ALGEBRAIC STRUCTURE OF CYCLIC AND NEGACYCLIC CODES OVER A FINITE CHAIN RING ALPHABET AND APPLICATIONS

Dinh Quang Hai
Department of Mathematical Sciences, Kent State University,
4314 Mahoning Avenue, Warren, Ohio 44483, USA
Received on 17/5/2019, accepted for publication on 29/6/2019

Abstract: Foundational and theoretical aspects of algebraic coding theory are discussed with the concentration in the classes of cyclic and negacyclic codes over finite chain rings. The significant role of finite rings as alphabets in coding theory is presented. We surveys results on both simple-root and repeated-root cases of such codes. Many directions in which the notions of cyclicity and negacyclicity have been generalized are also considered. The paper is devoted to giving an introduction to this area of applied algebra. We do not intend to be encyclopedic, the topics included are bounded to reflect our own research interest.

1 What is Coding Theory?

The existence of noise in communication channels is an unavoidable fact of life. A response to this problem has been the creation of error-correcting codes. Coding Theory is the study of the properties of codes and their properties for a specific application. Codes are used for data compression, cryptography, error-correction, and more recently for network coding. In 1948, Claude Shannon's[1] landmark paper [114] on the mathematical theory of communication, which showed that good codes exist, marked the beginning of both Information Theory and Coding Theory.

The common feature of communication channels is that the original information is sent across a noisy channel to a receiver at the other end. The channel is "noisy" in the sense that the received message is not always the same as what was sent. The fundamental problem is to detect if there is an error, and in such case, to determine what message was sent based on the approximation that was received. An example that motivated the study of coding theory is telephone transmission. It is impossible to avoid errors that occur as

[1)] Email: hdinh@kent.edu

[1]Claude Elwood Shannon (April 30, 1916 - February 24, 2001) was an American mathematician, electronic engineer, and cryptographer, who is refered to as "the father of information theory" [76]. Shannon is also credited as the founder of both digital computer and digital circuit design theory, when, in 1937, as a 21-year-old master's student at MIT, he wrote a thesis establishing that electrical application of Boolean algebra could construct and resolve any logical, numerical relationship. It has been claimed that this was the most important master's thesis of all time. Shannon contributed to the field of cryptanalysis during World War II and afterwards, including basic work on code breaking.

messages pass through long telephone lines and are corrupted by things such as lightening and crosstalk. The transmission and reception capabilities of many modems are increased by error handling capability in hardware. Another area in which coding theory has been applied successfully is deep space communication. The meassge sourse is the satellite, the channel is the out space and hardware that sends and receives date, the receiver is the ground station on earth, and the noise are outside problems such as atmospheric conditions and thermal disturbance. Data from space missions has been coded for transmission, since it is normally impractical to retransmit. It is also important to protect communication across time from inaccuracies. Data stored in computer banks or on tapes is subject to the intrusion of gamma rays and magnetic interference. Personal computers are exposed to much battering, their hard disks are often equipped with an error correcting code called "cyclic redundancy check" (CRC)[2] designed to detect accidental changes to raw computer data. Leading computer companies like IBM an Dell have devoted much energy and time to the study and implementation of error correcting techniques for data storage. Electronics firms too need correction techniques. When Phillips introduced compact disc technology, they wanted the information stored on the disc face to be immune to many types of damage. In this case, the mesage is the voice, music, or data to be stored in the disc, the channel is the disc itself, the receiver is the listener, and the noise here can be caused by fingerprints or scratches on the disc. Recently the sound tracks of movies, prone to film breakage and scratching, have been digitized and protected with error correction techniques.

The study of codes has grown into an important subject that intersects various scientific disciplines, such as information theory, electrical engineering, mathematics, and computer science, for the purpose of designing efficient and reliable data transmission methods. This typically involves the removal of redundancy and the detection and correction of errors in the transmitted data. There are essentially two aspects to coding theory, namely, source coding (i.e, data compression) and channel coding (i.e, error correction). These two aspects may be studied in combination.

Source coding attempts to compress the data from a source in order to transmit it more efficiently. This process can be found every day on the internet where the common

[2]A cyclic redundancy check (CRC) is an error-detecting code designed to detect accidental changes to raw computer data, and is commonly used in digidelltal networks and storage devices such as hard disk drives. The CRC was first introduced by Peterson and Brown in 1961 [105], the 32-bit polynomial used in the CRC function of Ethernet and many other standards is the work of several researchers and was published in 1975. Blocks of data entering these systems get a short check value attached, derived from the remainder of a polynomial division of their contents; on retrieval the calculation is repeated, and corrective action can be taken against presumed data corruption if the check values do not match. CRCs are so called because the check (data verification) value is a redundancy (it adds zero information to the message) and the algorithm is based on cyclic codes. CRCs are popular because they are simple to implement in binary hardware, are easy to analyze mathematically, and are particularly good at detecting common errors caused by noise in transmission channels. Because the check value has a fixed length, the function that generates it is occasionally used as a hash function.

Zip data compression is used to reduce the network bandwidth and make files smaller. The second aspect, channel coding, adds extra data bits to make the transmission of data more robust to disturbances present on the transmission channel. The ordinary users usually are not aware of many applications using channel coding. A typical music CD uses the Reed-Solomon code to correct damages caused by scratches and dust. In this application the transmission channel is the CD itself. Cellular phones also use coding techniques to correct for the fading and noise of high frequency radio transmission. Data modems, telephone transmissions, and NASA all employ channel coding techniques to get the bits through, for example the turbo code and LDPC codes.

Algebraic coding theory studies the subfield of coding theory where the properties of codes are expressed in algebraic terms. Algebraic coding theory is basically divided into two major types of codes, namely block codes and convolutional codes. It analyzes the following three important properties of a code: code length, total number of codewords, and the minimum distance between two codewords, using mainly the Hamming[3] distance, sometimes also other distances such as the Lee distance, Euclidean distance.

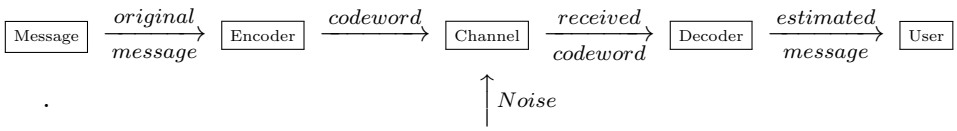
Given an alphabet $\mathcal{A}$ with q symbols, a block code C of length n over the alphabet $\mathcal{A}$ is simply a subset of $\mathcal{A}^n$. The q-ary n-tuples from C are called the codewords of the code C. One normally envisions K, the number of codewords in C, as a power of q, i.e., $K = q^k$, thus replacing the parameter K with the dimension $k = \log_q K$. This dimension k is the smallest integer such that each message for C can be assigned its own individual message k-tuple from the q-ary alphabet $\mathcal{A}$. Thus, the dimension k can be considered as the number of codeword symbols that are carrying message rather than redundancy. Hence, the number $n - k$ is sometimes called the redundancy of the code C. The error correction performance of a block code is described by the minimum Hamming distance d between each pair of code words, and is normally referred as the distance of the code.

In a block code, each input message has a fixed length of $k < n$ input symbols. The redundancy added to a message by transforming it into a larger codeword enables a receiver to detect and correct errors in a transmitted code word, and to recover the original message by using a suitable decoding algorithm. The redundancy is described in terms of its information rate, or more simply, for a block code, in terms of its code rate, k/n.

At the receiver end, a decision is made about the codeword transmitted based on the information in the received n-tuple. This decision is statistical, that is, it is a best guess on the basis of available information. A good code is one where k/n, the rate of the code, is as close to one as possible (so that, without too much redundancy, information may be transmited efficiently) while the codewords are far enough from one another that the probability of an incorrect interpretation of the received message is very small. The following

[3]The Hamming distance is named after Richard Hamming, who first introduced it in his fundamental paper on Hamming codes in 1950 [70]. It is used in telecommunication to count the number of flipped bits in a fixed-length binary word as an estimate of error, and hence it is sometimes refered to as the *signal distance*.

diagram describes a communication channel that includes an encoding/decoding scheme:



Shannon's theorem ensures that our hopes of getting the correct messages to the users will be fulfilled a certain percentage of the time. Based on the characteristics of the communication channel, it is possible to build the right encoders and decoders so that this percentage, although not 100%, can be made as high as we desire. However, the proof of Shannon's theorem is probabilistic and only guarantees the exixtence of such good codes. No specific codes were constructed in the proof that provides the desired accuracy for a given channel. The main goal of Coding Theory is to establish good codes that fulfill the assertions of Shannon's theorem. During the last 50 years, while many good codes have been constructed, but only from 1993, with the introduction of turbo codes[4], the rediscoveries of LDPC codes[5], and the study of related codes and associated iterative decoding algorithms, researchers started to see codes that approach the expectation of Shannon's theorem in practice.

2 Alphabets: Fields and Rings

While the algebraic theory of error-correcting codes has traditionally taken place in the setting of vector spaces over finite fields, codes over finite rings have been studied since the

[4]Turbo codes were first introduced and developed in 1993 by Berrou, Glavieux, and Thitimajshima [11]. Turbo codes are a class of high-performance forward error correction (FEC) codes, which were the first practical codes to closely approach the channel capacity, a theoretical maximum for the code rate at which reliable communication is still possible given a specific noise level. Turbo codes are widely used in deep space communications and other applications where designers seek to achieve reliable information transfer over bandwidth-constrained or latency-constrained communication links in the presence of data-corrupting noise.

The first class of turbo code was the parallel concatenated convolutional code (PCCC). Since the introduction of the original parallel turbo codes in 1993, many other classes of turbo code have been discovered, including serial versions and repeat-accumulate codes. Iterative Turbo decoding methods have also been applied to more conventional FEC systems, including Reed-Solomon corrected convolutional codes.

[5]LDPC (low-density parity-check) codes were first introduced in 1963 by Robert G. Gallager in his doctoral dissertation at MIT. At that time, it was impractical to implement and LDPC codes were forgotten, but they were rediscovered in 1996. A LDPC code is a linear error correcting code, a method of transmitting a message over a noisy transmission channel, and is constructed using a sparse bipartite graph. LDPC codes are capacity-approaching codes, which means that practical constructions exist that allow the noise threshold to be set arbitrarily close on the binary erasure channel (BEC) to the Shannon limit for a symmetric memoryless channel. The noise threshold defines an upper bound for the channel noise, up to which the probability of lost information can be made as small as desired. Using iterative belief propagation techniques, LDPC codes can be decoded in time linear to their block length.

early 1970s. However, the papers on the subject during the 1970s and 1980s were scarse and may have been considered mostly as a mere mathematical curiosity since they did not seem to be aimed at solving any of the pressing open problems that were considered of utmost importance at the time by coding theorists.

Some of the highlights of that period include the work of Blake [7], who, in 1972, showed how to contruct codes over $\mathbb{Z}_m$ from cyclic codes over $GF(p)$ where p is a prime factor of m. He then focused on studying the structure of codes over $\mathbb{Z}_{p^r}$ (cf. [8]). In 1977, Spiegel [118], [119] generalized those results to codes over $\mathbb{Z}_m$, where m is an arbitrary positive integer.

There are well known families of nonlinear codes (over finite fields), such as Kerdock, Preparata, Nordstrom-Robinson, Goethals, and Delsarte-Goethals codes [18], [39], [64], [65], [82], [92], [102], [110], that have more codewords than every comparable linear codes known to date. They have great error-correcting capabilities as well as remarkable structure, for example, the weight distributions of Kerdock and Preparata codes are MacWilliams transform of each other. Several researchers have investigated these codes and have shown that they are not unique, and large numbers of codes exist with the same weight distributions [4], [25], [77], [78], [79], [80], [120].

It was only until the early 1990s that the study of linear codes over finite rings gained prominence, due to the discovery that these codes are actually equivalent to linear codes over the ring of integers modulo four, the so-called Quaternary codes[6] (cf. [23], [36], [71], [98], [99], [108], [109]. Nechaev pointed out that the Kerdock codes are, in fact, cyclic codes over $\mathbb{Z}_4$ in [99]. Furthermore, the intriguing relationship between the weight distributions of Kerdock and Preparata codes, a relation that is akin to that between the weight distributions of a linear code and its dual, was explained by Calderbank, Hammons, Kumar, Sloane and Solé [23], [71] when they showed in 1993 that these well-known codes are in fact equivalent to linear codes over the ring $\mathbb{Z}_4$ which are dual to one another. The families of Kerdock and Preparata codes exist for all length $n = 4^k \geq 16$, and at length 16, they coincide, providing the Nordstrom-Robison code [65], [102], [116], this code is the unique binary code of length 16, consisting 256 codewords, and minimum distance 6. In [23], [71] (see also [35], [36]), it has also been shown that the Nordstrom-Robison code is equivalent to a quaternary code which is self-dual. From that point on, codes over finite rings in general and over $\mathbb{Z}_4$ in particular, have gained considerable prominence in the literature. There are now numerous research papers on this subject and at least one book devoted to the study of Quaternary Codes [122].

Although we did not elaborate much on the meaning of the "remarkable structure" mentioned above between the Kerdock and Preparata codes and the corresponding codes over $\mathbb{Z}_4$, let it suffice to say that there is an isometry between them that is induced by the

[6]In the coding theory literature, the term "quaternary codes" sometimes is used for codes over the finite field GF(4). Throughout this paper, including references, unless otherwise stated, by quatenary codes we mean codes over $\mathbb{Z}_4$.

Gray map $\mu : \mathbb{Z}_4 \to (\mathbb{Z}_2)^2$ sending 0 to 00, 1 to 01, 2 to 11, and 3 to 10. The isometry relates codes over $\mathbb{Z}_4$ equipped with the so-called Lee metric with the Kerdock and Preparata codes with the standard Hamming metric. The point is that, from its inception, the theory of codes over rings was not only about the introduction of an alternate algebraic structure for the alphabet but also of a different metric for the new codes over rings. In addition to the Lee metric, other alternative metrics have been considered by several authors.

There are at least two reasons why cyclic codes have been one of the most important class of codes in coding theory. First of all, cyclic codes can be efficiently encoded using shift registers, which explains their preferred role in engineering. In addition,cyclic codes are easily characterized as the ideals of the specific quotient ring $\frac{F[x]}{\langle x^n-1\rangle}$ of the(infinite) ring $F[x]$ of polynomials with coefficients in the alphabet field F. It is this characterization that makes cyclic codes suitable for generalizations of various sorts. The concepts of negacyclic and constacyclic codes, for example, may be seen as focusing on those codes that correspond to ideals of the quotient rings $\frac{F[x]}{\langle x^n+1\rangle}$ and $\frac{F[x]}{\langle x^n-\lambda\rangle}$ (where $\lambda \in F - \{0\}$) of $F[x]$. In fact, the most general such generalization is the notion of a polycyclic code. Namely those codes that correspond to ideals of some quotient ring $\frac{F[x]}{\langle f(x)\rangle}$ of $F[x]$ [89].

All of notions above can easily be extended to the finite ring alphabet case by replacing the finite field F by the finite ring R in each definition. Those concepts, when R is a chain ring, are the main subject of our survey, which is an update version of the survey [55].

3 Chain Rings

Let R be a finite commutative ring. An ideal I of R is called *principal* if it is generated by a single element. A ring R is a *principal ideal ring* if all of its ideals are principal. R is called a *local ring* if R has a unique maximal ideal. Furthermore, a ring R is called a *chain ring* if the set of all ideals of R is a chain under set-theoretic inclusion. It can be shown easily that chain rings are principal ideal rings. Examples of finite commutative chain rings include the ring $\mathbb{Z}_{p^k}$ of integers modulo p^k, for a prime p, and the Galois rings $\mathrm{GR}(p^k, m)$, i.e. the Galois extension of degree m of $\mathbb{Z}_{p^k}$ (cf. [75], [96])[7]. These classes of rings have been used widely as an alphabet for constacyclic codes. Various decoding schemes for codes over Galois rings have been considered in [19]-[22].

