda
kguenda@usthb.dz

1 Faculty of Mathematics USTHB, University of Science and Technology of Algiers, Algiers, Algeria

2 Institute of Mathematics, University of Valladolid, Valladolid, Spain
A finite commutative chain ring is a finite local ring whose maximal ideals are principal. Any finite chain ring can be constructed from \( p \)-adic fields (see for example [5]) as follows: let \( K \) be a finite extension of the field of \( p \)-adic numbers \( \mathbb{Q}_p \) with residue degree \( r \) and ramification index \( s \), let \( \mathcal{O}_K \) be the ring of integers of \( K \) and let \( \pi \) be a prime of \( K \). Then \( \mathcal{O}_K / \pi^{(n-1)s+r} \) is a finite commutative chain ring with invariants \((p, n, r, s, t)\). Further every finite commutative chain ring can be obtained in this way.

This paper uses the definition of chain rings as non-trivial quotient of ring integers of \( p \)-adic fields to provide a general and a unified treatment of lifted codes for any finite chain ring. Then this definition allows to introduce a general construction of lifted cyclic codes that can be used to lift codes over finite fields \( \mathbb{F}_p \) to codes over finite chain rings. Thus the lifted codes are used to give a general construction \( A \) of lattices from codes over finite chain rings that generalizes the construction of lattices in [7].

The structure of the paper is as follows: Section 2 introduces the \( p \)-adic fields and their extensions and it describes the connection between \( p \)-adic fields and the construction of a finite chain ring. In Section 3 we propose a unified treatment for lifted codes which is valid for all chain rings. Based on that fact, the construction of lifted codes is generalized. Section 4 provides some definitions of lattices over \( p \)-adic integers showing a lattice construction over finite chain rings from codes and its properties and we propose also a particular constructions of lattices that can be used to construct self-dual codes over finite chain rings.

## 2 Preliminaries

### 2.1 \( p \)-adic fields

The results presented in this section can be found in [6, 12]. Let \( p \) be a prime number and let \( x \) be an element of the rational field \( \mathbb{Q} \), then \( x \) can be written in a unique way as \( x = p^a m/n \), where \( m' \in \mathbb{Z}^* \) and \( n' \in \mathbb{N}^* \), and both \( m' \) and \( n' \) are not divisible by \( p \). The \( p \)-adic valuation \( v_p(x) \) of \( x \in \mathbb{Q} \) is defined as:

\[
v_p(x) = \begin{cases} +\infty & \text{if } x = 0 \\ a & \text{if } x = p^a m'/n', p \nmid m' \cdot n' \end{cases}
\]

and the \( p \)-adic norm (which is an ultra-metric absolute value) is given by: \( |x|_p = p^{-v_p(x)} \). The completion of \( \mathbb{Q} \) by the absolute value \( | \cdot |_p \) is the field of \( p \)-adic numbers and is denoted as usual by \( \mathbb{Q}_p \). In order to keep our notation simpler we will denote \( v_p \) by \( v \). Next proposition characterizes the field \( \mathbb{Q}_p \) as follows:

**Proposition 1** If \( v \) and \( \mathbb{Q}_p \) are defined as above then:

1. The set \( \mathbb{Z}_p = \{ a \in \mathbb{Q}_p ; v(a) \geq 0 \} = \{ a \in \mathbb{Q}_p ; |a| \leq 1 \} \) is a unitary ring called the valuation ring or the ring of integers of \( \mathbb{Q}_p \).
2. \( \mathbb{Q}_p = \mathcal{F}(\mathbb{Z}_p) \) is the fractions field of \( \mathbb{Z}_p \).
3. The set \( \mathfrak{m} = \{ a \in \mathbb{Q}_p ; v(a) > 0 \} = \{ a \in \mathbb{Q}_p ; |a| < 1 \} \), is the unique maximal ideal of \( \mathbb{Z}_p \) and it is generated by \( p \). The ideal \( \mathfrak{m} = \langle p \rangle \) is called the maximal ideal of the valuation \( v \).
4. The ring \( \mathbb{Z}_p \) is a local ring and the quotient ring \( \mathbb{Z}_p / \mathfrak{m} = \mathbb{F}_p \) is the finite field with \( p \) elements which is the residual field of the valuation \( v \). Further, we have that \( v(p) = 1 \) and \( p \) is a prime element in \( \mathbb{Z}_p \).

5. Let \( E \) be a complete set of representatives of the residue field \( \mathbb{F}_p = \mathbb{Z}_p / p \mathbb{Z}_p \) in \( \mathbb{Z}_p \) that is, a subset of \( \mathbb{Z}_p \) such that each residue class of \( \mathbb{Z}_p \) mod \( p \) contains a unique element in \( E \). We assume that 0 is the representative of \( p \) in \( E \). Let \( a \in \mathbb{Z}_p \), we may set \( E = \{ 1, \cdots, p - 1 \} \), then \( a \) can be expressed in a unique form \( a = \sum_{i=0}^{\infty} a_i p^i \), where \( a_i \in E = \{ 1, \cdots, p - 1 \} \). This is the well known p-adic expansion of \( a \).

Let \( K \) be an algebraic extension of \( \mathbb{Q}_p \) of degree \( n \) and \( x \in K \). The norm \( \text{N}_{K\lvert \mathbb{Q}_p}(x) \) is the endomorphism of the \( \mathbb{Q}_p \)-vector space \( K \) defined by multiplication by \( x \). Then the characteristic polynomial of this endomorphism is expressed as \( x^n + \cdots + (-1)^n \text{N}_{K\lvert \mathbb{Q}_p}(x) \) and \( x \) in \( K \) is a zero of it. In other words, \( x \) is an integer of \( K \) and \( \mathbb{Z}_p = \mathcal{O}_K \cap \mathbb{Q}_p \), where \( \mathcal{O}_K \) denotes the ring of integers of \( K \). Then, the relation given by

\[
\text{w}(x) = \frac{1}{n} \text{v}(\text{N}_{K\lvert \mathbb{Q}_p}(x)),
\]

defines the unique valuation \( \text{w} \) of \( K \) extending the valuation \( v \) of \( \mathbb{Q}_p \). Let \( u \) be the restriction of the valuation \( \text{w} \) to the elements in \( \mathbb{Q}_p \). The ramification index of \( K \lvert \mathbb{Q}_p \) is defined as follows:

\[
e = [\text{w}(K^*) : u(\mathbb{Q}_p^*)] = w(p),
\]

where \([w(K^*) : u(\mathbb{Q}_p^*)]\) is the group index.