The following equivalent conditions are well-known for the class of finite commutative chain rings (cf. [54, Proposition 2.1]).

[7]Although we only consider finite commutative chain rings in this paper, it is worth noting that a finite chain ring need not be commutative. The smallest noncommutative chain ring has order 16 [84], that can be represented as $R = \mathrm{GF}(4) \oplus \mathrm{GF}(4)$, where the operations $+, \cdot$ are

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),$$

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, a_1 b_2 + b_1 a_2^2).$$

Proposition 3.1. *For a finite commutative ring R the following conditions are equivalent:*

(*i*) *R is a local ring and the maximal ideal M of R is principal,*

(*ii*) *R is a local principal ideal ring,*

(*iii*) *R is a chain ring.*

Let ζ be a fixed generator of the maximal ideal M of a finite commutative chain ring R. Then ζ is nilpotent and we denote its nilpotency index by t. The ideals of R form a chain:

$$R = \langle \zeta^0 \rangle \supsetneq \langle \zeta^1 \rangle \supsetneq \cdots \supsetneq \langle \zeta^{t-1} \rangle \supsetneq \langle \zeta^t \rangle = \langle 0 \rangle.$$

Let $\overline{R} = \frac{R}{M}$. By $^- : R[x] \longrightarrow \overline{R}[x]$, we denote the natural ring homomorphism that maps $r \mapsto r + M$ and the variable x to x. The following is a well-known fact about finite commutative chain ring (cf. [96]).

Proposition 3.2. *Let R be a finite commutative chain ring, with maximal ideal $M = \langle \zeta \rangle$, and let t be the nilpotency ζ. Then*

(*a*) *For some prime p and positive integers k, l $(k \geq l)$, $|R| = p^k, |\overline{R}| = p^l$, and the characteristic of R and $\overline{R}$ are powers of p,*

(*b*) *For $i = 0, 1, \ldots, t$, $|\langle \zeta^i \rangle| = |\overline{R}|^{t-i}$. In particular, $|R| = |\overline{R}|^t$, i.e., $k = lt$.*

Two polynomials $f_1, f_2 \in R[x]$ are called *coprime* if $\langle f_1 \rangle + \langle f_2 \rangle = R[x]$, or equivalently, if there exist polynomials $g_1, g_2 \in R[x]$ such that $f_1 g_1 + f_2 g_2 = 1$. The coprimeness of two polynomials in $\overline{R}[x]$ is defined similarly.

Lemma 3.3. (cf. [54, Lemma 2.3, Remark 2.4]) *Two polynomials $f_1, f_2 \in R[x]$ are coprime if and only if $\overline{f}_1$ and $\overline{f}_2$ are coprime in $\overline{R}[x]$. Moreover, if $f_1, f_2, \ldots, f_k$ are pairwise coprime polynomials in $R[x]$, then f_i and $\prod_{j \neq i}^{k} f_j$ are coprime in $R[x]$.*

A polynomial $f \in R[x]$ is called *basic irreducible* if $\overline{f}$ is irreducible in $\overline{R}[x]$. A polynomial $f \in R[x]$ is called *regular* if it is not a zero divisor.

Proposition 3.4. (cf. [96, [Theorem XIII.2(c)]) *Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ be in $R[x]$, then the following are equivalent:*

(*i*) *f is regular,*

(*ii*) *$\langle a_0, a_1, \ldots, a_n \rangle = R$,*

(*iii*) *a_i is a unit for some i, $0 \leq i \leq n$,*

(*iv*) *$\overline{f} \neq 0$.*

The following Lemma guarantees that factorizations into product of pairwise coprime polynomials over $\overline{R}$ lift to such factorizations over R (cf. [96, Theorem XIII.4]).

Lemma 3.5. (Hensel's Lemma) *Let f be a polynomial over R and assume $\overline{f} = g_1 g_2 \dots g_r$ where $g_1, g_2, \dots, g_r$ are pairwise coprime polynomials over $\overline{R}$. Then there exist pairwise coprime polynomials $f_1, f_2, \dots, f_r$ over R such that $f = f_1 f_2 \dots f_r$ and $\overline{f}_i = g_i$ for $i = 1, 2, \dots, r$.*

Proposition 3.6. *If f is a monic polynomial over R such that $\overline{f}$ is square free, then f factors uniquely as a product of monic basic irreducible pairwise coprime polynomial.*

In the general case, when $\overline{f}$ is not necessarily square-free, [26, Theorem 4], [27, Theorem 2], [113,Theorem 3.2] provide a necessary and sufficient condition for $\frac{R[x]}{\langle f \rangle}$ to be a principal ideal ring:

Proposition 3.7. *Let $f \in R[x]$ be a monic polynomial such that $\overline{f}$ is not square-free. Let $g, h \in R[x]$ be such that $\overline{f} = \overline{g}\overline{h}$ and $\overline{g}$ is the square-free part of $\overline{f}$. Write $f = gh + \zeta w$ with $w \in R[x]$. Then $\frac{R[x]}{\langle f \rangle}$ is a principal ideal ring if and only if $\overline{u} \neq 0$, and $\overline{u}$ and $\overline{h}$ are coprime.*

The Galois ring of characteristic p^a and dimension m, denoted by $\mathrm{GR}(p^a, m)$, is the Galois extension of degree m of the ring $\mathbb{Z}_{p^a}$. Equivalently,

$$\mathrm{GR}(p^a, m) = \frac{\mathbb{Z}_{p^a}[z]}{\langle h(z) \rangle},$$

where $h(z)$ is a monic basic irreducible polynomial of degree m in $\mathbb{Z}_{p^a}[z]$.

Note that if $a = 1$, then $\mathrm{GR}(p, m) = \mathrm{GF}(p^m)$, and if $m = 1$, then $\mathrm{GR}(p^a, 1) = \mathbb{Z}_{p^a}$. We gather here some well-known facts about Galois rings (cf. [71], [75], [96]):

Proposition 3.8. *Let $\mathrm{GR}(p^a, m) = \frac{\mathbb{Z}_{p^a}[z]}{\langle h(z) \rangle}$ be a Galois ring, then the following hold:*

(*i*) *Each ideal of $\mathrm{GR}(p^a, m)$ is of the form $\langle p^k \rangle = p^k \,\mathrm{GR}(p^a, m)$, for $0 \leq k \leq a$. In particular, $\mathrm{GR}(p^a, m)$ is a chain ring with maximal ideal $\langle p \rangle = p\,\mathrm{GR}(p^a, m)$, and residue field $\mathrm{GF}(p^m)$.*

(*ii*) *For $0 \leq i \leq a$, $|p^i \,\mathrm{GR}(p^a, m)| = p^{m(a-i)}$.*

(*iii*) *Each element of $\mathrm{GR}(p^a, m)$ can be represented as up^k, where u is a unit and $0 \leq k \leq a$, in this representation k is unique and u is unique modulo $\langle p^{n-k} \rangle$*

(*iv*) *$h(z)$ has a root ξ, which is also a primitive $(p^m - 1)$th root of unity. The set*

$$\mathcal{T}_m = \{0, 1, \xi, \xi^2, \dots, \xi^{p^m - 2}\}$$

is a complete set of representatives of the cosets $\frac{\mathrm{GR}(p^a, m)}{p\,\mathrm{GR}(p^a, m)} = \mathrm{GF}(p^m)$ in $\mathrm{GR}(p^a, m)$. Each element $r \in \mathrm{GR}(p^a, m)$ can be written uniquely as

$$r = \xi_0 + \xi_1 p + \cdots + \xi_{a-1} p^{a-1},$$

with $\xi_i \in \mathcal{T}_m$, $0 \le i \le a-1$.

(*v*) *For each positive integer* d, *there is a natural injective ring homomorphism* $\mathrm{GR}(p^a, m) \to \mathrm{GR}(p^a, md)$.

(*vi*) *There is a natural surjective ring homomorphism* $\mathrm{GR}(p^a, m) \to \mathrm{GR}(p^{a-1}, m)$ *with kernel* $\langle p^{a-1} \rangle$.

(*vii*) *Each subring of* $\mathrm{GR}(p^a, m)$ *is a Galois ring of the form* $\mathrm{GR}(p^a, l)$, *where* l *divides* m. *Conversely, if* l *divides* m *then* $\mathrm{GR}(p^a, m)$ *contains a unique copy of* $\mathrm{GR}(p^a, l)$. *That means, the number of subrings of* $\mathrm{GR}(p^a, m)$ *is the number of positive divisors of* m.

4 Constacyclic Codes over Arbitrary Commutative Finite Rings

Given an n-tuple $(x_0, x_1, \ldots, x_{n-1}) \in R^n$, the *cyclic shift* τ and *negashift* ν on R^n are defined as usual, i.e.,

$$\tau(x_0, x_1, \ldots, x_{n-1}) = (x_{n-1}, x_0, x_1, \cdots, x_{n-2}),$$

and

$$\nu(x_0, x_1, \ldots, x_{n-1}) = (-x_{n-1}, x_0, x_1, \cdots, x_{n-2}).$$

A code C is called *cyclic* if $\tau(C) = C$, and C is called *negacyclic* if $\nu(C) = C$.

More generally, if λ is a unit of the ring R, then the λ-*constacyclic* (λ-twisted) *shift* τ_λ on R^n is the shift

$$\tau_\lambda(x_0, x_1, \ldots, x_{n-1}) = (\lambda x_{n-1}, x_0, x_1, \cdots, x_{n-2}),$$

and a code C is said to be λ-*constacyclic* if $\tau_\lambda(C) = C$, i.e., if C is closed under the λ-constacyclic shift τ_λ.

Equivalently, C ia a λ-constacyclic code if and only if

$$CS_\lambda \subseteq C,$$

where S_λ is the λ-constacyclic shift matrix given by

$$S_\lambda = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ \lambda & 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} 0 & & & \\ \vdots & & I_{n-1} & \\ 0 & & & \\ \lambda & 0 & \cdots & 0 \end{pmatrix} \subseteq R_{n\times n}.$$

In light of this definition, when $\lambda = 1$, λ-constacyclic codes are cyclic codes, and when $\lambda = -1$, λ-constacyclic codes are just negacyclic codes.

Each codeword $c = (c_0, c_1, \ldots, c_{n-1})$ is customarily identified with its polynomial representation $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$, and the code C is in turn identified with the set of all polynomial representations of its codewords. Then in the ring $\frac{R[x]}{\langle x^n-\lambda\rangle}$, $xc(x)$ corresponds to a λ-constacyclic shift of $c(x)$. From that, the following fact is well-known and straightforward:

Proposition 4.1. *A linear code C of length n is λ-constacyclic over R if and only if C is an ideal of $\frac{R[x]}{\langle x^n-\lambda\rangle}$.*

The dual of a cyclic code is a cyclic code, and the dual of a negacyclic code is a negacyclic code. In general, we have the following implication of the dual of a λ-constacyclic code.

Proposition 4.2. (cf. [45]) *The dual of a λ-constacyclic code is a λ^{-1}-constacyclic code.*

For a nonempty subset S of the ring R, the *annihilator* of S, denoted by $\mathrm{ann}(S)$, is the set

$$\mathrm{ann}(S) = \{f \mid fg = 0, \text{ for all } g \in R\}.$$

Then $\mathrm{ann}(S)$ is an ideal of R.

Customarily, for a polynomial f of degree k, its reciprocal polynomial $x^k f(x^{-1})$ will be denoted by f^*. Thus, for example, if

$$f(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1} + a_kx^k,$$

then

$$f^*(x) = x^k(a_0 + a_1x^{-1} + \cdots + a_{k-1}x^{-(k-1)} + a_kx^{-k}) = a_k + a_{k-1}x + \cdots + a_1x^{k-1} + a_0x^k.$$

Note that $(f^*)^* = f$ if and only if the constant term of f is nonzero, if and only if $\deg(f) = \deg(f^*)$. We denote $A^* = \{f^*(x) \mid f(x) \in A\}$. It is easy to see that if A is an ideal, then A^* is also an ideal.

Proposition 4.3. (cf. [53, Propositions 3.3, 3.4]) *Let R be a finite commutative ring, and λ be a unit of R.*

(*a*) *Let* $a(x), b(x) \in R[x]$ *be given as*

$$a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1},$$

$$b(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}.$$

Then $a(x)b(x) = 0$ *in* $\frac{R[x]}{\langle x^n - \lambda \rangle}$ *if and only if* $(a_0, a_1, \ldots, a_{n-1})$ *is orthogonal to*

$$(b_{n-1}, b_{n-2}, \ldots, b_0)$$

and all its λ^{-1}*-constacyclic shifts.*

(*b*) *Assume in addition that* $\lambda^2 = 1$*, and* C *is a* λ*-constacyclic code of length* n *over* R*. Then the dual* $C^\perp$ *of* C *is* $(ann(C))^*$*.*

When studying λ-constacyclic codes over finite fields, most researchers assume that the code-length n is not divisible by the characteristic p of the field. This ensures that $x^n - \lambda$, and hence the generator polynomial of any λ-constacyclic code, will have no multiple factors, and hence no repeated roots in an extension field. The case when the code length n is divisible by the characteristic p of the field yields the so-called *repeated-root codes*, which were first studied in 1967 by Berman [6], and then in the 1970s and 1980s by several authors such as Massey *et al.* [95], Falkner *et al.* [62], Roth and Seroussi [111]. However, repeated-root codes over finite fields were investigated in the most generality in the 1990s by Castagnoli *et al.* [28], and van Lint [121], where they showed that repeated-root cyclic codes have a concatenated construction, and are asymptotically bad. Nevertheless, such codes are optimal in a few cases and that motivates further study of the class.

Repeated-root constacyclic codes over a class of finite chain rings have been extensively studied over the last few years by many researchers, such as Abualrub and Oehmke [1], [2], Blackford [12], [13], Dinh [40]-[46], Ling *et al* [60], [83], [86], Sălăgean *et al* [104], [113], etc.

To distinguish the two cases, codes where the code-length is not divisible by the characteristic p of the residue field $\overline{R}$ are called *simple-root codes*. We will consider this class of codes in Section 5, and the class of repeated-root codes in Section 6.

A recent publication [80] introduces the dual notions of polycyclic and sequential codes. In addition to being generalizations of constacyclicity, they serve to characterize precisely that concept in terms of a symmetry criterion. We mention this result as Theorem 7.2 at the end of this paper.

5 Simple-Root Cyclic and Negacyclic Codes over Finite Chain Rings

All codes considered in this section are simple-root codes over a finite chain ring R, i.e., the code-length n is not divisible by the characteristic p of the residue field $\overline{R}$. The structure of cyclic codes over $\mathbb{Z}_{p^a}$ was obtained by Calderbank and Sloane in 1995 [24], and later on with a different proof by Kanwar and López-Permouth in 1997 [81]. In 1999, with a different technique, Norton and Sălăgean extended the structure theorems given in [24] and [81] to cyclic codes over finite chain rings (cf. [103]), they used an elementary approach which did not appeal to Commutative Algebra as that of [24] and [81] did.

Let R be a finite chain ring with the maximal ideal $\langle\zeta\rangle$, and t be the nilpotency of ζ. For a linear code C of length n over R, the *submodule quotient* of C by $r \in R$ is the code

$$(C : r) = \left\{ e \in R^n \,\middle|\, er \in C \right\}.$$

Thus we have a tower of linear codes over R

$$C = (C : \zeta^0) \subseteq \ldots (C : \zeta^i) \cdots \subseteq (C : \zeta^{t-1}).$$

Its projection to $\overline{R}$ forms a tower of linear codes over $\overline{R}$

$$\overline{C} = \overline{(C : \zeta^0)} \subseteq \ldots \overline{(C : \zeta^i)} \cdots \subseteq \overline{(C : \zeta^{t-1})}.$$

If C is a cyclic code over R, then for $0 \leq i \leq t-1$, $(C : \zeta^i)$ is a cyclic over R, and $\overline{(C : \zeta^i)}$ is a cyclic over $\overline{R}$. For codes over $\mathbb{Z}_4$, $\overline{C} = \overline{(C : \zeta^0)} \subseteq \overline{(C : \zeta)}$, were first introduced by Conway and Sloane in [36], and later were generalized to codes over any chain ring by Norton and Sălăgean [103].

For a code C of length n over R, a matrix G is called a *generator matrix* of C if the rows of G span C, and none of them can be written as a linear combination of other rows of G. A generator matrix G is said to be in *standard form* if after a suitable permutation of the coordinates,

$$G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & A_{0,t-1} & A_{0,t} \\ 0 & \zeta I_{k_1} & \zeta A_{1,2} & \zeta A_{1,3} & \cdots & \zeta A_{1,t-1} & \zeta A_{1,t} \\ 0 & 0 & \zeta^2 I_{k_2} & \zeta^2 A_{2,3} & \cdots & \zeta^2 A_{2,t-1} & \zeta^2 A_{2,t} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \zeta^{t-1} I_{k_{t-1}} & \zeta^{t-1} A_{t-1,t} \end{pmatrix} = \begin{pmatrix} A_0 \\ \zeta A_1 \\ \zeta^2 A_2 \\ \vdots \\ \zeta^{t-1} A_{t-1} \end{pmatrix},$$

where the columns are grouped into blocks of sizes $k_0, k_1, \ldots, k_{t-1}, n - \sum_{i=0}^{t-1} k_i$. The generator matrix in standard form G is associated to the matrix

$$A = \begin{pmatrix} A_0 \\ A_1 \\ A_2 \\ \vdots \\ A_{t-1} \end{pmatrix}.$$

We denote by $\gamma(C)$ the number of rows of a generator matrix in standard form of C, and $\gamma_i(C)$ the number of rows divisible by ζ^i but not by ζ^{i+1}. Equivalently, $\gamma_0(C) = \dim(\overline{C})$, and $\gamma_i(C) = \dim \overline{(C : \zeta^i)} - \dim \overline{(C : \zeta^{i-1})}$, for $1 \le i \le t-1$

Obviously, $\gamma(C) = \sum_{i=0}^{t-1} \gamma_i(C)$.

For a linear code C of length n over a finite chain ring R, the information on generator matrices, parity check matrices, and sizes of C, its dual $C^\perp$, its projection $\overline{C}$ to the residue field $\overline{R}$, is given as follows.

Theorem 5.1. (cf. [103, Lemma 3.4, Theorems 3.5, 3.10]) *Let C be a linear code of length n over a finite chain ring R, and*

$$G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & A_{0,t-1} & A_{0,t} \\ 0 & \zeta I_{k_1} & \zeta A_{1,2} & \zeta A_{1,3} & \cdots & \zeta A_{1,t-1} & \zeta A_{1,t} \\ 0 & 0 & \zeta^2 I_{k_2} & \zeta^2 A_{2,3} & \cdots & \zeta^2 A_{2,t-1} & \zeta^2 A_{2,t} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \zeta^{t-1} I_{k_{t-1}} & \zeta^{t-1} A_{t-1,t} \end{pmatrix} = \begin{pmatrix} A_0 \\ \zeta A_1 \\ \zeta^2 A_2 \\ \vdots \\ \zeta^{t-1} A_{t-1} \end{pmatrix},$$

is a generator matrix in standard form of C, which is associated to the matrix

$$A = \begin{pmatrix} A_0 \\ A_1 \\ A_2 \\ \vdots \\ A_{t-1} \end{pmatrix}.$$

Then

(a) *For $0 \le i \le t-1$, $\overline{(C : \zeta^i)}$ has generator matrix*

$$\begin{pmatrix} \overline{A_0} \\ \overline{A_1} \\ \vdots \\ \overline{A_i} \end{pmatrix},$$

and $\dim \overline{(C : \zeta^i)} = k_0 + k_1 + \cdots + k_i$.

(*b*) *If* $E_0 \subseteq E_1 \subseteq \cdots \subseteq E_{t-1}$ *are linear codes of length* n *over* $\overline{R}$*, then there is a code* D *of length* n *over* R *such that* $\overline{(D:\zeta^i)} = E_i$*, for* $0 \le i \le t-1$.

(*c*) *The parameters* $k_0, k_1, \ldots, k_{t-1}$ *are the same for any generator matrix* G *in standard form for* C.

(*d*) *Any codeword* $c \in C$ *can be written uniquely as*

$$c = (v_0, v_1, \ldots, v_{t-1})\, G,$$

where $v_i \in (R/\zeta^{t-i}R)^{k_i} \cong (\zeta^i R)^{k_i}$.

(*e*) *The number of codewords in* C *is*

$$|C| = \left|\overline{R}\right|^{\sum_{i=0}^{t-1}(t-i)k_i}.$$

(*f*) *If, for* $0 \le i < j \le t$,

$$B_{i,j} = -\sum_{l=i+1}^{j-1} B_{i,l} A^{\mathrm{tr}}_{t-j,t-l} - A^{\mathrm{tr}}_{t-j,t-i},$$

then

$$H = \begin{pmatrix} B_{0,t} & B_{0,t-1} & \cdots & B_{0,1} & I_{n-\gamma(C)} \\ \zeta B_{1,t} & \zeta B_{1,t-1} & \cdots & \zeta I_{\gamma_{t-1}(C)} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \zeta^{t-1} B_{t-1,t} & \zeta^{t-1} I_{\gamma_1(C)} & \cdots & 0 & 0 \end{pmatrix} = \begin{pmatrix} B_0 \\ \zeta B_1 \\ \vdots \\ \zeta^{t-1} B_{t-1} \end{pmatrix}$$

is a generator matrix for $C^\perp$ *and a parity check matrix for* C.

(*g*) *For* $0 \le i \le t-1$, $\overline{(C^\perp:\zeta^i)} = \overline{(C:\zeta^i)}^\perp$, $\gamma_0(C^\perp) = n - \gamma(C)$, *and* $\gamma_i(C^\perp) = \gamma_{t-i}(C)$.

(*h*) $|C^\perp| = |R^n|/|C|$, *and* $\left(C^\perp\right)^\perp = C$.

(*i*) *Associate the generator matrix* H *of* $C^\perp$ *with the matrix*

$$B = \begin{pmatrix} B_0 \\ B_1 \\ \vdots \\ B_{t-1} \end{pmatrix}.$$

Then $\overline{C}$ has generator matrix $\overline{A_0}$, and parity check matrix

$$\overline{B} = \begin{pmatrix} \overline{B_0} \\ \overline{B_1} \\ \vdots \\ \overline{B_{t-1}} \end{pmatrix}.$$

The set $\{\zeta^{a_0} g_{a_0}, \zeta^{a_1} g_{a_1}, \ldots, \zeta^{a_k} g_{a_k}\}$ is said to be a *generating set in standard form* of the cyclic code C if the following conditions hold:

- $C = \langle \zeta^{a_0} g_{a_0}, \zeta^{a_1} g_{a_1}, \ldots, \zeta^{a_k} g_{a_k} \rangle$;
- $0 \leq k < t$;
- $0 \leq a_0 < a_1 < \cdots < a_k < t$;
- $g_{a_i} \in R[x]$ is monic for $0 \leq i \leq k$;
- $\deg(g_{a_i}) > \deg(g_{a_{i+1}})$ for $0 \leq i \leq k-1$;
- $g_{a_k} \mid g_{a_{k-1}} \mid \ldots \mid g_{a_0} \mid (x^n - 1)$.

The existence and uniqueness of a generator set in standard form of a cyclic code were proven by Calderbank and Sloane [24] in 1995 for the alphabet Z_{p^a}, and in 2000, that were extended to the general case of any chain ring R by Norton and Sălăgean [103].

Proposition 5.2. (cf. [24, Theorem 6], [103, Theorem 4.4] *Any non-zero cyclic code C over a finite chain ring R has a unique generator set in standard form.*

If the constant term a_0 of f is a unit, we denote $f^{\#} = a_0^{-1} f^*$. In particular, the constant term of any factor of $x^n - 1$ is a unit.

Moreover, if $f(x)$ is a factor of $x^n - 1$, we denote $\widehat{f}(x) = \frac{x^n - 1}{f(x)}$.

The generator set in standard form of a cyclic code is related to its generating matrix, and the generator set in standard form of its dual as follows:

Theorem 5.3. (cf. [103, Theorems 4.5, 4.9]) *Let C be a cyclic code, and*

$$\{\zeta^{a_0} g_{a_0}, \zeta^{a_1} g_{a_1}, \ldots, \zeta^{a_k} g_{a_k}\}$$

be its generating set in standard form. Then

(a) If, for $0 \leq i \leq k$, $d_i = \deg(g_{a_k})$, and by convention, $d_{-1} = n$, $d_{k+1} = 0$, and

$$T = \bigcup_{i=0}^{k} \left\{ \zeta^{a_i} g_{a_i} x^{d_{i-1} - d_i - 1}, \ldots, \zeta^{a_i} g_{a_i} x, \zeta^{a_i} g_{a_i} \right\},$$

then T defines a generator matrix for C;

(*b*) *Any* $c \in C$ *can be uniquely represented as* $c = \sum_{i=0}^{k} h_i g_{a_i} \zeta^{a_i}$, *where*

$$h_i \in \left(R/R\zeta^{t-a_i}\right)[x] \cong \left(R\zeta^{a_i}\right)[x],$$

and $\deg(h_i) < d_{i-1} - d_i$;

(*c*)

$$\gamma_j(C) = \begin{cases} d_{i-1} - d_i, & \text{if } j = a_i \text{ for some } i, \\ 0, & \text{otherwise} \end{cases},$$

and

$$|C| = \left|\overline{R}\right|^{\sum_{i=0}^{k}(t-a_i)(d_{i-1}-d_i)}.$$

(*d*) *Let* $a_{k+1} = t$, *and* $g_{a_{-1}} = x^n - 1$. *For* $0 \le i \le k+1$, *denote* $b_i = t - a_{k+1-i}$, *and* $g'_{b_i} = \widehat{g}^{\#}_{a_{k-i}}$. *Then* $\{\zeta^{b_0} g'_{b_0}, \zeta^{b_1} g'_{b_1}, \ldots, \zeta^{b_k} g'_{b_k}\}$ *is the generating set in standard form for* $C^{\perp}$.

In 2004, Dinh and López-Permouth [54] generalized the methods of [24], [81] for simple-root cyclic codes over $\mathbb{Z}_{p^a}$to obtain the structures of simple-root cyclic and self-dual cyclic codes over finite chain rings R. The strategy was independent from the approach in [103] and the results were more detailed.

Since the code-length n and the characteristic p of the residue field $\overline{R}$ are coprime, $x^n - 1$ factors uniquely to a product of monic basic irreducible pairwise-coprime polynomials in $R[x]$. The ambient ring $\frac{R[x]}{\langle x^n-1\rangle}$ can be decomposed as a direct sum of chain rings. So, any cyclic code of length n over R, viewed as an ideal of this ambient ring $\frac{R[x]}{\langle x^n-1\rangle}$, is represented as a direct sum of ideals from those chain rings.

Theorem 5.4. (cf. [54, Lemma 3.1, Theorem 3.2, Corollary 3.3]) *Let* R *be a finite chain ring with the maximal ideal* $\langle\zeta\rangle$, *and* t *be the nilpotency of* ζ. *Then*

(*a*) *If* f *is a regular basic irreducible polynomial of the ring* $R[x]$, *then* $\frac{R[x]}{\langle f\rangle}$ *is also a chain ring whose ideals are* $\langle\zeta^i\rangle$, $0 \le i \le t$.

(*b*) *Let* $x^n - 1 = f_1 f_2 \ldots f_r$ *be a representation of* $x^n - 1$ *as a product of monic basic irreducible pairwise-coprime polynomials in* $R[x]$. *Then* $\frac{R[x]}{\langle x^n-1\rangle}$ *can be represented as a direct sum of chain rings* $\frac{R[x]}{\langle f_i\rangle}$.

$$\frac{R[x]}{\langle x^n - 1\rangle} \cong \bigoplus_{i=1}^{r} \frac{R[x]}{\langle f_i\rangle}.$$

(c) *Each cyclic code of length n over R, i.e., each ideal of $\frac{R[x]}{\langle x^n-1\rangle}$, is a sum of ideals of the form $\langle \zeta^j \widehat{f}_i\rangle$, where $0 \le j \le t, 1 \le i \le r$.*

(d) *The numbers of cyclic codes over R of length n is $(t+1)^r$, where r is the number of factors in the unique factorization of x^n-1 into a product of monic basic irreducible pairwise coprime polynomials.*

For each cyclic code C, using the decomposition above, a unique set of pairwise coprime monic polynomials that generates C is constructed, which in turn provides the sizes of C and its dual $C^\perp$, and a set of generators for $C^\perp$. The set of pairwise coprime monic polynomials generators of C also gives a single generator of C, that implies $\frac{R[x]}{\langle x^n-1\rangle}$ is a principle ideal ring.

Theorem 5.5. (cf. [54, Theorems 3.4, 3.5, 3.6, 3.8, 3.10, 4.1]) *Let R be a finite chain ring with the maximal ideal $\langle\zeta\rangle$, and t be the nilpotency of ζ, and let C be a cyclic code of length n over R. Then*

(a) *There exists a unique family of pairwise coprime monic polynomials $F_0, F_1, \ldots, F_t$ in $R[x]$ such that $F_0F_1\ldots F_t = x^n-1$ and $C = \langle \widehat{F}_1, \zeta\widehat{F}_2, \ldots, \zeta^{t-1}\widehat{F}_t\rangle$.*

(b) *The number of codewords in C is*

$$|C| = \left|\overline{R}\right|^{\sum_{i=0}^{t-1}(t-i)\deg F_{i+1}}.$$

(c) *There exist polynomials $g_0, g_1, \ldots, g_{t-1}$ in $R[x]$ such that $C = \langle g_0, \zeta g_1, \ldots, \zeta^{t-1}g_{t-1}\rangle$ and*

$$g_{t-1}|g_{t-2}|\ldots|g_1|g_0|(x^n-1).$$

(d) *Let $F = \widehat{F}_1 + \zeta\widehat{F}_2 + \cdots + \zeta^{t-1}\widehat{F}_t$. Then F is a generating polynomial of C, i.e., $C = \langle F\rangle$. In particular, $\frac{R[x]}{\langle x^n-1\rangle}$ is a principal ideal ring.*

(e) *The dual $C^\perp$ of C is the cyclic code*

$$C^\perp = \langle \widehat{F}_0^*, \zeta\widehat{F}_t^*, \ldots, \zeta^{t-1}\widehat{F}_2^*\rangle,$$

and

$$|C^\perp| = \left|\overline{R}\right|^{\sum_{i=1}^{t} i\deg F_{i+1}}.$$

(*f*) *Let* $G = \widehat{F}_0^* + \zeta\widehat{F}_t^* + \cdots + \zeta^{t-1}\widehat{F}_2^*$. *Then* G *is a generating polynomial of* $C^\perp$, *i.e.,* $C^\perp = \langle G \rangle$.

(*g*) C *is self-dual if and only if* F_i *is an associate of* F_j^* *for all* $i, j \in \{0, \ldots, t\}$ *such that* $i + j \equiv 1 \pmod{t+1}$.

If the nilpotency t of ζ is even, then $\langle \zeta^{t/2} \rangle$ is a cyclic self-dual code, which is the so-called trivial self-dual code. Using the structure of cyclic codes above, a necessary and sufficient condition for the existence of nontrivial self-dual cyclic codes were obtained.

Theorem 5.6. (cf. [54, Theorems 4.3, 4.4]) *Assume that* t *is an even integer, then the following conditions are equivalent:*

(*a*) *Nontrivial self-dual cyclic codes exist,*

(*b*) *There exists a basic irreducible factor* $f \in R[x]$ *of* $x^n - 1$ *such that* f *and* f^* *are not associate,*

(*c*) $p^i \not\equiv -1 \pmod{n}$ *for all positive integers* i.

When p is an odd prime, a characterization of integers n, where $p^i \not\equiv -1 \pmod{n}$ for all positive integers i, is still unknown. When $p = 2$, the integer n, where $2^i \not\equiv -1 \pmod{n}$ for all positive integers i, was completely characterized by Moree in Appendix B of [109] and more details in [97].