**Proposition 2** Let \( K \) be an algebraic extension of \( \mathbb{Q}_p \) of degree \( n \). Then:

1. The ring of integers of \( K \) is given by \( \mathcal{O}_K = \{ a \in \mathbb{Q}_p \mid \text{v}(a) \geq 0 \} \). There exists an element \( \pi \in K \) such that \( w(\pi) = 1 \) and those elements \( \pi \) are called primes of \((K, w)\).
2. The maximal ideal of the ring \( \mathcal{O}_K \) is generated by a prime element \( \pi \) called the uniformizer, we will denote the maximal ideal of \( \mathcal{O}_K \) as \( \mathfrak{m}_K = \langle \pi \rangle \).
3. The residual field is \( \mathcal{O}_K / \mathfrak{m}_K = \mathbb{F}_p \). The residual field \( \mathbb{F}_p \) of \( v \) is naturally embedded in the residual field \( \mathbb{F}_p \) of \( \text{w} \). On the other hand \( f = f(w/v) = [\mathbb{F}_p^* : \mathbb{F}_p] \) where \([\mathbb{F}_p^* : \mathbb{F}_p]\) is the degree of the extension \( \mathbb{F}_p^* / \mathbb{F}_p \). Then we call \( f \) the inertial degree.
4. If \( p \) is an uniformizer of \( \mathbb{Q}_p \) and \( \pi \) is an uniformizer of \( K \), then

\[
|p|_p = |\pi|_p^e,
\]

where \( e \) is ramification index.
5. \([K : \mathbb{Q}_p] = n = ef\).
6. Let \( E' \) be a complete set of representatives of the residue field \( \mathbb{F}_p' = \mathcal{O}_K / \mathfrak{m}_K \) in \( \mathcal{O}_K \) containing 0. An element \( \alpha \) of \( \mathcal{O}_K \) can be written as \( \alpha = \sum_{i=0}^{\infty} a_i \pi^i \) where the \( a_i \)'s are elements of \( E' \).

Finally, the following theorem is a local version of the fact that if \( K \) is a number field. Hence, \( \mathcal{O}_K \) is a free \( \mathbb{Z}_p \)-module of rank \([K : \mathbb{Q}_p]\).
Theorem 1 The $\mathbb{Z}_p$-module $\mathcal{O}_K$ is free of rank $n = [K : \mathbb{Q}_p] = ef$. Moreover, if $\{a_1, \ldots, a_f\} \subset \mathbb{Z}_p$ is a set such that the reductions $\overline{a}_j$ generate $\mathbb{F}_p$ as an $\mathbb{F}_p$-vector space, then the set $\{a_j\pi_K^k\}$ where $0 \leq k \leq e$ and $1 \leq j \leq f$ is a $\mathbb{Z}_p$-basis of $\mathcal{O}_K$.

The proof of this theorem can be found in [6].

2.2 Chain rings and $p$-adic fields

A finite commutative chain ring is a finite commutative ring whose ideals form a chain under inclusion. A complete description and proofs of the basic facts of this type of rings can be found in [8].

Let $R$ be a finite chain ring of characteristic $p^n$ with maximal ideal $M$ and nilpotency index $s$, thus its residue field is $R/M = \mathbb{F}_p^e$ (the finite field with $p^e$ elements). Every finite chain ring can be written as $R = GR(p^n, r)(x)/\langle g, p^{n-1}x^s \rangle$, where $GR(p^n, r)$ is the Galois ring of size $p^{nr}$ and characteristic $p^n$ and $g = g(x)$ is an Eisenstein polynomial in $GR(p^n, r)[x]$ of degree $e$. The integers $(p, n, r, e, t)$ are called the invariants of the finite chain ring $R$. The ring $R$ can also be constructed from $p$-adic fields because finite commutative chain rings are the non-trivial quotients of rings of integers of $p$-adic fields [4, 5]. Next proposition summarizes the connection between $p$-adic fields and finite chain rings.

Proposition 3 [4] Let $K$ be a finite extension of $\mathbb{Q}_p$ such as $[K : \mathbb{Q}_p] = n$ with residue degree $r$ and ramification index $e$. Let $\mathcal{O}_K$ be the ring of integers of $K$ and $\pi$ a prime of $K$. Then

$$\mathcal{O}_K / \pi^s \mathcal{O}_K \cong GR(p^n, r)(x)/\langle g, p^{n-1}x^s \rangle.$$ 

2.3 Finite chain rings and lifted codes

A linear code $C \subseteq R^m$ of length $m$ over a finite chain ring $R$ is a submodule of $R^m$. The length $m$ is assumed to be not divisible by the characteristic of the residue field $R/M = \mathbb{F}_p^e$. A matrix $G$ with entries in $R$ is called a generator matrix for the code $C$ if its rows span $C$ and none of them can be written as an $R$-linear combination of other remaining rows of $G$.

The generator matrix is in standard form if it is written as follows (see [10])

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

(2)

where the columns are grouped into blocks of sizes $k_0, k_1, \ldots, k_{s-1}, m - \sum_{i=0}^{s-1} k_i$.

Definition 1 Let $C$ be a linear code with a generator matrix of the form given in (2). We say that $C$ is of type $1^{k_0} \pi^{k_1} (\pi^2)^{k_2} \cdots (\pi^{s-1})^{k_{s-1}}$.