Theorem 5.7. (cf. [109, Theorem 4], [54, Theorem 4.5]) *Let* R *be a finite chain ring with the maximal ideal* $\langle \zeta \rangle$ *where* $|R| = 2^{lt}$, $|\overline{R}| = 2^l$ *and* t *is the nilpotency of* ζ. *If* t *is even,* n *is odd, then nontrivial self-dual cyclic codes of length* n *over* R *exist if and only if* n *is divisible by either of the followings:*

- *a prime* $\tau \equiv 7 \pmod{8}$, *or*
- *a prime* $\tau \equiv 1 \pmod{8}$, *where the order of* $2 \pmod{\rho}$ *is odd, or*
- *different odd primes* ϱ *and* σ *such that the order of* $2 \pmod{\varrho}$ *is* $2^\varsigma i$ *and the order of* $2 \pmod{\sigma}$ *is* $2^\varsigma j$, *where* i *is odd,* j *is even, and* $\varsigma \geq 1$.

There are cases where $p^i \equiv -1 \pmod{n}$ for some integer i, which leads to the non-existence of nontrivial self-dual cyclic codes for certain values of n and p. Recall that for relatively prime integers a, m, a is called a quadratic residue or quadratic nonresidue of m according to whether the congruence $x^2 \equiv a \pmod{m}$ has a solution or not. We refer to [54] for important properties of quadratic residues and related concepts.

Theorem 5.8. (cf. [54, Corollaries 4.6, 4.7, 4.8]) *Let* R *be a finite chain ring with the maximal ideal* $\langle \zeta \rangle$, $|R| = p^{lt}$, *where* $|\bar{R}| = p^l$, *and* t *is the nilpotency of* ζ, *such that* t *is even. Then*

(*a*) *If n is a prime, then nontrivial self-dual cyclic codes of length n over R do not exist in the following cases*

- $p = 2$, $n \equiv 3, 5 \pmod 8$,
- $p = 3$, $n \equiv 5, 7 \pmod{12}$,
- $p = 5$, $n \equiv 3, 7, 13, 17 \pmod{20}$,
- $p = 7$, $n \equiv 5, 11, 13, 15, 17, 23 \pmod{28}$,
- $p = 11$, $n \equiv 3, 13, 15, 17, 21, 23, 27, 29, 31, 41 \pmod{44}$.

(*b*) *If n is an odd prime different than p, and p is a quadratic nonresidue of n^k, where $k \geq 1$, then nontrivial self-dual cyclic codes of length n over R do not exist.*

(*c*) *If n is an odd prime, then nontrivial self-dual cyclic codes of length n over R do not exist in the following cases:*

- $p \equiv 1 \pmod 4$, *and there exists a positive integer k such that* $\gcd(p, 4n^k) = 1$ *and p is a quadratic nonresidue of $4n^k$,*
- $p \equiv 1 \pmod 8$, *and there exist positive integers i, j such that $i > 2$,* $\gcd(p, 2^i n^j) = 1$ *and p is a quadratic nonresidue of $2^i n^j$.*

Furthermore, let $m = 2^{k_0} p_1^{k_1} \dots p_r^{k_r}$ be the prime factorization of $m > 1$. Assume that $\gcd(p, m) = 1$, *p is a quadratic nonresidue of m, and*

$$p \equiv \begin{cases} 1 \pmod 4, & \text{if } 4 \mid m \text{ but } 8 \nmid m, \\ 1 \pmod 8, & \text{if } 8 \mid m, \end{cases}$$

then there exists an integer $i \in \{1, 2, \dots, r\}$ such that nontrivial self-dual cyclic codes of length p_i over R do not exist.

Remark 5.9.

5.9.1. All results in this section for simple-root cyclic codes also hold for simple-root negacyclic codes, reformulated accordingly. We obtain valid results if we replace "cyclic" by "negacyclic" and $x^n - 1$ by $x^n + 1$.

5.9.2. Most of the techniques that Dinh and López-Permouth [54] used for simple-root cyclic codes over finite chain rings (Theorems $5.4 - 5.8$) are the most general form of the techniques that were first introduced by Pless *et al* [108], [109] in 1996 for simple-root cyclic codes over $\mathbb{Z}_4$. Those were previously extended to the setting of simple-root cyclic codes over $\mathbb{Z}_{p^m}$ by Kanwar and López-Permouth [81] in 1997, and simple-root cyclic codes over Galois rings $\mathrm{GR}(p^a, m)$ by Wan [123] in 1999.

5.9.3. As shown by Hammons *et al.* [71], well-known nonlinear binary codes can be constructed from quaternary linear codes using the Gray map. The Gray map is the map $\mathcal{G} : \mathbb{Z}_4^n \longrightarrow \mathbb{Z}_2^{2n}$, defined as follows: for each $c \in \mathbb{Z}_4^n$, c is uniquely represented as $c = a + 2b$, where $a, b \in \mathbb{Z}_2^n$, then $\mathcal{G}(c) = (b, a \oplus b)$, where $\oplus$ is the componentwise addition of vectors modulo 2. The Gray map is significant because it is an isometry, in the sense that the Lee weight of c is equal to the Hamming weight of $\mathcal{G}(c)$. The Gray map also preserves duality, since for any linear code C over $\mathbb{Z}_4$, $\mathcal{G}(C)$ and $\mathcal{G}(C^{\perp})$ are formally dual, i.e., their Hamming weight enumerators are MacWilliams transforms of each other.

However, the Gray map does not preserve linearity, in fact the Gray image of a linear code is usually not linear. It was shown in [71] that for a $\mathbb{Z}_4$-linear cyclic code of odd length C, its Gray image $\mathcal{G}(C)$ is linear if and only if for any codewords $c_1, c_2 \in C$, $2(c_1 * c_2) \in C$, where $*$ is the componentwise multiplication of vectors, which is defined as $a * b = (a_0 b_0, \ldots, a_{n-1} b_{n-1})$. Indeed, binary nonlinear codes having better parameters than their linear counterparts have been constructed via the Gray map.

Wolfmann [124], [125] showed that the Gray image of a simple-root linear negacyclic code over $\mathbb{Z}_4$ is a (not necessarily linear) cyclic binary code. He classified all $\mathbb{Z}_4$-linear negacyclic codes of odd length and provided a method to determine all linear binary cyclic codes of length $2n$ (n is odd), that are images of negacyclic codes under the Gray map. Therefore, the Gray image of a simple-root negacyclic code over $\mathbb{Z}_4$ is permutation-equivalent to a binary cyclic code under the Nechaev permutation.

6 Repeated-Root Cyclic and Negacyclic Codes over Finite Chain Rings

Except otherwise stated, all codes in this section are repeated-root codes over a finite chain ring R, i.e., the code-length n is divisible by the characteristic p of the residue field $\overline{R}$.

When the code length n is odd, there is a one-to-one correspondence between cyclic and negacyclic codes (single-root or repeated-root) over any finite commutative ring:

Proposition 6.1. (cf.[54, Proposition 5.1]) *Let R be a finite commutative ring and n be an odd integer. The map $\xi : \frac{R[x]}{\langle x^n-1\rangle} \longrightarrow \frac{R[x]}{\langle x^n+1\rangle}$ defined by*

$\xi(f(x)) = f(-x)$, *is a ring isomorphism. In particular, A is an ideal of $\frac{R[x]}{\langle x^n-1\rangle}$ if and only if $\xi(A)$ is an ideal of $\frac{R[x]}{\langle x^n+1\rangle}$. Equivalently, A is a cyclic code of length n over R if and only if $\xi(A)$ is a negacyclic code of length n over R.*

It was shown by Sălăgean in [113] that repeated-root cyclic and negacyclic codes over finite chain rings in general are not principally generated:

Proposition 6.2. (cf. [113, Theorem 3.4]) *Let R be a finite chain ring whose residue field has characteristic p. If $p \mid n$ then:*

(*i*) $\frac{R[x]}{\langle x^n-1\rangle}$ *is not a principal ideal ring.*

(*ii*) *If p is odd or $p = 2$ and R is not a Galois ring then* $\frac{R[x]}{\langle x^n+1\rangle}$ *is not a principal ideal ring.*

(*iii*) *If $p = 2$ and R is a Galois ring then* $\frac{R[x]}{\langle x^n+1\rangle}$ *is a principal ideal ring.*

The description of generators of ideals of $R[x]$ by Gröbner bases were developed in [100], [101], [104] for a chain ring R. Sălăgean [104], [113] used Gröbner bases to obtain structure of repeated-root cyclic codes over finite chain rings, and furthermore provide generating matrices, sizes, and Hamming distances of such codes.

Theorem 6.3. (cf. [104, Theorem 4.2], [113, Theorems 4.1, 5.1, 6.1]) *Let R be a finite chain ring with the maximal ideal $\langle\zeta\rangle$, and t be the nilpotency of ζ. If C is a non-zero cyclic code of length n over R, then*

(*a*) *C admits a set of generators*

$$C = \langle \zeta^{a_0} g_{a_0}, \zeta^{a_1} g_{a_1}, \ldots, \zeta^{a_k} g_{a_k} \rangle$$

such that

(*i*) $0 \le k < t$;

(*ii*) $0 \le a_0 < a_1 < \cdots < a_k < t$;

(*iii*) $g_{a_i} \in R[x]$ *is monic for* $0 \le i \le k$;

(*iv*) $\deg(g_{a_i}) > \deg(g_{a_{i+1}})$ *for* $0 \le i \le k-1$;

(*v*) *For* $0 \le i \le k$, $\zeta^{a_{i+1}} g_{a_i} \in \langle \zeta^{a_{i+1}} g_{a_{i+1}}, \ldots, \zeta^{a_k} g_{a_k} \rangle$ *in* $R[x]$;

(*vi*) $\zeta^{a_0}(x^n - 1) \in \langle \zeta^{a_0} g_{a_0}, \zeta^{a_1} g_{a_1}, \ldots, \zeta^{a_k} g_{a_k} \rangle$ *in* $R[x]$.

(*b*) *This set $\{\zeta^{a_0} g_{a_0}, \zeta^{a_1} g_{a_1}, \ldots, \zeta^{a_k} g_{a_k}\}$ of generator is a strong Gröbner basis. It is not necessarily unique. However, the cardinality k of the basis, the degrees of its polynomials and the exponents $a_0, a_1, \ldots, a_k$ are unique.*

(*c*) *Denote $d_i = \deg(g_{a_i})$ for $0 \le i \le k$, and $d_{-1} = n$. Then the matrix consisting of the rows corresponding to the codewords $\zeta^{a_i} x^j g_{a_i}$, with $0 \le i \le k$ and $0 \le j \le d_{i-1} - d_i - 1$, is a generator matrix for C.*

(*d*) *The number of codewords in* C *is*

$$|C| = \left|\overline{R}\right|^{\sum_{i=0}^{k}(t-a_i)(d_{i-1}-d_i)}.$$

(*e*) *The Hamming distance of* C *equals the Hamming distance of* $\langle \overline{g_{a_k}} \rangle$.

(*f*) *The results in parts* $(a), (b), (c), (d), (e)$ *hold for negacyclic codes, reformulated accordingly by replacing* $x^n - 1$ *by* $x^n + 1$.

In fact, Theorem 6.3(a) provides a structure theorem for both simple-root and repeated-root cyclic codes. Conditions (v) and (vi) imply that $g_{a_k} \,|\, g_{a_{k-1}} \,|\, \ldots \,|\, g_{a_0} \,|\, (x^n - 1)$. In the simple-root case, the conditions (v) and (vi) can be replaced by the stronger condition $g_{a_k} \,|\, g_{a_{k-1}} \,|\, \ldots \,|\, g_{a_0} \,|\, (x^n - 1)$, as in Proposition 5.2, giving a structure theorem for simple-root cyclic codes. For repeated-root cyclic codes, conditions (v) and (vi) can not be improved in general, [104, Example 3.3] gave cyclic codes for

which no set of generators of the form given in Theorem 6.3(a) has the property $g_{a_k} \,|\, g_{a_{k-1}} \,|\, \ldots \,|\, g_{a_0} \,|\, (x^n - 1)$.

Most of the research on repeated-root codes concentrated on the situation where the chain ring is a Galois ring, i.e., $R = \mathrm{GR}(p^a, m)$. In this case, using polynimial representation, it is easy to show that the ideals $\langle x - 1, p\rangle$, and $\langle x + 1, p\rangle$ are the sets of non-invertible elements of $\frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{p^s}-1\rangle}$, and $\frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$, respectively. Therefore, $\frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{p^s}-1\rangle}$, and $\frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ are local rings whose maximal ideals are $\langle x - 1, p\rangle$, and $\langle x + 1, p\rangle$. When $a \geq 2$, $\mathrm{GR}(p^a, m)$ is not a field, and Proposition 6.2 gives us information on the ambient rings of cyclic and negecyclic codes of length p^s over $\mathrm{GR}(p^a, m)$:

Proposition 6.4. *Let* $a \geq 2$*, then the following conditions hold true:*

(*i*) $\frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{p^s}-1\rangle}$ *is a local ring with maximal ideal* $\langle x - 1, p\rangle$*, but it is not a chain ring.*

(*ii*) *If* p *is odd,* $\frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ *is a local ring with maximal ideal* $\langle x+1, p\rangle$*, but it is not a chain ring*

(*iii*) *If* $p = 2$*,* $\frac{\mathrm{GR}(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ *is a chain ring with maximal ideal* $\langle x + 1\rangle$.

When $a = 1$, the Galois ring $\mathrm{GR}(p^a, m)$ is the Galois field $\mathbb{F}_{p^m}$. Dinh [44] showed that the ambient rings $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1\rangle}$ and $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}+1\rangle}$ are chain rings, and used this to establish structure of cyclic and negacyclic codes of length p^s over $\mathbb{F}_{p^m}$, as well as the Hamming distances of all such codes:

Theorem 6.5 (cf. [44]). *The ring* $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1\rangle}$ *and* $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}+1\rangle}$ *are chain ring with maximal ideals* $\langle x - 1\rangle$*,* $\langle x + 1\rangle$*, respectively. Cyclic and negacyclic codes of length* p^s *over* $\mathbb{F}_{p^m}$ *are precisely the ideals* $\langle (x-1)^i\rangle$ *of* $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1\rangle}$*, and* $\langle (x+1)^i\rangle$ *of* $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}+1\rangle}$*, for* $i \in \{0, 1, \ldots, p^s\}$*. The*

cyclic code $\langle (x-1)^i \rangle \subseteq \frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1\rangle}$, *and negacyclic code* $\langle (x+1)^i \rangle \subseteq \frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}+1\rangle}$ *each has* $p^{m(p^s-i)}$ *codewords. Their dual codes are the cyclic code* $\langle (x-1)^{p^s-i} \rangle \subseteq \frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1\rangle}$ *and negacyclic code* $\langle (x+1)^{p^s-i} \rangle \subseteq \frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}+1\rangle}$, *respectively. The cyclic code* $\langle (x-1)^i \rangle \subseteq \frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1\rangle}$ *and negacyclic code* $\langle (x+1)^i \rangle \subseteq \frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1\rangle}$ *have the same Hamming distance* d_i, *which is determined by:*

$$d_i = \begin{cases} 1, & \text{if } \ i = 0 \\ \beta + 2, & \text{if } \ \beta\, p^{s-1} + 1 \le i \le (\beta+1)\, p^{s-1} \\ & \quad \text{where } \ 0 \le \beta \le p-2 \\ (t+1)p^k, & \text{if } \ p^s - p^{s-k} + (t-1)p^{s-k-1} + 1 \le i \le p^s - p^{s-k} + tp^{s-k-1} \\ & \quad \text{where } \ 1 \le t \le p-1, \ \text{ and } \ 1 \le k \le s-1 \\ 0, & \text{if } \ i = p^s. \end{cases}$$

When $p = 2$, there is no one-to-one correspondence between cyclic and negacyclic codes of length 2^s over $\mathrm{GR}(2^a, m)$ (Proposition 6.1 does not hold when the code length is even). In 2005, Dinh gave the structure of such negacyclic codes, and the Hamming distances of most of them in [40], and later on, in [46], obtained the Hamming and homogeneous distances[8] of all of them, using their structure in [40], and the Hamming distances of 2^m-ary cyclic codes in Theorem 6.5:

Theorem 6.6. (cf. [40], [46]) *The ring* $\frac{\mathrm{GR}(2^a,m)[x]}{\langle x^{2^s}+1\rangle}$ *is a chain ring with maximal ideal* $\langle x+1\rangle$ *and residue field* $\mathrm{GF}(2^m)$. *Negacyclic codes of length* 2^s *over the Galois ring* $\mathrm{GR}(2^a, m)$ *are*

[8]The homogeneous weight was first introduced in [32] (see also [33], [34]) over integer residue rings, and later over finite Frobenius rings. This weight has numerous applications for codes over finite rings, such as constructing extensions of the Gray isometry to finite chain rings [66], [72], [73], or providing a combinatorial approach to MacWilliams equivalence theorems (cf. [90], [91], [126]) for codes over finite Frobenius rings [67]. The homogeneous distance of codes over the Galois rings $\mathrm{GR}(2^a, m)$ is defined as follows.

Let $a \ge 2$, the *homogeneous weight* on $\mathrm{GR}(2^a, m)$ is a weight function on $\mathrm{GR}(2^a, m)$ given as

$$\mathrm{wt_h} : \mathrm{GR}(2^a, m) \longrightarrow \mathbb{N}, \qquad r \mapsto \begin{cases} 0, & \text{if } \ r = 0 \\ (2^m - 1)\, 2^{m(a-2)}, & \text{if } \ r \in \mathrm{GR}(2^a, m) \setminus 2^{a-1}\, \mathrm{GR}(2^a, m) \\ 2^{m(a-1)}, & \text{if } \ r \in 2^{a-1}\, \mathrm{GR}(2^a, m) \setminus \{0\}. \end{cases}$$

The homogeneous weight of a codeword $(c_0, c_1, \ldots, c_{n-1})$ of length n over $\mathrm{GR}(2^a, m)$ is the rational sum of the homogeneous weights of its components, i.e.,

$$\mathrm{wt_h}(c_0, c_1, \ldots, c_{n-1}) = \mathrm{wt_h}(c_0) + \mathrm{wt_h}(c_1) + \cdots + \mathrm{wt_h}(c_{n-1}).$$

The *homogeneous distance* (or minimum homogeneous weight) d_h of a linear code C is the minimum homogeneous weight of nonzero codewords of C:

$$d_\mathrm{h}(C) = \min\{\mathrm{wt_h}(x-y) : x, y \in C, \ x \ne y\} = \min\{\mathrm{wt_h}(c) : c \in C, \ c \ne 0\}.$$

precisely the ideals $\langle (x+1)^i \rangle$, $0 \le i \le 2^s a$, *of* $\frac{\mathrm{GR}(2^a,m)[x]}{\langle x^{2^s}+1\rangle}$. *Each negacyclic code* $C = \langle (x+1)^i \rangle$ *has* $2^{m(2^s a-i)}$ *codewords, its dual is the negacyclic code* $\langle (x+1)^{2^s a-i} \rangle$, *which contains* 2^{mi} *codewords. The Hamming distance* $d(C)$ *and homogeneous distances* $d_{\mathrm{h}}(C)$ *are completely determined as follows:*

$$d(C) = \begin{cases} 0 & \text{if} \quad i = 2^s a \\ 1 & \text{if} \quad 0 \le i \le 2^s(a-1) \\ 2 & \text{if} \quad 2^s(a-1)+1 \le i \le 2^s(a-1)+2^{s-1} \\ 2^{k+1} & \text{if} \quad 2^s(a-1)+2^s-2^{s-k}+1 \le i \le 2^s(a-1)+2^s-2^{s-k}+2^{s-k-1}, \\ & \quad \text{i.e.,} \ \ 2^s(a-1)+1+\sum_{l=1}^{k} 2^{s-l} \le i \le 2^s(a-1)+\sum_{l=1}^{k+1} 2^{s-l}, \\ & \quad \text{where} \ \ 1 \le k \le s-1. \end{cases}$$

$$d_{\mathrm{h}}(C) = \begin{cases} 0 & \text{if} \quad i = 2^s a \\ (2^m-1)\,2^{m(a-2)} & \text{if} \quad 0 \le i \le 2^s(a-2) \\ 2^{m(a-1)} & \text{if} \quad 2^s(a-2)+1 \le i \le 2^s(a-1) \\ 2^{m(a-1)+1} & \text{if} \quad 2^s(a-1)+1 \le i \le 2^s(a-1)+2^{s-1} \\ 2^{m(a-1)+k+1} & \text{if} \quad 2^s(a-1)+2^s-2^{s-k}+1 \le i \le 2^s(a-1)+2^s-2^{s-k}+2^{s-k-1}, \\ & \quad \text{i.e.,} \ \ 2^s(a-1)+1+\sum_{l=1}^{k} 2^{s-l} \le i \le 2^s(a-1)+\sum_{l=1}^{k+1} 2^{s-l}, \\ & \quad \text{where} \ \ 1 \le k \le s-1. \end{cases}$$

If the dimension $m = 1$, the Galois ring $\mathrm{GR}(2^a, m)$ is the ring $\mathbb{Z}_{2^a}$. [43] Established the Hamming, homogeneous, Lee[9], and Euclidean[10] distances of all negacyclic code of length

[9]The Lee distance, named after its originator [85], is a good alternative to the Hamming distance in algebraic coding theory, especially for codes over $\mathbb{Z}_4$. For instance, the Lee distance plays an important role in constructing an isometry between binary and quarternary codes via the Gray map in a landmark paper of the theory of codes over rings (cf. [23], [71]). Classically, for codes over finite fields, Berlekamp's negacyclic codes [9], [10], the class of cyclic codes investigated in [31], the class of alternant codes discussed in [112], are examples of codes designed with the Lee metric in mind.

Let $z \in \mathbb{Z}_{2^a}$, the *Lee value* of z, denoted by $|z|_L$, is given as

$$|z|_L = \begin{cases} z, & \text{if} \ \ 0 \le z \le 2^{a-1} \\ 2^a - z, & \text{if} \ \ 2^{a-1} < z \le 2^a - 1 \end{cases}$$

The *Lee weight* of a codeword $(c_0, c_1, \ldots, c_{n-1})$ of length n over $\mathbb{Z}_{2^a}$ is the rational sum of the Lee values of its components:

$$\mathrm{wt}_L(c_0, c_1, \ldots, c_{n-1}) = |c_0|_L + |c_1|_L + \cdots + |c_{n-1}|_L.$$

The *Lee distance* (or *minimum Lee weight*) d_L of a linear code C is the minimum Lee weight of nonzero codewords of C:

$$d_L(C) = \min\{\mathrm{wt}_L(x-y) : x, y \in C, \ x \ne y\} = \min\{\mathrm{wt}_L(c) : c \in C, \ c \ne 0\}.$$

[10]As codes over $\mathbb{Z}_4$ have gained more prominence, interesting connections with binary codes and unimod-

2^s over $\mathbb{Z}_{2^a}$:

Theorem 6.7. (cf. [43]) *Let C be a negacyclic code of length 2^s over $\mathbb{Z}_{2^a}$. Then $C = \langle (x+1)^i \rangle \subseteq \frac{\mathbb{Z}_{2^a}[x]}{\langle x^{2^s}+1 \rangle}$, for $i \in \{0, 1, \ldots, 2^s a\}$, and the Hamming distance $d(C)$, homogeneous distance $d_{\mathrm{h}}(C)$, Lee distance $d_L(C)$, and Euclidean distance $d_E(C)$ of C are determined by*

- $$d(C) = \begin{cases} 0 & \text{if } \ i = 2^s a \\ 1 & \text{if } \ 0 \le i \le 2^s(a-1) \\ 2 & \text{if } \ 2^s(a-1)+1 \le i \le 2^s(a-1)+2^{s-1} \\ 2^{k+1} & \text{if } \ 2^s(a-1)+1+\sum\limits_{j=1}^{k} 2^{s-j} \le i \le 2^s(a-1)+\sum\limits_{j=1}^{k+1} 2^{s-j}, \quad \text{for } \ 1 \le k \le s-1 \end{cases}$$

- $$d_{\mathrm{h}}(C) = \begin{cases} 0 & \text{if } \ i = 2^s a \\ 2^{a-2} & \text{if } \ 0 \le i \le 2^s(a-2) \\ 2^{a-1} & \text{if } \ 2^s(a-2)+1 \le i \le 2^s(a-1) \\ 2^a & \text{if } \ 2^s(a-1)+1 \le i \le 2^s(a-1)+2^{s-1} \\ 2^{a+k} & \text{if } \ 2^s(a-1)+1+\sum\limits_{j=1}^{k} 2^{s-j} \le i \le 2^s(a-1)+\sum\limits_{j=1}^{k+1} 2^{s-j}, \quad \text{for } \ 1 \le k \le s-1 \end{cases}$$

- $$d_L(C) = \begin{cases} 0 & \text{if } \ i = 2^s a \\ 1 & \text{if } \ i = 0 \\ 2 & \text{if } \ 1 \le i \le 2^s \\ 2^{l+1} & \text{if } \ 2^s l+1 \le i \le 2^s(l+1), \quad \text{for } \ 1 \le l \le a-2 \\ 2^a & \text{if } \ 2^s(a-1)+1 \le i \le 2^s(a-1)+2^{s-1} \\ 2^{a+k} & \text{if } \ 2^s(a-1)+1+\sum\limits_{j=1}^{k} 2^{s-j} \le i \le 2^s(a-1)+\sum\limits_{j=1}^{k+1} 2^{s-j}, \quad \text{for } \ 1 \le k \le s-1 \end{cases}$$

---

ular lattices were found with relations to codes over $\mathbb{Z}_{2k}$ (cf. [5]). The connection between codes over $\mathbb{Z}_4$ and unimodular lattices prompted the definition of the Euclidean weight of codewords of length n over $\mathbb{Z}_4$ (cf. 14], [15]), and more generally, over $\mathbb{Z}_{2k}$ (cf. [5], [58], [59]).

Let $z \in \mathbb{Z}_{2^a}$, the *Euclidean weight* of z, denoted by $|z|_E$, is given as

$$|z|_E = \begin{cases} z^2, & \text{if } \ 0 \le z \le 2^{a-1} \\ (2^a - z)^2, & \text{if } \ 2^{a-1} < z \le 2^a - 1 \end{cases}$$

The *Euclidean weight* of a codeword $(c_0, c_1, \ldots, c_{n-1})$ of length n over $\mathbb{Z}_{2^a}$ is the rational sum of the Euclidean weights of its components:

$$\mathrm{wt}_E(c_0, c_1, \ldots, c_{n-1}) = |c_0|_E + |c_1|_E + \cdots + |c_{n-1}|_E.$$

The *Euclidean distance* (or *minimum Euclidean weight*) d_E of a linear code C is the minimum Euclidean weight of nonzero codewords of C:

$$d_E(C) = \min\{\mathrm{wt}_E(x-y) : x, y \in C, \ x \ne y\} = \min\{\mathrm{wt}_E(c) : c \in C, \ c \ne 0\}.$$

$$\bullet\ d_E(C) = \begin{cases} 0 & \text{if } i = 2^s a \\ 1 & \text{if } i = 0 \\ 2^{2l+1} & \text{if } 2^s l + 1 \le i \le 2^s l + 2^{s-1}, \text{ for } 0 \le l \le a-2 \\ 2^{2l+2} & \text{if } 2^s l + 2^{s-1} + 1 \le i \le 2^s(l+1), \text{ for } 0 \le l \le a-2 \\ 2^{2a-1} & \text{if } 2^s(a-1) + 1 \le i \le 2^s(a-1) + 2^{s-1} \\ 2^{2a+k-1} & \text{if } 2^s(a-1) + 1 + \sum_{j=1}^{k} 2^{s-j} \le i \le 2^s(a-1) + \sum_{j=1}^{k+1} 2^{s-j}, \text{ for } 1 \le k \le s-1. \end{cases}$$

In the special case when the alphabet is $\mathbb{Z}_4$, or its Galois extension $\mathrm{GR}(4, m)$, repeated-root cyclic and negacyclic codes have been studied in more details. Among other partial results, the structures of negacyclic and cyclic codes over $\mathbb{Z}_4$ of any length were respectively provided by Blackford in 2003 [12], and Dougherty and Ling in 2006 [60].

The Discrete Fourier Transform is an useful tool to study structures of codes, for instance, it was used by Blackford [12], [13], and Dougherty and Ling [60] to recover an tuple c from its Mattson-Solomon polynomial. In 2003, Blackford used the Discrete Fourier Transform to give a decomposition of the ambient ring $\frac{\mathbb{Z}_4[x]}{\langle x^{2^a n}+1\rangle}$ of cyclic codes of length $2^a n$ over $\mathbb{Z}_4$ as a direct sum of $\frac{\mathrm{GR}(4,m_i)[u]}{\langle u^{2^a}+1\rangle}$. The rings $\frac{\mathrm{GR}(4,m_i)[u]}{\langle u^{2^a}+1\rangle}$ are the ambient ring of negacyclic codes of length 2^a over $\mathrm{GR}(4, m_i)$, which were shown to be chain rings by Blackford, and later by Dinh [40], for the more general case over $\mathrm{GR}(2^z, m_i)$.

Theorem 6.8. (cf. [12, Lemma 2, Theorem 1]) *Let n be an odd positive integer, and a be any non-negative integer. Let I denote a complete set of representatives of the 2-cyclotomic cosets modulo n, and for each $i \in I$, let m_i be the size of the 2-cyclotomic coset containing i. Then*

(a) *For any $m \ge 1$, the ring $\frac{\mathrm{GR}(4,m)[u]}{\langle u^{2^a}+1\rangle}$ is a chain ring with maximal ideal $\langle u+1\rangle$, and residue field $\mathbb{F}_{2^m}$. Its ideals, i.e., negacyclic codes of length 2^a over $\mathrm{GR}(4, m)$ are $\langle 0\rangle$, $\langle 1\rangle$, $\langle (u+1)^i\rangle$, and $\langle 2(u+1)^i\rangle$, where $1 \le i \le 2^a - 1$.*

(b) *The map*

$$\phi : \frac{\mathbb{Z}_4[x]}{\langle x^{2^a n}+1\rangle} \longrightarrow \bigoplus_{i\in I} \frac{\mathrm{GR}(4, m_i)[u]}{\langle u^{2^a}+1\rangle},$$

given by

$$\gamma(c(x)) = [\widehat{c}_i]_{i\in I}\,,$$

where $(\widehat{c}_0, \widehat{c}_1, \ldots, \widehat{c}_{n-1})$ is the Discrete Fourier Transform of $c(x)$, is a ring isomorphism.