It is clear that the size of the code is $|C| = |M| \sum_{i=0}^{s-1}(s-i)k_i$. The rank of the code $C$ is defined to be $k(C) = \sum_{i=0}^{s-1} k_i$. Both the type and the rank are invariants of the code. The linear code $C$
is free if its rank is equal to the maximum of the ranks of the free submodules of $C$. Then, the code $C$ is a free $R$-submodule which is isomorphic as a module to $R^k(G)$.

If we consider the standard inner product in $R^n$ given by $x \cdot y = \sum x_i \cdot y_i$, where $x, y \in R^n$. The dual code $C^\perp$ of $C$ is defined by $C^\perp = \{ x \in R^n \mid x \cdot y = 0 \text{ for all } y \in C \}$. If $C \subseteq C^\perp$, then the code $C$ is said to be self-orthogonal. If $C = C^\perp$, then the code $C$ is said to be self-dual.

### 2.4 Lattices over integers of $p$-adic fields

Let $L$ be a vector space of dimension $n$ over $\mathbb{Q}_p$ and let $\Lambda$ be a $\mathbb{Z}_p$-submodule of $L$ of finite rank associated by a non-degenerate bilinear form $b : \Lambda \times \Lambda \to \mathbb{Z}_p$. The pair $(\Lambda, b)$ is called an integral lattice over $L$. The dual lattice of $\Lambda$ over $L$ is given by

$$\Lambda^\ast = \{ y \in L : b(y, x) \in \mathbb{Z}_p, \forall x \in \Lambda \}.$$

The lattice $\Lambda$ is a unimodular lattice if $\Lambda = \Lambda^\ast$. If $\Lambda$ is a free lattice with a $\mathbb{Z}_p$-basis $\{x_1, \ldots, x_n \}$, then the matrix given by $G = ((x_i, x_j))_{ij}$ is the generator matrix corresponding to the lattice $\Lambda$. For an integral lattice $\Lambda$, the discriminant group is $d_\Lambda = \Lambda^\ast / \Lambda$. If $\Lambda$ is free, then the discriminant of $\Lambda$ denoted by $\text{disc}(\Lambda)$ is

$$\text{disc}(\Lambda) = \det(G) = \det((x_i, x_j))_{ij}.$$

The norm ideal of $\Lambda$ is the $\mathbb{Z}_p$-ideal generated by $\{b(x, x); x \in \Lambda \}$.

Now, let $K$ be a Galois extension over $\mathbb{Q}_p$ of degree $n$, $K$ can be seen as a $\mathbb{Q}_p$-vector space of dimension $n$. Let $\Omega$ be an algebraic closure of $\mathbb{Q}_p$. Since $K$ is a separable extension of $\mathbb{Q}_p$, there are $n$ distinct $\mathbb{Q}_p$-embeddings $\sigma_1, \ldots, \sigma_n$ from $K$ into $\Omega$. For an element $\alpha \in K$ the norm and the trace maps are given by

$$N_{K|\mathbb{Q}_p}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha), \quad \text{Tr}_{K|\mathbb{Q}_p}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha).$$

Note that the $\mathbb{Q}_p$-bilinear symmetric form that associates $(x, y) \in K \times K$ to the element $\text{Tr}_{K|\mathbb{Q}_p}(xy) \in \mathbb{Q}_p$ is non-degenerate.

The ring of integers $\mathcal{O}_K$ of the field $K$ can be considered as the set of those elements in $K$ which are integral over $\mathcal{O}_p$, then $\mathcal{O}_K$ can be written as

$$\mathcal{O}_K = \mathbb{Z}_p e_1 \oplus \cdots \oplus \mathbb{Z}_p e_n,$$

where $\{e_1, \ldots, e_n\}$ is a free basis of the $\mathbb{Z}_p$-module $\mathcal{O}_K$. Since for $\alpha \in \mathcal{O}_K$ we can write $\alpha e_i = \sum_{j=1}^n \alpha_{ij} e_j$, where $\alpha_{ij} \in \mathbb{Z}_p$, then $\text{Tr}_{K|\mathbb{Q}_p}(\alpha)$ is the trace of the $n \times n$ matrix $\alpha_{ij}$ and $\text{Tr}_{K|\mathbb{Q}_p}(\alpha) \in \mathbb{Z}_p$.

As $\mathcal{O}_K$ is a free $\mathbb{Z}_p$-module of rank $n$, with a basis $\{e_1, \ldots, e_n\}$ over $\mathbb{Z}_p$, then a generator matrix of the lattice is written as follows:

$$M = \begin{pmatrix}
\sigma_1(e_1) & \sigma_2(e_1) & \cdots & \sigma_n(e_1) \\
\vdots & \vdots & \ddots & \vdots \\
\sigma_1(e_n) & \sigma_2(e_2) & \cdots & \sigma_n(e_n)
\end{pmatrix}.$$
lattices which are the general framework for the construction $A$ of lattices. Before that we will introduce one further notion.

**Definition 2** A lattice $A \in \mathcal{O}_K$ is cyclic if $\text{rot}(x_1, \ldots, x_{n-1}, x_n) = (x_n, x_1, \ldots, x_{n-1})$ for every $(x_1, \ldots, x_{n-1}, x_n) \in A$, where $\text{rot}(x)$ is the rotational shift operator in $\mathcal{O}_K$.

### 2.5 $\mathbb{Z}_p$-ideal lattices

Let $I$ be an ideal of $\mathcal{O}_K$, note that $I$ is also an $\mathcal{O}_K$-submodule of $K$ different from $\{0\}$. The norm $N_{K|\mathbb{Q}_p}(I)$ of $I$ is defined as the $\mathbb{Z}_p$-submodule generated by $N_{K|\mathbb{Q}_p}(x)$ for all $x \in I$.