(c) *Each negacyclic code of length* $2^a n$ *over* $\mathbb{Z}_4$*, i.e., an ideal of the ring* $\frac{\mathbb{Z}_4[x]}{\langle x^{2^a n}+1\rangle}$*, is isomorphic to* $\oplus_{i\in I} C_i$*, where* C_i *is an ideal of* $\frac{\mathrm{GR}(4,m_i)[u]}{\langle u^{2^a}+1\rangle}$ *(such ideals are provided in part (a)).*

Using this, Blackford went on to show that $\frac{\mathbb{Z}_4[x]}{\langle x^{2^a n}+1\rangle}$ is a pricipal ideal ring, as its ideals are principally generated, and established a concatenated structure of negacyclic codes over $\mathbb{Z}_4$:

Theorem 6.9. (cf. [12, Theorems 2, 3]B03a) *Let* C *be a negacyclic code of length* $2^a n$ *over* $\mathbb{Z}_4$*, i.e., an ideal of the ring* $\frac{\mathbb{Z}_4[x]}{\langle x^{2^a n}+1\rangle}$*. Then*

(a) $C = \langle g(x)\rangle$*, where* $g(x) = \prod_{i=0}^{2^{a+1}} [g_i(x)]^i$*, and* $\{g_i(x)\}$ *are monic coprime divisors of* $x^n - 1$ *in* $\mathbb{Z}_4[x]$*.*

(b) *Any codeword of* C *is equivalent to an* $(2^a n)$*-tuple of the form* $(\mathbf{b}_0 \,|\, \mathbf{b}_1 \,|\, \cdots \,|\, \mathbf{b}_{2^a-1})$*, where*

$$\mathbf{b}_i = \sum_{j=0}^{2^a-1} \overline{\binom{j}{i}}\, \mathbf{a}_j, \qquad \overline{\binom{j}{i}} = \binom{j}{i} \pmod 2,$$

and

$$\mathbf{a}_j \in \langle g_{j+1} \ldots g_{2^{a+1}} + 2 g_{j+2^a+1} \ldots g_{2^{a+1}} \rangle \subseteq \frac{\mathbb{Z}_4[x]}{\langle x^n - 1\rangle}.$$

We now turn our attention to repeated-root cyclic codes over $\mathbb{Z}_4$. In 2003, Abualrub and Oehmke [1] classified cyclic codes of length 2^k over $\mathbb{Z}_4$ by their generators, and after that they derived in 2004 a mass formula for the number of such codes [2]. In 2006, Dougherty and Ling [60] generalized that to give a classification of cyclic codes of length 2^k over Galois ring $\mathrm{GR}(4, m)$:

Theorem 6.10. (cf. [60, Lemma 2.3, Theorem 2.6]) *Let* η *be a primitive* $(2^m - 1)$*th root of unity, and the Teichmüller set of representatives* $\mathcal{T}_m = \{0, 1, \eta, \eta^2, \ldots, \eta^{2^m-2}\}$*. Then the ambient ring* $\frac{\mathrm{GR}(4,m)[u]}{\langle u^{2^k}-1\rangle}$ *is a local ring with maximal ideal* $\langle 2, u-1\rangle$*, and residue field* $\mathbb{F}_{2^m}$*. Cyclic codes of length* 2^k *over* $\mathrm{GR}(4, m)$*, i.e., ideals of* $\frac{\mathrm{GR}(4,m)[u]}{\langle u^{2^k}-1\rangle}$*, are*

- $\langle 0\rangle$, $\langle 1\rangle$,
- $\langle 2(x-1)^i\rangle$,
  where $0 \le i \le 2^k - 1$,
- $\left\langle (x-1)^i + 2\sum_{j=0}^{i-1} s_j (x-1)^j \right\rangle$,
  where $1 \le i \le 2^k - 1$*, and* $s_j \in \mathcal{T}_m$ *for all* j*,*

- $\left\langle 2(u-1)^l, (x-1)^i + 2\sum_{j=0}^{i-1} s_j (x-1)^j \right\rangle$,
  where $1 \le i \le 2^k - 1$, $l < i$, *and* $s_j \in \mathcal{T}_m$ *for all* j.

  Furthermore, the number of such cyclic codes is

$$\mathcal{N}(m) = 5 + 2^{2^{k-1}m} + 2^m \left(5 \cdot 2^m - 1\right) \frac{2^{m(2^{k-1}-1)} - 1}{(2^m - 1)^2} - 4 \cdot \frac{2^{k-1} - 1}{2^m - 1}.$$

In 2003, using the Discrete Fourier Transform, Blackford [13] gave the structure of cyclic codes of length $2n$ (n is odd) over $\mathbb{Z}_4$. Later, in 2006, Dougherty and Ling [60] generalized that to obtain a description of cyclic codes of any length over $\mathbb{Z}_4$ as a direct sum of cyclic codes of length 2^k over $\mathrm{GR}(4, m_\alpha)$.

Theorem 6.11. (cf. [13, Theorem 2], [60, Theorem 3.2, Corollaries 3.3, 3.4] *Let n be an odd positive integer, and k be any non-negative integer. Let J denote a complete set of representatives of the 2-cyclotomic cosets modulo n, and for each $\alpha \in J$, let m_α be the size of the 2-cyclotomic coset containing α. Then*

(*a*) *The map*

$$\gamma : \frac{\mathbb{Z}_4[x]}{\langle x^{2^k n} - 1\rangle} \longrightarrow \bigoplus_{\alpha \in J} \frac{\mathrm{GR}(4, m_\alpha)[u]}{\langle u^{2^k} - 1\rangle},$$

given by

$$\gamma(c(x)) = \left[\widehat{c}_\alpha\right]_{\alpha \in J},$$

where $(\widehat{c}_0, \widehat{c}_1, \ldots, \widehat{c}_{n-1})$ is the Discrete Fourier Transform of $c(x)$, is a ring isomorphism.

(*b*) *Each cyclic code of length $2^k n$ over $\mathbb{Z}_4$, i.e., an ideal of the ring $\frac{\mathbb{Z}_4[x]}{\langle x^{2^k n} - 1\rangle}$, is isomorphic to $\oplus_{\alpha \in J} C_\alpha$, where C_α is an ideal of $\frac{\mathrm{GR}(4, m_\alpha)[u]}{\langle u^{2^k} - 1\rangle}$ (such ideals are classified in Theorem).*

(*c*) *The number of distinct cyclic code of length $2^k n$ over $\mathbb{Z}_4$ is $\prod_{\alpha \in J} \mathcal{N}(m_\alpha)$, where $\mathcal{N}(m_\alpha)$ is the number of cyclic codes of length 2^k over $\mathrm{GR}(4, m_\alpha)$, which is given in Theorem.*

This decomposition of cyclic codes were then used to completely determine the generators of all cyclic codes, and their sizes:

Theorem 6.12. (cf. [60, Theorems 4.2, 4.3]) *Let n be an odd positive integer, and k be any non-negative integer, and let C be a cyclic code of length $2^k n$ over $\mathbb{Z}_4$, i.e., C is an ideal of the ring $\frac{\mathbb{Z}_4[x]}{\langle x^{2^k n} - 1\rangle}$. Then*

(*a*) *C is of the form*

$$\left\langle p(x^{2^k})\prod_{i=0}^{2^k-1} q_i(x^{2^k})\prod_{i=i}^{2^k-1}\left(\prod_T \widetilde{r_{i,T}(x)}^{\,i}\right)\prod_{i=i}^{2^k-1}\left(\prod_{l=0}^{i-1}\widetilde{s_{i,l}(x)}^{\,i}\right)\right.$$
$$\left. 2p(x^{2^k})\prod_{i=0}^{2^k-1} q_i(x)^i\prod_{i=i}^{2^k-1}\left(\prod_T r_{i,T}(x)^T\right)\prod_{i=i}^{2^k-1}\left(\prod_{l=0}^{i-1} s_{i,l}(x)^l\right)\right\rangle,$$

where

$$x^n-1=p(x)\left(\prod_{i=0}^{2^k-1} q_i(x)\right)\left(\prod_{i=i}^{2^k-1}\left(\prod_T r_{i,T}(x)\right)\right)\left(\prod_{i=i}^{2^k-1}\left(\prod_{l=0}^{i-1} s_{i,l}(x)\right)\right)\,y(x),$$

and $\widetilde{r_{i,T}(x)} = r_{i,T}(x) \pmod 2$, $\widetilde{s_{i,l}(x)} = s_{i,l}(x) \pmod 2$, *and for each i, the product $\prod_T$ is taken over all possible values of T as follows:*

- *if* $1 \le i \le 2^{k-1}$, *then* $T = i$,
- *if* $2^{k-1} < i < 2^{k-1}+t$ $(t>0)$, *then* $T = 2^{k-1}$,
- *if* $i = 2^{k-1}+t$ $(t>0)$, *then* $2^{k-1} \le T \le i$,
- *if* $i > 2^{k-1}+t$ $(t>0)$, *then* $T = 2^{k-1}$ *or* $2^k - i + t$.

(*b*) *The number of codewords in C is*

$$|C| = 4^{2^k \deg(p)}\prod_{i=0}^{2^k-1} 2^{(2^k-i)\deg(q_i)}\prod_{i=1}^{2^k-1}\left(\prod_T 2^{(2^{k+1}-i-T)\deg(r_{i,T})}\right)\prod_{i=1}^{2^k-1}\left(\prod_{l=0}^{i-1} 2^{(2^{k+1}-i-l)\deg(s_{i,l})}\right).$$

There are four finite commutative rings of four elements, namely, the Galois field $\mathbb{F}_4$, the ring of integers modulo four $\mathbb{Z}_4$, the ring $\mathbb{F}_2+u\mathbb{F}_2$ where $u^2=0$, and the ring $\mathbb{F}_2+v\mathbb{F}_2$ where $v^2=v$. The first three are chain rings, while the last one, $\mathbb{F}_2+v\mathbb{F}_2$, is not. Indeed, $\mathbb{F}_2+v\mathbb{F}_2 \cong \mathbb{F}_2\times\mathbb{F}_2$, which is not even a local ring. The ring $\mathbb{F}_2+u\mathbb{F}_2$ consists of all binary polynomials of degree 0 and 1 in indeterminate u, it is closed under binary polynomial addition and multiplication modulo u^2. Thus, $\mathbb{F}_2+u\mathbb{F}_2 = \frac{\mathbb{F}_2[u]}{\langle u^2\rangle} = \{0,1,u,\overline{u}=u+1\}$ is a chain ring with maximal ideal $\{0,u\}$.

The addition of $\mathbb{F}_2+u\mathbb{F}_2$ is similar to that of the Galois field $\mathbb{F}_4=\{0,1,\xi,\xi^2=\xi+1\}$, where u is replaced by ξ. The multiplication of $\mathbb{F}_2+u\mathbb{F}_2$ is similar to the multiplication of the ring $\mathbb{Z}_4$, where u is replaced by 2. In fact, $(\mathbb{F}_2+u\mathbb{F}_2,+)\cong(\mathbb{F}_4,+)$, and $(\mathbb{F}_2+u\mathbb{F}_2,*)\cong(\mathbb{F}_4,*)$. Thus, $\mathbb{F}_2+u\mathbb{F}_2$ lies between $\mathbb{F}_4$ and $\mathbb{Z}_4$, in the sense that it is additively analogous to $\mathbb{F}_4$, and multiplicatively analogous to $\mathbb{Z}_4$. In 2009, Dinh [45] established the structure of all

constacyclic codes of length 2^s over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$, for any positive integer m. Of course, over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$, cyclic and negacyclic codes coincide, their structure, and sizes are as follows:

Theorem 6.13. (cf. [45])

(*a*) *The ring* $\frac{(\mathbb{F}_{2^m}+u\mathbb{F}_{2^m})[x]}{\langle x^{2^s}+1\rangle}$ *is a local ring with maximal ideal* $\langle u, x+1\rangle$*, but it is not a chain ring.*

(*b*) *Cyclic codes of length* 2^s *over* $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ *are precisely the ideals of the ring* $\frac{(\mathbb{F}_{2^m}+u\mathbb{F}_{2^m})[x]}{\langle x^{2^s}+1\rangle}$*, which are*

- Type 1: (trivial ideals)

$$\langle 0\rangle,\ \langle 1\rangle$$

- Type 2: (principal ideals with nonmonic polynomial generators)

$$\langle u(x+1)^i\rangle,$$

  where $0 \le i \le 2^s-1$,

- Type 3: (principal ideals with monic polynomial generators)

$$\left\langle (x+1)^i + u(x+1)^t h(x)\right\rangle,$$

  where $1 \le i \le 2^s-1$, $0 \le t < i$, and either $h(x)$ is 0 or $h(x)$ is a unit where it can be represented as $h(x)=\sum_j h_j(x+1)^j$, with $h_j \in \mathbb{F}_{2^m}$, and $h_0 \neq 0$.

- Type 4: (nonprincipal ideals)

$$\left\langle (x+1)^i + u\sum_{j=0}^{\kappa-1} c_j(x+1)^j, u(x+1)^\kappa\right\rangle,$$

  where $1 \le i \le 2^s-1$, $c_j \in \mathbb{F}_{2^m}$, and $\kappa < T$, where T is the smallest integer such that $u(x+1)^T \in \left\langle (x+1)^i + u\sum_{j=0}^{i-1} c_j(x+1)^j\right\rangle$; or equivalently,

$$\left\langle (x+1)^i + u(x+1)^t h(x), u(x+1)^\kappa\right\rangle,$$

  with $h(x)$ as in Type 3, and $\deg(h) \le \kappa - t - 1$.

(*c*) *The number of distinct cyclic codes of length* 2^s *over* $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ *is*

$$\frac{2^{m(2^{s-1}-1)}(2^{2m}+2^m+2)-2^{2m+1}-2}{(2^m-1)^2} + \frac{6\cdot 2^{m(2^s-1)}-2^{s+1}-1}{2^m-1} + 2^{m2^{s-1}} + 4\cdot 2^{m(2^{s-1}-1)} + 3\cdot 2^{s-1} - 1.$$

(*d*) *Let C be a cyclic code of length 2^s over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$, as classified in (b). Then the number of codewords n_C of C is given as follows.*

- If $C = \langle 0 \rangle$, then $n_C = 1$.
- If $C = \langle 1 \rangle$, then $n_C = 2^{m2^{s+1}}$.
- If $C = \langle u(x+1)^i \rangle$, where $0 \le i \le 2^s - 1$, then $n_C = 2^{m(2^s - i)}$.
- If $C = \langle (x+1)^i \rangle$, where $1 \le i \le 2^s - 1$, then $n_C = 2^{2m(2^s - i)}$.
- If $C = \langle (x+1)^i + u(x+1)^t h(x) \rangle$, where $1 \le i \le 2^s - 1$, $0 \le t < i$, and $h(x)$ is a unit, then

$$n_C = \begin{cases} 2^{2m(2^s - i)}, & \text{if } 1 \le i \le 2^{s-1} + \frac{t}{2} \\ 2^{m(2^s - t)}, & \text{if } 2^{s-1} + \frac{t}{2} < i \le 2^s - 1 \end{cases}.$$

- If $C = \langle (x+1)^i + u(x+1)^t h(x), u(x+1)^\kappa \rangle$, where $1 \le i \le 2^s - 1$, $0 \le t < i$, either $h(x)$ is 0 or $h(x)$ is a unit, and

$$\kappa < T = \begin{cases} i, & \text{if } h(x) = 0 \\ \min\{i, 2^s - i + t\}, & \text{if } h(x) \neq 0 \end{cases},$$

then $n_C = 2^{m(2^{s+1} - i - \kappa)}$.

Remark 6.14.

- For any odd prime p, the structure of all constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, for any positive integer m, is provided in [47]. Duals and all self-dual codes among such codes are given in [49].
- Algebraic structure of all constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ are completely determinded by Dinh et al. in [29], [57].
- Structure of all constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ are given by Dinh et al. in [48], [50], [51], [52], [56].

7 Some Generalizations

In this section we briefly mention but a few alternative directions in which the theories studied here have been extended.

As mentioned in Section 4, for a unit λ the ring R, the λ-constacyclic (or λ-twisted) shift τ_λ on R^n is the shift

$$\tau_\lambda(x_0, x_1, \ldots, x_{n-1}) = (\lambda x_{n-1}, x_0, x_1, \cdots, x_{n-2}).$$

A code C is said to be a *quasi-cyclic code of index* l if C is closed under the cyclic shift of l symbols τ^l, i.e., if $\tau^l(C) = C$, and C is called a λ-*quasi-twisted code of index* l if it is closed under the λ-twisted shift of l symbols, i.e., $\tau_\lambda^l(C) = C$. Of course, when $\lambda = 1$, a λ-quasi-twisted code of index l is just a quasi-cyclic code of index l, and it becomes a λ-constacyclic code if $l = 1$. It is easy to see that a code of length n is λ-quasi-twisted (quasi-cyclic) of index l if and only if it is λ-quasi-twisted (quasi-cyclic) of index $\gcd(l, n)$. Therefore, without loss of generality, one only need to consider λ-quasi-twisted (quasi-cyclic) codes of index l where l is a divisor of the length n.