**Lemma 1** Let $I$ be an ideal of $\mathcal{O}_K$, then $N_{K|\mathbb{Q}_p}(I) = p^i$ for some $i > 0$.

**Proof** Since $\mathcal{O}_K$ is a principal ideal domain, then every ideal $I$ of $\mathcal{O}_K$ is of the form $I = \langle \pi^i \rangle$; $i > 0$, and $N_{K|\mathbb{Q}_p}(\langle \pi \rangle) = p$, then $N_{K|\mathbb{Q}_p}(\langle \pi^i \rangle) = (p^i)^i = p^i$.

The lattice $(I, b_I)$ associated to the ideal $I \subseteq \mathcal{O}_K$ is called an **ideal lattice**. We have an associated symmetric bilinear form $b_I : I \times I \to \mathbb{Z}_p$ by

$$b_I(x, y) = \text{Tr}_{K|\mathbb{Q}_p}(\alpha x y), \forall x, y \in I,$$

where $\alpha$ is an element in $K$ such that $\sigma_i(\alpha) > 0$ for all $i$. A generator matrix of $(I, b_I)$ is given by

$$G_I = \begin{pmatrix} \sqrt{\alpha_1 \sigma_1(u_1)} & \sqrt{\alpha_2 \sigma_2(u_1)} & \cdots & \sqrt{\alpha_n \sigma_n(u_1)} \\ \vdots & \vdots & \ddots & \vdots \\ \sqrt{\alpha_1 \sigma_1(u_n)} & \sqrt{\alpha_2 \sigma_2(u_n)} & \cdots & \sqrt{\alpha_n \sigma_n(u_n)} \end{pmatrix}$$

Its discriminant is (see [12]) $\text{disc}(A_I) = N_{K|\mathbb{Q}_p}(\alpha) \cdot N_{K|\mathbb{Q}_p}(I)^2 \cdot D_K$. Finally, a lattice $A$ in $\mathcal{O}_K^m$ is cyclic if $A$ is an ideal of $\mathcal{O}_K[x]/(x^m - 1)$ (see [2] for a proof).

### 3 Lifted codes over finite chain rings

Let $\pi$ be a uniformizer of the valuation ring $\mathcal{O}_K$. For each $i \leq n$ we define

$$R_i = \mathcal{O}_K / \pi^i \mathcal{O}_K = \{ a_0 + a_1 \pi + \ldots + a_{i-1} \pi^{i-1} \mid a_i \in E' \},$$

where $E'$ is a complete set of representatives of the residue field $\mathbb{F}_{p^r} = \mathcal{O}_K / \pi \mathcal{O}_K$ in $\mathcal{O}_K$ containing 0.

Since every finite chain ring is isomorphic to a nontrivial quotient of rings of integers of $p$-adic fields, then the ring $R_i$ is a finite chain ring with maximal ideal $\langle \pi \rangle$. The **ring of formal power series in $\pi$** with coefficient in a finite chain ring $R$ is defined to be

$$R[[\pi]] = \left\{ a(x) = \sum_{i=0}^{\infty} a_i \pi^i \mid a_i \in R \text{ for all } i \in \mathbb{N} \right\},$$
where addition and multiplication operators are defined as usual. We have that the uniformizer of the valuation ring $\mathcal{O}_K$ is the generator of the maximal ideal of the finite chain ring $R_i$, then:

**Theorem 2** The ring of formal power series in $\pi$ with coefficients in a nontrivial quotient rings of integers of $K$ is the ring of integers of $K$, that is $R_\infty = \mathcal{O}_K$.

**Proof** Every element $a \in \mathcal{O}_K$ can be written in a unique way as $a = \sum_{j=0}^\infty b_j\pi^j$ where $b_j \in E'$, then:

$$R_\infty = \left\{ \sum_{j=0}^\infty \left( \sum_{i=0}^\infty b_{ij}\pi^j \right) \pi^i \right\} = \left\{ \sum_{j=0}^\infty \left( \sum_{i+j=m} b_{ij} \right) \pi^i ; b_{ij} \in E' \right\}.$$  

Consider $a_s = \sum_{i+j=m} b_{ij}$ with $b_{ij} \in E'$, then $\sum_{i+j=m} b_{ij}$ with $b_{ij} \in E'$ is a finite sum. Therefore:

$$R_\infty = \left\{ \sum_s a_s\pi^s ; a_s \in E' \right\} = \mathcal{O}_K.$$  

The chain of ideals of $\mathcal{O}_K$ is given as (see [6])

$$\{0\} \subset \cdots \subset (\pi^m) \subset \cdots \subset (\pi^2) \subset (\pi) \subset (\pi^0) = \mathcal{O}_K.$$  

Thus $R_\infty$ satisfies the ascending chain condition, which means that $R_\infty = \mathcal{O}_K$ is a Noetherian ring. Moreover, it is an Euclidean domain (and therefore is a Dedekind domain). Indeed, if $a$ and $b \neq 0$ are in $R_\infty$, then there are $q$ and $r$ in $R_\infty$ such that $a = bq + r$ and either $r = 0$ or $f(r) < f(b)$, where $f$ is a function from $R_\infty$ to $\mathbb{Z}^+$.

Moreover, $V : R_\infty \to \mathbb{Z}^+$ is the function defined by $V(0) = 0$ and $V(r) = v(r)$ if $r \neq 0$.

If $v(a) \geq v(b)$, then $v(a/b) = v(a) - v(b) \geq 0$ and if $q = a/b \in R_\infty$, then $r = 0$. Thus, if $v(a) < v(b)$, then $q = 0$ and $r = a$.

A submodule $C$ of rank $k$ over $R_\infty$ is called $\pi$-adic code of length $m$ and rank $k$. Let $C$ be a nonzero linear code over $R_\infty$ of length $m$, then any generator matrix of $C$ is permutation-equivalent to a matrix of the following form

$$G = \begin{pmatrix} \pi^{m_0}I_{k_0} & \pi^{m_0}A_{0,1} & \pi^{m_0}A_{0,2} & \pi^{m_0}A_{0,3} & \cdots & \pi^{m_0}A_{0,z} \\ \pi^{m_1}I_{k_1} & \pi^{m_1}A_{1,0} & \pi^{m_1}A_{1,1} & \pi^{m_1}A_{1,2} & \cdots & \pi^{m_1}A_{1,z} \\ \pi^{m_2}I_{k_2} & \pi^{m_2}A_{2,0} & \pi^{m_2}A_{2,2} & \cdots & \pi^{m_2}A_{2,z} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \pi^{m_{z-1}}I_{k_{z-1}} & \pi^{m_{z-1}}A_{z-1,0} & \cdots & \cdots & \cdots & \pi^{m_{z-1}}A_{z-1,z} \end{pmatrix}. \tag{3}$$

The code $C$ with generator matrix of this form is said to be of type $(\pi^{m_0})^{k_0}(\pi^{m_1})^{k_1} \cdots (\pi^{m_{z-1}})^{k_{z-1}}$, where $k = k_0 + k_1 + \cdots + k_{z-1}$ is called its rank and $k_z = m - k$.

For two integers $i < j$, we define a map as in [3]:

$$\Psi^j_i : \begin{array}{ccc} R_j & \to & R_j \\ \sum_{l=0}^{j-1} a_l \pi^l & \mapsto & \sum_{l=0}^{i-1} a_l \pi^l. \end{array} \tag{4}$$

If $R_j$ is replaced with $R_\infty$, then $\Psi^\infty_i$ is denoted by $\Psi_i$. For any two elements $a, b \in R_\infty$ we have that $\Psi_i(a + b) = \Psi_i(a) + \Psi_i(b)$, $\Psi_i(ab) = \Psi_i(a)\Psi_i(b)$. The two maps $\Psi_i$ and $\Psi_i^j$ can be extended naturally from $R_\infty$ to $R_i$ and $R_j$ to $R_i$ respectively.
Remark 1 based on the above construction in (4) the following series of chain rings is obtained:

\[ R_\infty \rightarrow \cdots \rightarrow R_j \rightarrow \cdots \rightarrow R_s \rightarrow R_t \rightarrow \cdots \rightarrow R_1 \]

Note that \( R_1 = \mathcal{O}_K / \pi^i \mathcal{O}_K \cong \mathbb{F}_{p^i} \), \( R_t = \mathcal{O}_K / \pi^j \mathcal{O}_K \), \( R_{s-1} = \mathcal{O}_K / \pi^{s-1} \mathcal{O}_K \) and \( R_s = \mathcal{O}_K / \pi^s \mathcal{O}_K \).

The following definition gives the lifts of a code \( C \) over a finite chain ring which are defined in a similar way as described in [3] but using this more general setting.

Definition 3 Let \( i, j \) be two integers such that \( 1 \leq i \leq j < \infty \). An \([m, k]\)-code \( C_1 \) over \( R_i \) lifts to an \([m, k]\) code \( C_2 \) over \( R_j \), denoted by \( C_1 \leq C_2 \), if \( C_2 \) has a generator matrix \( G_2 \) where \( \Psi_i(G_2) \) is a generator matrix of \( C_1 \).

It can be proven (the proof in [3] can be followed in our general setting) that \( C_1 = \Psi_i(C_2) \).

If \( C \) is an \([m, k]\)-\( \pi \)-adic code, then for any \( i < \infty \), \( \Psi_i(C) \) will be called the projection of \( C \).

The lattice \( \Psi_i(C) \) is denoted by \( C^i \) and we have the following result:

Lemma 2 Let \( C \) be a linear code over \( R_i \) and \( \tilde{C} \) be the lifted code of \( C \) over \( R_j \), where \( i < j \leq \infty \). Hence if \( C \) is free over \( R_i \), then \( \tilde{C} \) is free over \( R_j \).

4 Lattices and codes over finite chain rings

4.1 Construction A of lattices

Let \( R = \mathcal{O}_K / \pi^i \mathcal{O}_K \) be a finite chain ring defined as in Section 2.2 and let \( C \) be a code over the ring \( R \) of length \( m \). We consider the map \( \Psi : \mathcal{O}_K \rightarrow R \) the reduction modulo the prime \( \pi^i \) given in Section 2.3 such that the preimage of \( C \) by \( \Psi \) is the lifted code of \( C \) over \( \mathcal{O}_K \).

Then, \( \Psi^{-1}(C) \) is an \( \mathcal{O}_K \)-module of finite rank (see Section 2.3) and since \( \Psi^{-1}(C) \) is a \( \mathbb{Z}_p \)-submodule, then a lattice can be described as follows:

Definition 4 Given a code \( C \) over the finite chain ring \( R = \mathcal{O}_K / \pi^i \mathcal{O}_K \) and the symmetric bilinear form \( b_C = \sum_{i=1}^{m} \text{Tr}_{K/\mathbb{Q}_p}(\alpha x_i \bar{y}_i) \) where \( \alpha \in \mathcal{O}_K \) the lattice \( \Lambda_c = (\Psi^{-1}(C), b_C) \) is defined as the preimage \( \Psi^{-1}(C) \) of \( C \) in \( \mathcal{O}_K^m \) together with the symmetric bilinear form \( b_C \).

Lemma 3 The lattice \( \Lambda_c = (\Psi^{-1}(C), b_C) \) is an integral lattice.

Proof Let \( x, y \in \mathcal{O}_K^m \), then \( \text{Tr}_{K/\mathbb{Q}_p}(x_i \bar{y}_i) \in \mathbb{Z}_p \) for all \( i = 1, \ldots, m \). Since \( \alpha \in \mathcal{O}_K \), then \( \text{Tr}(\alpha x_i \bar{y}_i) \) belongs to \( \mathbb{Z}_p \), thus, \( b_c(x, y) \in \mathbb{Z}_p \) and therefore, \( \Lambda_c \) is an integral lattice.