Quasi-cyclic codes over finite fields have a rich history in and of themselves. They have obtained many useful results, such as providing connections between quasi-cyclic block codes and convolutional codes [61], [117].

Quasi-cyclic codes over finite rings have received much attention since the 1990s, many new linear codes which are quasi-cyclic (over finite fields or finite rings) have been provided (see, for example, [3], [30], [37], [38], [68], [69], [87], [88], [115]).

Another variation that yields interesting results both for codes over fields and codes over rings is when one starts with a non-commutative ambient for codes rather than the usual commutative setting of quotient rings of the polynomial ring $F[x]$. Specifically, consider the codes that are ideals of quotient rings of the (infinite) ring of skew polynomial rings $R[x; \sigma]$ (where σ is an automorphism of the ring R). These are the skew cyclic codes. They have the property that if $(a_0, a_1, \ldots, a_{n-1})$ is a code word in a skew cyclic code C, then $(\sigma(a_{n-1}), \sigma(a_0), \ldots, \sigma(a_{n-2}))$ is also a codeword in C. Of course when σ is the identity this produces the normal cyclic shift. This approach, introduced in [16] for skew cyclic codes over finite fields, was later extended to the code over rings settings in [17] for skew constacyclic codes over Galois rings.

If quotients of a multivariable polynomial ring $R[x_1, \ldots, x_n]$ are used as ambients for codes, one gets the so-called *multivariable codes*. The study of multivariable codes goes back to the work of Poli in [93], [94] where multivariable codes over finite fields were first introduced and studied. There, ideals of $\frac{R[x,y,z]}{\langle t_1(x), t_2(y), t_3(z)\rangle}$, where R is a finite field, were considered. This notion then was extended by Martínez-Moro and Rúa in [93], [94] where R is assumed to be a finite chain ring.

Finally, there are the notions of polycyclic codes and sequential codes, which were introduced in [74] and [89], respectively. A linear code C of length n is *right polycyclic* if there exists an n-tupple $c = (c_0, c_1, \ldots, c_{n-1}) \in F^n$ such that for every codeword $(a_0, a_1, \ldots, a_{n-1}) \in C$, $(0, a_0, a_1, \ldots, a_{n-2}) + a_{n-1}(c_0, c_1, \ldots, c_{n-1}) \in C$. Left polycyclic is defined similarly. C is *bi-polycyclic* if it is both left and right polycyclic. Polycyclicity of codes is clearly a generalization of cyclicity, as a λ-constacyclic code is right polycyclic induced by $c = (\lambda, 0, \ldots, 0)$, and left polycyclic using $d = (0, \ldots, 0, \lambda^{-1})$. So, indeed a

λ-constacyclic code is bi-polycyclic.

As with cyclic and constacyclic codes, polycyclic codes may be understood in terms of ideals in quotient rings of polynomial rings. Given $c = (c_0, c_1, \ldots, c_{n-1}) \in F^n$, and let $f(x) = x^n - c(x)$, where $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ then the F-linear isomorphism $\rho : F^n \to \frac{F[x]}{\langle f(x)\rangle} = R_n$ sending the codeword $a = (a_0, a_1, \ldots, a_{n-1})$ to the polynomial $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$, identify the right polycyclic codes induced by c with the ideals of R_n.

Similarly, when C is a left polycyclic code, a slightly different isomorphism gives the identification of the left polycyclic codes induced by c as ideals of the corresponding ambient ring. As before, let $c = (c_0, c_1, \ldots, c_{n-1}) \in F^n$ but this time let $c'(x) = c_0x^{n-1} + c_1x^{n-2} + \cdots + c_{n-1}$. Then let $f'(x) = x^n - c'(x)$ and consider $\gamma : F^n \to \frac{F[x]}{\langle f'(x)\rangle} = L_n$ defined via $\gamma : (a_0, a_1, \ldots, a_{n-1}) \mapsto a_0x^{n-1} + \cdots + a_{n-2}x + a_{n-1}$. In this setting, very much like before, one can see that $\gamma(C)$ is an ideal of the quotient ring $L_n = \frac{F[x]}{\langle f'(x)\rangle}$.

Since all ideals of $F[x]$ are principal, the same is true in $\frac{F[x]}{\langle f(x)\rangle}$, thus the ambient $\frac{F[x]}{\langle f(x)\rangle}$ is a PIR. Furthermore, following the usual arguments used in the theory of cyclic codes, one easily sees that every polycyclic code C of dimension k has a monic polynomial $g(x)$ of minimum degree $n - k$ belonging to the code. This polynomial is a factor of $f(x)$ which is called a *generator polynomial* of C. Also, a generator of a code is unique up to associates in the sense that if $g_1(x) \in F[x]$ has degree $n - k$, it is easy to show that $g_1(x)$ is in the code generated by $g(x)$ if and only if$g_1(x) = ag(x)$ for some $0 \neq a \in F$.

As with cyclic codes, using the generator polynomial of a polycyclic code C, one can readily construct a generator matrix for it. It turns out that this property in fact characterizes polycyclic codes, as pointed out in [89, Theorem 2.3].

Theorem 7.1. *A code $C \subseteq F^n$ is right polycyclic if and only if it has a $k \times n$ generating matrix of the form*

$$G = \begin{pmatrix} g_0 & g_1 & \ldots & g_{n-k} & 0 & \ldots & 0 \\ 0 & g_0 & \ldots & g_{n-k-1} & g_{n-k} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & g_0 & g_1 & \ldots & g_{n-k} \end{pmatrix},$$

with $g_{n-k} \neq 0$. In this case $\rho(C) = \langle g_0 + g_1x + \cdots + g_{n-k}x^{n-k}\rangle$ is an ideal of $R_n = \frac{F[x]}{\langle f(x)\rangle}$. The same criterion, but requiring that $g_0 \neq 0$ instead of $g_{n-k} \neq 0$, serves to characterize left polycyclic codes. In the latter case, $\gamma(C) = \langle g_{n-k} + g_{n-k-1}x + \cdots + g_0x^{n-k}\rangle$ is an ideal of $L_n = \frac{F[x]}{\langle f(x)\rangle}$.

A code C is *right sequential* if there is a function $\phi : F^n \to F$ such that for every $(a_0, a_1, \ldots, a_{n-1}) \in C$, $(a_1, \ldots, a_{n-1}, b) \in C$ where $b = \phi(a_0, a_1, \ldots, a_{n-1})$. Left sequential is defined similarly. C is *bi-sequential* if it is both right and left sequential. [74, Examples

6.3, 6.4] gave examples to illustrate the promise of sequential codes as a source for good (even optimal) codes.

It has been shown in [89] that a code C over a field F is right sequential if and only if its dual $C^\perp$ is right polycyclic. Also, C is sequential and polycyclic if and only if C and $C^\perp$ are both sequential if and only if C and $C^\perp$ are both polycyclic. Furthermore, any one of these equivalent statements characterizes the family of constacyclic codes. In fact, the following results of [89. Theorems 3.2, 3.5] are true:

Theorem 7.2. *Let C be a code of length n over the finite field F. Then*

(a) *The following conditions are equivalent:*

(i) *C is right (respectively, left, bi-) sequential,*

(ii) *$C^\perp$ is right (respectively, left, bi-) polycyclic.*

(b) *The following conditions are equivalent:*

(1-R) *C and $C^\perp$ are right sequential,*

(2-R) *C and $C^\perp$ are right polycyclic,*

(3-R) *C is right sequential and right polycyclic,*

(4-R) *C is right sequential and bi-polycyclic,*

(5-R) *C is right sequential and left polycyclic with generator polynomial not a monomial of the form x^t ($t \geq 1$),*

(1-L) *C and $C^\perp$ are left sequential,*

(2-L) *C and $C^\perp$ are left polycyclic,*

(3-L) *C is left sequential and left polycyclic,*

(4-L) *C is left sequential and bi-polycyclic,*

(5-L) *C is left sequential and right polycyclic with generator polynomial not a monomial of the form x^t ($t \geq 1$),*

(A) *C is right polycyclic and bisequential,*

(B) *C is left polycyclic and bisequential,*

(C) *C is constacyclic.*

In particular, this theorem highlights in theoretical terms the significance of constacyclic codes as a central notion in coding theory.

REFERENCES

[1] T. Abualrub and R. Oehmke, "On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e," *IEEE Trans. Inform. Theory* **49**, pp. 2126-2133, 2003.

[2] T. Abualrub, A. Ghrayeb, and R. Oehmke, "A mass formula and rank of $\mathbb{Z}_4$ cyclic codes of length 2^e," *IEEE Trans. Inform. Theory*, **50**, pp. 3306-3312, 2004.

[3] N. Aydin and D. Ray-Chaudhuri, "Quasi-cyclic codes over $\mathbb{Z}_4$ and some new binary codes," *IEEE Trans. Inform. Theory*, **48**, pp. 2065-2069, 2002.

[4] R. D. Baker, J. H. van Lint, and R. M. Wilson, "On the Preparata and Goethals codes," *IEEE Trans. Inform. Theory*, **29**, pp. 342-345, 1983.

[5] E. Bannai, S. T. Dougherty, M. Harada and M. Oura, "Type II Codes, Even Unimodular Lattices, and Invariant Rings," *IEEE Trans. Inform. Theory*, **45**, pp. 1194-1205, 1999.

[6] S. D. Berman, *Semisimple cyclic and Abelian codes. II*, Kibernetika (Kiev) **3** (1967), 21-30 (Russian). English translation: Cybernetics **3**, pp. 17-23, 1967.

[7] I. F. Blake, "Codes over certain rings," *Inform. and Control*, **20**, pp. 396-404, 1972.

[8] I. F. Blake, "Codes over Integer Residue Rings," *Inform. and Control*, **29**, pp. 295-300, 1975.

[9] E. R. Berlekamp, *Negacyclic Codes for the Lee Metric*, Proceedings of the Conference on Combinatorial Mathematics and Its Applications, Chapel Hill, N. C., University of North Carolina Press, pp. 298-316, 1968.

[10] E. R. Berlekamp, *Algebraic Coding Theory*, revised 1984 edition, Aegean Park Press, 1984.

[11] C. Berrou, A. Glavieux and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes," *IEEE International Conference on Communications*, 1993.

[12] T. Blackford, "Negacyclic codes over $\mathbb{Z}_4$ of even length," *IEEE Trans. Inform. Theory*, **49**, pp. 1417-1424, 2003.

[13] T. Blackford, "Cyclic codes over $\mathbb{Z}_4$ of oddly even length", *International Workshop on Coding and Cryptography (WCC 2001) (Paris), Appl. Discr. Math.*, **128**, pp. 27-46, 2003.

[14] A. Bonnecaze, P. Solé and A. R. Calderbank, "Quarternary quadratic residue codes and unimodular lattices," *IEEE Trans. Inform. Theory*, **41**, pp. 366-377, 1995.

[15] A. Bonnecaze, P. Solé, C. Bachoc and B. Mourrain, "Type II codes over $\mathbb{Z}_4$," *IEEE Trans. Inform. Theory* , **43**, pp. 969-976, 1997.

[16] D. Boucher, W. Geiselmann, and F. Ulmer, "Skew-cyclic codes," *Appl. Algebra Engrg. Comm. Comput.*, **18**, pp. 79-389, 2007.

[17] D. Boucher, P. Solé and F. Ulmer, "Skew constacyclic codes over Galois rings," *Adv. Math. Commun.*, **2**, pp. 273-292, 2008.

[18] A.E. Brouwer and L. M. G. M. Tolhuizen, "A sharpening of the Johnson bound for binary linear codes and the nonexistence of linear codes with Preparata parameters," *Des. Codes Cryptogr.*, **3**, pp. 95-98, 1993.

[19] E. Byrne, *Lifting decoding schemes over a Galois ring*, Applied algebra, algebraic algorithms and Error-Correcting Codes (Melbourne, 2001), Lecture Notes in Comput. Sci. **2227**, Springer, pp. 323-332, 2001.

[20] E. Byrne, "Decoding a class of Lee metric codes over a Galois ring," *IEEE Trans. Inform. Theory*, **48**, pp. 966-975, 2002.

[21] E. Byrne and P. Fitzpatrick, "Grobner bases over Galois rings with an application to decoding alternant codes," *J. Symbolic Comput*, **31**, pp. 565-584, 2001.

[22] E. Byrne and P. Fitzpatrick, "Hamming metric decoding of alternant codes over Galois rings," *IEEE Trans. Inform. Theory*, **48**, pp. 683-694, 2002.

[23] A. R. Calderbank, A. R. Hammons Jr., P. V. Kumar, N. J. A. Sloane and P. Solé, *A linear construction for certain Kerdock and Preparata codes*, Bull. AMS, **29**, pp. 218-222, 1993.

[24] A. R. Calderbank and N. J. A. Sloane, "Modular and p-adic codes," *Des. Codes Cryptogr*, **6**, pp. 21-35, 1995.

[25] C. Carlet, *A simple description of Kerdock codes*, Lecture Notes in Computer Science **388**, pp. 202-208, 1989.

[26] J. Cazaran and A. V. Kelarev, "Generators and weights of polynomial codes," *Arch. Math.*, **69**, pp. 479-486, 1997.

[27] J. Cazaran and A. V. Kelarev, "On finite principal ideal rings," *Acta Math. Univ. Comenianae*, **LXVIII**, pp. 77-84, 1999.

[28] G. Castagnoli, J. L. Massey, P. A. Schoeller and N. von Seemann, "On repeated-root cyclic codes," *IEEE Trans. Inform. Theory*, **37**, 3pp. 37-342, 1991.

[29] B. Chen, H. Q. Dinh, Y. Fan and S. Ling, "Polyadic constacyclic codes," *IEEE Trans. Inform. Theory*, **61**, pp. 4895-4904, 2015.

[30] Z. Chen, "Six new binary quasicyclic codes," *IEEE Trans. Inform. Theory*, **40**, pp. 1666-1667, 1994.

[31] J. C.-Y. Chiang and J. Wolf, "On channels and codes for the Lee metric," *Inform. Contr.*, **19**, pp. 159-173, 1971.

[32] I. Constaninescu, *Lineare Codes uber Restklassenringen ganzer Zahlen und ihre Auto-*

morphismen bezuglich einer verallgemeinerten Hamming-Metrik, Ph.D. dissertation, Technische Universitat, Munchen, Germany, 1995.

[33] I. Constaninescu and W. Heise, "A metric for codes over residue class rings of integers," *Problemy Peredachi Informatsii*, **33**, pp. 22-28, 1997.

[34] I. Constaninescu, W. Heise, and T. Honold, "Monomial extensions of isometries between codes over $\mathbb{Z}_m$," *Proceedings of the* 5^{th} *International Workshop on Algebraic and Combinatorial Coding Theory (ACCT'96), Unicorn Shumen,* pp. 98-104, 1996.

[35] J. H. Conway, and N. J. A. Sloane, *Sphere-Packings, Lattices and Groups*, 2^{nd} edition, Springer-Verlag, New York, 1992.

[36] J. H. Conway, and N. J. A. Sloane, "Self-dual codes over the integers modulo 4," *J. Combin. Theory Ser. A*, **62**, pp. 30-45, 1993.

[37] R. N. Daskalov, T. A. Gulliver and E. Metodieva, "New good quasi-cyclic ternary and quaternary linear codes," *IEEE Trans. Inform. Theory*, **43**, pp. 1647-1650, 1997.

[38] R. N. Daskalov, T. A. Gulliver and E. Metodieva, "New ternary linear codes," *IEEE Trans. Inform. Theory*, **45**, pp. 1687-1688, 1999.

[39] P. Delsarte and J. M. Goethals, "Alternating bilinear forms over GF(q)," *J. Combin. Theory Ser. A*, **19**, pp. 26-50, 1975.

[40] H. Q. Dinh, "Negacyclic codes of length 2^s over Galois rings," *IEEE Trans. Inform. Theory*, **51**, pp. 4252-4262, 2005.