The dual lattice of \( (\Psi^{-1}(C), b_C) \) is the pair \( \Lambda_C^* = (\Psi^{-1}(C)^*, b_C) \) defined as follows:

\[ \Psi^{-1}(C)^* = \{x \in K^m : b_C(x, y) \in \mathbb{Z}_p, \forall y \in \Psi^{-1}(C) \}. \]

Let \( A \) and \( B \) be two finite \( \mathcal{O}_K \)-modules such that \( B \subset A \), then the quotient \( A/B \) is a module of finite rank. The invariant of \( A/B \) denoted by \( \chi(A/B) \) (see [12]) is a non-zero ideal of \( A \). The following statement is straightforward.
Proposition 4 Let \( \Lambda_C \) be the integral lattice defined above. The discriminant of \( \Lambda_C \) is

\[
\text{disc}(\Lambda_C) = N_{K/O_p}(\alpha)^m \cdot D_K^m \cdot N_{K/O_p}(\chi(\mathcal{O}_K/m))^2.
\]

If \( C \) is a free code, then the lifted code given as the preimage of \( C \) by \( \Psi \) is also free, thus \( \Psi^{-1}(C) \) is isomorphic as a module to \( \mathcal{O}_K^k \), where \( k = k(\Psi^{-1}(C)) \) is the rank of the lifted code of \( C \). Then, the following result follows.

Corollary 1 For a free code \( C \) the discriminant of \( \Lambda_C \) is

\[
\text{disc}(\Lambda_C) = D_K^m(p^r)^{2(m-k)}.
\]

If we let \( K \mid \mathbb{Q}_p \) be a Galois extension and the prime \(\pi\) is chosen so that \(\pi\) is totally ramified, therefore, we have \(n = e, f = 1, \) and \(\pi^n = p, \) and let \( C_i \) be a self-orthogonal code of length \(m\) over a finite chain ring \( R_i = \mathcal{O}_K/\pi^i \mathcal{O}_K. \) Then, we have the following result.

Lemma 4 The lattice formed by the lifted code of a self-orthogonal code \( C_i \) over \( R_i = \mathcal{O}_K/\pi^i \mathcal{O}_K \) is integral with respect to the bilinear form given by

\[
b_{C_i} = \sum_{i=1}^{m} \text{Tr}_{K/Q_p}(x_i \bar{y}_i/p).
\]

Proof Let \( x = (x_1, \ldots, x_m) \) and \( y = (y_1, \ldots, y_m) \) in \( \Lambda_C, \) then:

\[
\Psi(x \cdot y) = \Psi\left(\sum_{i=1}^{m} x_i y_i\right) = \sum_{i=1}^{m} \Psi(x_i)\Psi(y_i) = \Psi(x) \cdot \Psi(y) = 0.
\]

Since \( \Psi(x) \cdot \Psi(y) \in C \) and \( C \subset C_i^\perp, \) then:

\[
\sum_{i=1}^{m} x_i y_i = x \cdot y \equiv 0 \mod \pi^k.
\]

Since \( \pi \) is the only prime above \( p, \) all conjugates of \( \sum_{i=1}^{m} x_i y_i \) must lie in \( \pi \) and thus this is also true for its trace. In other words, \( \text{Tr}_{K/Q_p}(x_i \bar{y}_i) \in \pi^k, \) thus \( \text{Tr}_{K/Q_p}(x_i \bar{y}_i) \in p \mathbb{Z}_p. \) Therefore, by the linearity of the trace we have:

\[
\langle x, y \rangle = \sum_{i=1}^{m} \text{Tr}_{K/Q_p}(x_i \bar{y}_i/p) = \frac{1}{p} \cdot \text{Tr}_{K/Q}(\sum_{i=1}^{m} x_i \bar{y}_i)
\]

and \( \Lambda_C \) is integral.

Example 1 Let us consider lattices over integers of \( p \)-adic cyclotomic fields as follows. Let \( L \) be the field obtained from \( \mathbb{Q}_p \) by adjoining a \( p \)th root of unity \( \zeta, \) where \([L : \mathbb{Q}_p] = p - 1. \) The ring of integers of \( L \) is given by the set

\[
\mathcal{O}_L = \left\{ \alpha = \sum_{i=0}^{p-2} a_i \zeta^i ; \alpha_i \in \mathbb{Z}_p \text{ for } i = 0, 1, \cdots, p-2 \right\}.
\]
Note that the principal ideal of $\mathcal{O}_L$ is $m_L = \langle 1 - \zeta \rangle$. There exist $p - 1$ distinct embeddings $\sigma_i : L \to \mathbb{C}$, the trace of an element $a \in L$ over $\mathbb{Q}_p$ is $\text{Tr}_{L|\mathbb{Q}_p}(a) = \sum_{i=1}^{p-1} \sigma_i(a)$. Therefore, $\text{Tr}_{L|\mathbb{Q}_p}(a) \in \mathbb{Z}_{p'}$.

For $x \in \mathbb{Q}_p(\zeta) \bar{x}$ denotes the complex conjugate. We consider the symmetric bilinear form $(x, y) \mapsto \text{Tr}_{L|\mathbb{Q}_p}(x \bar{y})$.

Now, let $L$ be the subfield of $L$ such that $l = \mathbb{Q}_p(\zeta + \zeta^{-1})$ then $[L : l] = 2$ and $[l : \mathbb{Q}_p] = \frac{p-1}{2}$. Moreover, $\text{Tr}_{L|\mathbb{Q}_p}(x \bar{x}) = 2\text{Tr}_{l|\mathbb{Q}_p}(x \bar{x})$. This shows that the bilinear form above is even.

Finally, consider $C$ a code over the finite chain ring $R \simeq \mathcal{O}_L/(1 - \zeta)^i\mathcal{O}_L$. The lattice formed by the preimage of $C$ over $\mathcal{O}_L$ associated with the bilinear form $\text{Tr}_{L|\mathbb{Q}_p}$ is integral, because $\text{Tr}_{L|\mathbb{Q}_p}(x) \in \mathbb{Z}_p$ then is also even. Therefore, the lattice is unimodular.

### 4.2 The case of cyclic codes

A cyclic code of length $m$ over the ring of integers $\mathcal{O}_K$ is a linear code $C$ such that if $(c_0, c_1, \ldots, c_{m-1}) \in C$, then $(c_{m-1}, c_0, \ldots, c_{m-2}) \in C$. The codewords of a cyclic code over $\mathcal{O}_K$ are represented as usual by polynomials, more precisely they are the ideals of the ring $\mathcal{O}_K/(x^m - 1)$. We propose in this subsection a general construction of lifting cyclic codes which generalizes the construction given in [11]. This general construction allows to lift cyclic codes over finite fields $\mathbb{F}_{p^r}$ to finite chain rings and to the ring of integers $\mathcal{O}_K$ and the case of cyclic lattices will be treated. We will need the Hensel’s lemma for the construction. Its proof can be found in [9].

**Theorem 3** (Hensel’s Lemma) Let $K$ be a finite extension of $\mathbb{Q}_p$ of degree $n$, and let $\mathcal{O}_K$ be the ring of integers of $K$ with maximal ideal $M = \langle \pi \rangle$ and residue field $k := \mathcal{O}_K/\langle \pi \rangle$. Let $f \in \mathcal{O}_K[x]$ and let $\bar{f}$ be its image in $k[X]$. Let $\bar{g}$, $\bar{h}$ be two coprime polynomials of $k[x]$ such that $\bar{f} = \bar{g}\bar{h}$, then there exist $g, h \in \mathcal{O}_K[x]$ for which $f = gh$ and $g \equiv \bar{g}[\pi]$ and $h \equiv \bar{h}[\pi]$ with $\deg g = \deg \bar{g}$.

It is well known that if $C$ is a cyclic code of length $m$ over the finite field $\mathbb{F}_{p^r} = \mathcal{O}_K/\langle \pi \rangle$ then, $C$ is generated by a monic factor $g(x)$ of $x^m - 1 = \bar{g}(x)\bar{h}(x)$. Taking into account Hensel’s Lemma, any decomposition modulo $\pi$ can be generalized to a decomposition modulo $\pi^s$ by $x^m - 1 = g_s(x)\bar{h}(x)[\pi^s]$ and therefore to $\mathcal{O}_K$ as $x^m - 1 = g(x)h(x)$. If we consider now $C$ a cyclic code over a finite chain ring $R$ we have the following result.

**Theorem 4** Let $C$ be a cyclic code over $R$. The lattice $\Lambda_C = (\Psi^{-1}(C), b_C)$ is a cyclic lattice of $\mathcal{O}_K$.

**Proof** We have that a lattice $\Lambda$ in $\mathcal{O}_K^n$ is cyclic if $\Lambda$ is an ideal of $\mathcal{O}_K[x]/(x^n - 1)$, and since $\Psi^{-1}(C)$ is a cyclic code of $\mathcal{O}_K$, it means that $\Psi^{-1}(C)$ is an ideal of $\mathcal{O}_K[x]/(x^n - 1)$ then the lattice $\Lambda_C = (\Psi^{-1}(C), b_C)$ is cyclic.

**Corollary 2** Let $\Lambda_C = (\Psi^{-1}(C), b_C)$ be a cyclic lattice in $\mathcal{O}_K$, then $C$ is a cyclic code.

Thus we can construct cyclic codes over finite chain rings easily using cyclic lattices over $\mathcal{O}_K$.  

Springer
**Example 2** Let \( L = \mathbb{Q}_{p^r} \) be the unramified extension of \( \mathbb{Q}_p \) of degree \( r \) obtained by adjoining to \( \mathbb{Q}_p \) a primitive \((p^r - 1)\)st root of unity. The ring of integers of \( L \) is denoted by \( \mathcal{O}_L \), the maximal ideal is given by \( \mathfrak{m} = (p) \) and the residue field is \( \mathbb{F}_{p^r} \). Let \( \mathcal{C} \) be a cyclic code over \( \mathbb{F}_{p^r} = \mathcal{O}_L/(p) \), then \( \mathcal{C} \) is generated by a monic factor \( g_r(x) \) such that \( x^m - 1 = g(x)h(x) \). Using the Hensel’s Lemma any class of cyclic codes can be generalized from \( \mathbb{F}_{p^r} \) to \( \mathcal{O}_L \) by \( x^m - 1 = g(x)h(x) \). Then, the lattice formed by the lifted code of \( \mathcal{C} \) is a cyclic lattice over \( \mathcal{O}_L \).

### 4.3 Lattices over \( p \)-adic cyclotomic fields

Now, we propose the construction \( A \) from codes over finite chain rings to \( p \)-adic cyclotomic fields and their subfields using the same steps in Lemma 2 and Lemma 3 from [7]. This construction can be used to construct self-dual codes over finite chain rings.

Let \( p \) be an odd prime and let \( \zeta_{p^r} \) be the \( p^r \)th primitive root of unity. We consider \( L = \mathbb{Q}_p(\zeta_{p^r} + \zeta_{p^r}^{-1}) \) the subfield of the cyclotomic field \( L = \mathbb{Q}_p(\zeta_{p^r}) \). Hence the rings \( \mathcal{O}_L = \mathbb{Z}_p[\zeta_{p^r} + \zeta_{p^r}^{-1}] \) and \( \mathcal{O}_L = \mathbb{Z}_p[\zeta_{p^r}] \) are respectively their rings of integers. The prime \( p \) totally ramifies in \( L \) and the degree of \( L \) over \( \mathbb{Q}_p \) is \( [L : \mathbb{Q}_p] = \frac{p^r - 1}{2} (p - 1) \). Therefore \( p\mathcal{O}_L = \beta \mathbb{Z}_p \) and \( \beta \) is a principal prime ideal with generator \((1 - \zeta_{p^r})(1 - \zeta_{p^r}^{-1})\) with residue field \( \mathcal{O}_L/\pi \cong \mathbb{F}_{p^r} \).