[41] H. Q. Dinh, *Structure of some classes of repeated-root constacyclic codes over integers modulo* 2^m, Ser. Lecture Notes in Pure & Appl. Math. **248** (2006), pp. 105-117.

[42] H.Q. Dinh, *Repeated-root constacyclic codes of length* 2^s *over* $\mathbb{Z}_{2^a}$, AMS Contemporary Mathematics, **419**, pp. 95-110, 2006.

[43] H. Q. Dinh, "Complete distances of all negacyclic codes of length 2^s over $\mathbb{Z}_{2^a}$," *IEEE Trans. Inform. Theory*, **53** , pp. 147-161, 2007.

[44] H. Q. Dinh, "On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions," *Finite Fields & Appl.*, **14**, pp. 22-40, 2008.

[45] H. Q. Dinh, "Constacyclic codes of length 2^s over Galois extension rings of $\mathbb{F}_2 + u\mathbb{F}_2$," *IEEE Trans. Inform. Theory*, **55**, 2009.

[46] H. Q. Dinh, *On some classes of repeated-root constacyclic codes of length a power of* 2 *over Galois rings*, Trends in Mathematics, pp. 131-147, 2010.

[47] H. Q. Dinh, "Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$," *J. Algebra*, **324**, pp. 940-950, 2010.

[48] H. Q. Dinh, S. Dhompongsa, and S. Sriboonchitta, "On constacyclic codes of length

$4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$," *Discrete Math.*, **340**, pp. 832-849, 2017.

[49] H. Q. Dinh, Y. Fan, H. Liu, X. Liu, and S. Sriboonchitta, "On self-dual constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$," *Discrete Math.*, **341**, pp. 324-335, 2018.

[50] H. Q. Dinh, B. T. Nguyen and S. Sriboonchitta, "Negacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ and their duals," *Discrete Math.* **341**, pp. 1055–1071, 2018.

[51] H. Q. Dinh, B. T. Nguyen, S. Sriboonchitta and T. M. Vo, "On a class of constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$", *J. Algebra Appl.*, **18**, 1950022.1-25, 2019.

[52] H. Q. Dinh, B. T. Nguyen, S. Sriboonchitta and T. M. Vo, "On $(\alpha + u\beta)$-constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$," *J. Algebra Appl.*, **18**, 1950023.1-16, 2019.

[53] H. Q. Dinh and H. D. T. Nguyen, "On some classes of constacyclic codes over polynomial residue rings," *Advances Math. Comm.*, to appear, 2011.

[54] H. Q. Dinh and S. R. López-Permouth, "Cyclic and negacyclic codes over finite chain rings," *IEEE Trans. Inform. Theory*, **50**, pp. 1728-1744, 2004.

[55] H. Q. Dinh, S. R. Lopez-Permouth and S. Szabo, *On the structure of cyclic and negacyclic codes over finite chain rings*, Codes over Rings, Series on Coding Theory and Cryptography **6**, 22-59, 2009.

[56] H. Q. Dinh, A. Sharma, S. Rani and S. Sriboonchitta, "Cyclic and negacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$," *J. Algebra Appl.*, **17**, 1850173, pp. 1-22, 2018.

[57] H. Q. Dinh, L. Wang and S. Zhu, "Negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$," *Finite Fields & Appl.*, **31**, pp. 178-201, 2015.

[58] S. T. Dougherty, T. A. Gulliver and M. Harada, "Type II Self-Dual Codes over Finite Rings and Even Unimodular Lattices," *J. Algebraic Combin.*, **9**, pp. 233-250, 1999.

[59] S. T. Dougherty, M. Harada and P. Solé, "Self-dual codes over rings and the Chinese remainder theorem," *Hokkaido Math. J.*, **28**, pp. 253-283, 1999.

[60] S. T. Dougherty and S. Ling, "Cyclic codes over $\mathbb{Z}_4$ of even length," *Des. Codes Cryptogr*, **39**, pp. 127-153, 2006.

[61] M. Esmaeili, T. A. Gulliver, N. P. Secord, and S. A. Mahmoud, "A link between quasi-cyclic codes and convolutional codes," *IEEE Trans. Inform. Theory*, **44**, pp. 431-435, 1998.

[62] G. Falkner, B. Kowol, W. Heise and E. Zehendner, "On the existence of cyclic optimal codes," *Atti Sem. Mat. Fis. Univ. Modena*, **28** , pp. 326-341, 1979.

[63] R.G. Gallager, *Low density parity check codes*, Monograph, M.I.T. Press, 1963.

[64] J.-M. Goethals, "Two dual families of nonlinear binary codes", *Electron. Lett.*, **10**, pp. 471-472, 1974.

[65] J.-M. Goethals, "The extended Nadler code is unique," *IEEE Trans. Inform. Theory*, **23**, pp. 132-135, 1977.

[66] M. Greferath and S. E. Schmidt, "Gray Isometries for Finite Chain Rings and a Nonlinear Ternary $(36, 3^{12}, 15)$ Code," *IEEE Trans. Inform. Theory*, **45**, pp. 2522-2524, 1999.

[67] M. Greferath and S. E. Schmidt, "Finite Ring Combinatorics and MacWilliams's Equivalence Theorem," *J. Combin. Theory Ser. A*, **92**, pp. 17-28, 2000.

[68] T. A. Gulliver and V. K Bhargava, "Nine good rate $(m-1)/pm$ quasi-cyclic codes," *IEEE Trans. Inform. Theory*, **38**, pp. 1366-1669, 1992.

[69] T. A. Gulliver and V. K Bhargava, "New good rate $(m-1)/pm$ ternary and quaternary quasicyclic codes," *Des. Codes Cryptogr.*, **7**, pp. 223-233, 1996.

[70] R. W. Hamming, "Error detecting and error correcting codes," *Bell Sys. Tech. J.*, **29**, pp. 147-160, 1950.

[71] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inform. Theory*, **40**, pp. 301-319, 1994.

[72] W. Heise, T. Honold and A. A. Nechaev, *Weighted modules and representations of codes*, Proceedings of the ACCT 6, Pskov, Russia, pp. 123-129, 1998.

[73] T. Honold and I. Landjev, *Linear representable codes over chain rings*, Proceedings of the ACCT 6, Pskov, Russia, pp. 135-141, 1998.

[74] X. Hou, S. R. López-Permouth and B. R. Parra-Avila, "Rational power series, sequential codes and periodicity of sequences," *J. Pure Appl Algebra*, 2009.

[75] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003.

[76] I. James, *Claude Elwood Shannon 30 April 1916 - 24 February 2001*, Biographical Memoirs of Fellows of the Royal Society **55**, pp. 257-265, 2009.

[77] W. M. Kantor, "An exponential number of generalized Kerdock codes," *Inform. and Control*, **53**, pp. 74-80, 1982.

[78] W. M. Kantor, "Spreads, translation planes and Kerdock sets. I.," *SIAM J. Algebraic Discrete Methods*, **3**, pp. 151-165, 1982.

[79] W. M. Kantor, "Spreads, translation planes and Kerdock sets. II.," *SIAM J. Algebraic Discrete Methods*, **3**, pp. 308-318, 1982.

[80] W. M. Kantor, "On the inequivalence of generalized Preparata codes," *IEEE Trans. Inform. Theory*, **29**, pp. 345-348, 1983.

[81] P. Kanwar and S. R. López-Permouth, "Cyclic codes over the integers modulo p^m,"

Finite Fields & Appl., **3**, pp. 334-352, 1997.

[82] A. M. Kerdock, "A class of low-rate nonlinear binary codes," *Inform. and Control*, **20**, pp. 182-187, 1972.

[83] H. M. Kiah, K. H. Leung and S. Ling, "Cyclic codes over GR(p^2, m) of length p^k," *Finite Fields & Appl.*, **14**, pp. 834-846, 2008.

[84] E. Kleinfeld, "Finite Hjelmslev planes," *Illinois J. Math.*, **3**, pp. 403-407, 1959.

[85] C. Y. Lee, "Some properties of non-binary error-correcting codes," *IEEE Trans. Inform. Theory*, **4**, pp. 77-82, 1958.

[86] S. Ling, H. Niederreiter and P. Solé, "On the algebraic structure of quasi-cyclic codes. IV. Repeated roots," *Des. Codes Cryptogr*, **38**, pp. 337-361, 2006.

[87] S. Ling and P. Solé, "On the Algebraic Structure of Quasi-Cyclic Codes I: Finite Fields," *IEEE Trans. Inform. Theory*, **47**, pp. 2751-2760, 2001.

[88] S. Ling and P. Solé, "On the Algebraic Structure of Quasi-Cyclic Codes II: Chain Rings," *Des. Codes Cryptogr.*, **30**, pp. 113-130, 2003.

[89] S. R. López-Permouth, B. R. Parra-Avila, and S. Szabo, "Dual generalizations of the concept of cyclicity of codes," *Adv. Math. Commun.*, **3**, 2009.

[90] F. J. MacWilliams, "Error-correcting codes for multiple-level transmissions," *Bell System Tech. J.*, **40**, pp. 281-308, 1961.

[91] F. J. MacWilliams, *Combinatorial problems of elementary abelian groups*, PhD. Dissertation, Harvard University, Cambridge, MA, 1962.

[92] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, 10^{th} impression, North-Holland, Amsterdam, 1998.

[93] E. Martínez-Moro and I. F. Rúa, "Multivariable codes over finite chain rings: serial codes," *SIAM J. Discrete Math.*, **20**, pp. 947-959, 2006.

[94] E. Martínez-Moro and I. F. Rúa, "On repeated-root multivariable codes over a finite chain ring," *Des. Codes Cryptogr.*, **45**, pp. 219-227. 2007.

[95] J. L. Massey, D. J. Costello and J. Justesen, "Polynomial weights and code constructions," *IEEE Trans. Information Theory*, **19**, pp. 101-110, 1973.

[96] B .R. McDonald, "Finite rings with identity," *Pure and Applied Mathematics*, Vol. **28**, Marcel Dekker, New York, 1974.

[97] P. Moree, "On the divisors of $a^k + b^k$", *Acta Arithm.*, **80**, pp. 197-212.

[98] A. A. Nechaev, *Trace functions in Galois ring and noise stable codes* (in Russian), V All-Union Symp. on theory of rings, algebras and modules, Novosibirsk, 1982, p. 97.

[99] A. A. Nechaev, "Kerdock code in a cyclic form," (in Russian), Diskr. Math. (USSR) **1**, 123-139, 1989. English translation: *Discrete Math. and Appl.*, **1**, pp. 365-384, 1991.

[100] A. A. Nechaev, "Linear recurrence sequences over commutative rings," *Discrete Math. and Appl.*, **2**, pp. 659-683, 1992.

[101] A. A. Nechaev and D. A. Mikhailov, "Canonical generating system of a monic polynomial ideal over a commutative artinian chain ring," *Discrete Math. Appl.*, **11**, pp. 545-586, 2001.

[102] A. W. Nordstrom and J. P. Robinson, "An optimum nonlinear code," *Inform. and Control*, **11**, 613-616, 1967.

[103] G. Norton and A. Sălăgean, "On the structure of linear and cyclic codes over finite chain rings," *Appl. Algebra Engrg. Comm. Comput.*, **10**, pp. 489-506, 2000.

[104] G. Norton and A. Sălăgean, "Cyclic codes and minimal strong Grobner bases over a principal ideal ring," *Finite Fields & Appl.*, **9**, pp. 237-249, 2003.

[105] W. W. Peterson and D. T Brown, *Cyclic Codes for Error Detection*, Proceedings of the IRE **49**, p. 228, 1961.

[106] A. Poli, "Important algebraic calculations for n-variables polynomial codes," *Discrete Math.*, **56**, pp. 255-263, 1985.

[107] A. Poli and Llorenç Huguet, *Error correcting codes*, Theory and applications (with a preface by G. Cullmann), Prentice Hall International, Hemel Hempstead, 1992. Translated from the 1989 French original by Iain Craig.

[108] V. Pless and Z. Qian, "Cyclic codes and quadratic codes over $\mathbb{Z}_4$," *IEEE Trans. Inform. Theory*, **42**, pp. 1594-1600, 1996.

[109] V. Pless, P. Solé and Z. Qian, "Cyclic self-dual $\mathbb{Z}_4$-codes," *Finite Fields & Appl.*, **3**, pp. 48-69, 1997.

[110] F. P. Preparata, "A class of optimum nonlinear double error-correcting codes," *Inform. and Control*, **13**, pp. 378-400, 1968.

[111] R. M. Roth and G. Seroussi, "On cyclic MDS codes of length q over GF(q)," *IEEE Trans. Inform. Theory*, **32**, pp. 284-285, 1986.

[112] R. M. Roth and P. H. Siegel, "Lee-metric BCH codes and their application to constrained and partial-response channels," *IEEE Trans. Inform. Theory*, **40**, pp. 1083-1095, 1994.

[113] A. Sălăgean, "Repeated-root cyclic and negacyclic codes over finite chain rings," *Discrete Appl. Math.*, **154**, pp. 413-419, 2006.

[114] C. E. Shannon, *A mathematical theory of communication*, Bell System Tech. J. **27**,

379-423, 623-656, 1948. Reprinted in: *A mathematical theory of communication*, (Eds. C.E. Shannon and W. Weaver), Univ. of Illinois Press, Urbana, IL, 1963.

[115] I. Siap, N. Aydin, and D. Ray-Chaudhuri, "New ternary quasicyclic codes with better minimum distances," *IEEE Trans. Inform. Theory*, **46**, pp. 1554-1558, 2000.

[116] S. L. Snover, *The uniqueness of the Nordstrom-Robinson and Golay binary codes*, Ph.D. dissertation, Michigan State University, MI, USA, 1973.

[117] G. Solomon and H. C. A. van Tilborg, "A connection between block and convolutional codes," *SIAM J. Appl. Math.*,**37**, pp. 358-269, 1979.

[118] E. Spiegel, "Codes over $\mathbb{Z}_m$," *Inform. and Control*, **35**, pp. 48-51, 1977.

[119] E. Spiegel, "Codes over $\mathbb{Z}_m$," revisited, *Inform. and Control*, **37**, pp. 100-104, 1978.

[120] J. H. van Lint, "Kerdock and Preparata codes," *Congressus Numerantium*, **39**, pp. 25-41, 1983.

[121] J. H. van Lint, "Repeated-root cyclic codes,"*IEEE Trans. Inform. Theory*, **37**, pp. 343-345, 1991.

[122] Z. Wan, *Quaternary codes*, World Scientific, Singapore, 1997.

[123] Z. Wan, "Cyclic Codes over Galois Rings," *Algebra Colloquium*, **6**, pp. 291-304, 1999.

[124] J. Wolfmann, "Negacyclic and Cyclic Codes over $\mathbb{Z}_4$," *IEEE Trans. Inform. Theory*, **45**, 2527-2532, 1999.

[125] J. Wolfmann, "Binary images of cyclic codes over $\mathbb{Z}_4$," *IEEE Trans. Inform. Theory*, **47**, pp. 1773-1779, 2001.

[126] J. A. Wood, "Duality for modules over finite rings and applications to coding theory," *American J. of Math.*, **121**, pp. 555-575, 1999.

TÓM TẮT

CẤU TRÚC ĐẠI SỐ CỦA MÃ CYCLIC VÀ NEGACYCLIC TRÊN VÀNH CHUỖI HỮU HẠN VÀ ỨNG DỤNG

Tổng quan về lý thuyết mã được trình bày trong bài báo, đặc biệt tập trung vào mã cyclic và negacyclic trên vành chuỗi hữu hạn. Vai trò quan trọng của vành hữu hạn với tư cách là bảng chữ cái trong lý thuyết mã. Chúng tôi đưa ra các kết quả về mã nghiệm đơn lẫn mã nghiệm lặp. Rất nhiều hướng nghiên cứu được tổng quát hóa đối với mã cyclic và negacyclic. Bài báo cũng giới thiệu về ứng dụng của nó trong lĩnh vực đại số.