Using the preceding facts and notations we can generalize the results on codes over finite fields in Corollary 2 from [7] to codes over finite chain rings.

**Lemma 5** Let \( L = \mathbb{Q}_p(\zeta_{p^r} + \zeta_{p^r}^{-1}) \) and let \( \mathcal{C} \) be a \( k \)-dimensional code over \( \mathbb{R}^n \) such that \( \mathcal{C} \subseteq \mathbb{C}_L \). The lattice \( (\Psi^{-1}(\mathcal{C}), b) \), where \( b = \sum_{i=1}^{m} \text{Tr}_{L/\mathbb{Q}_p}(a_i x_i) \) is integral of rank \( m \mathbb{p}^{r-1}(p - 1)/2 \). Using the same steps in [7], we get the same results over finite chain rings. A generator matrix of the lattice \( A_{\mathcal{C}} = (\Psi^{-1}(\mathcal{C}), b) \) is

\[
M_{A_{\mathcal{C}}} = \frac{1}{\sqrt{p}} \begin{pmatrix}
I_k \otimes M & A \otimes M
\end{pmatrix}
\]

where \( G = \left[ I_{n-1} \right] \) is a generator matrix of \( \mathcal{C} \). The ring of integers \( \mathcal{O}_L = \mathbb{Z}_p[\zeta_{p^r} + \zeta_{p^r}^{-1}] \) has \( \{ \zeta_{p^r} + \zeta_{p^r}^{-1} \}_{i=0} \) as a \( \mathbb{Z}_p \)-basis and the principal ideal \( \pi \) is generated by \( 2 - \zeta_{p^r} - \zeta_{p^r}^{-1} \).

**Lemma 6** (See [7]) Let \( L = \mathbb{Q}_p(\zeta_{p^r} + \zeta_{p^r}^{-1}) \) and let \( \mathcal{C} \) be a \( k \)-dimensional code over \( \mathbb{R}^n \) such that \( \mathcal{C} \subseteq \mathbb{C}_L \). Then:

\[
A_{\mathcal{C}}^* = A_{\mathcal{C}}^{\perp}.
\]

**Corollary 3** Let \( L = \mathbb{Q}_p(\zeta_{p^r} + \zeta_{p^r}^{-1}) \) and let \( \mathcal{C} \) be a \( k \)-dimensional code over \( \mathbb{R}^n \) such that \( \mathcal{C} \subseteq \mathbb{C}_L \) then the lattice \( (A_{\mathcal{C}}, b) \) where \( b \) is the bilinear form \( b = \sum_{i=1}^{m} \text{Tr}_{L/\mathbb{Q}_p}(a_i x_i) \) is an integral lattice of rank \( m \mathbb{p}^{r-1}(p - 1)/2 \). We have that the lattice \( A_{\mathcal{C}} \) is an odd unimodular if the code \( \mathcal{C} \) is self-dual code.

Note that, using this corollary we can construct self-dual codes over finite chain rings from odd unimodular lattices over \( \mathbb{Q}_p(\zeta_{p^r} + \zeta_{p^r}^{-1}) \).
5 Conclusions

This paper gives a general construction of lattices from codes over finite chain rings using $p$-adic fields. The connection between finite chain rings and $p$-adic fields was highlighted and based on this connection, the lifting of codes over finite chain rings was generalized. Also lattices were defined over $p$-adic integers with allow us to deal with lattices over the ring of integers of a Galois extension of $\mathbb{Q}_p$ from lifted codes over finite chain rings were constructed.

Acknowledgements We thank the anonymous referees for their helpful comments, and constructive remarks that improved the quality and scopus of this manuscript.

References

1. Calderbank, A.R., Sloane, N.J.A.: Modular and $p$-adic cyclic codes. Des. Codes Cryptogr. 6(1), 21–35 (1995)
2. Costa, S.I.R., Oggier, F., Campello, A., Belfiore, J.-C., Viterbo, E.: Lattices applied to coding for reliable and secure communications. Cham: Springer; Rio de Janeiro: Sociedade Brasileira de Matemática Aplicada e Computacional (SBMAC) (2017)
3. Dougherty, S.T., Liu, H., Park, Y.H.: Lifted codes over finite chain rings. Math. J. Okayama Univ. 53, 39–53 (2011)
4. Hou, X.-D., Keating, K.: Enumeration of isomorphism classes of extensions of $p$-adic fields. J. Number Theory 104(1), 14–61 (2004)
5. Hou, X.-D., Leung, K.H., Ma, S.L.: On the groups of units of finite commutative chain rings. Finite Fields Appl. 9(1), 20–38 (2003)
6. Iwasawa, K.: Local class field theory. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York. Oxford Mathematical Monographs (1986)
7. Kositwattanarerk, W., Ong, S.S., Oggier, F.: Construction A of lattices over number fields and block fading (wiretap) coding. IEEE Trans. Inform. Theory 61(5), 2273–2282 (2015)
8. McDonald, B.R.: Finite rings with identity. Marcel Dekker, Inc., New York. Pure and Applied Mathematics, vol. 28 (1974)
9. Neukirch, J.: Algebraic number theory. Transl. from the German by Norbert Schappacher, vol 322. Berlin: Springer (1999)
10. Norton, G.H., Sălâgean, A.: On the structure of linear and cyclic codes over a finite chain ring. Appl. Algebra Engrg. Comm. Comput. 10(6), 489–506 (2000)
11. Park, Y.H.: The $q$-adic liftings of codes over finite fields. Korean J. Math. 26(3), 537–544 (2018)
12. Serre, J.-P.: Local fields, volume 67 of graduate texts in mathematics. Springer-Verlag, New York-Berlin. Translated from the French by Marvin Jay Greenberg (1979)
13. Wood, J.A.: Mr2778905– review of: Lifted codes over finite chain rings. AMS Reviews (2012a)