East-West J. of Mathematics: Vol. 13, No 2 (2011) pp. 207-224

REPEATED-ROOT CYCLIC AND NEGACYCLIC CODES OF PRIME POWER LENGTHS WITH A FINITE COMMUTATIVE CHAIN RING ALPHABET

Hai Q. Dinh* and **Thang M. Vo†**

**Department of Mathematical Sciences*
Kent State University,
4314 Mahoning Avenue, Warren, Ohio 44483, USA.
e-mail: hdinh@kent.edu

† Department of Personnel and Organization
Vinh University of Technology Education
Vinh city, Nghe An, Vietnam.
e-mail: vomanhthang@vute.edu.vn

Abstract

We dicuss foundational and theoretical aspects of algebraic coding theory with the concentration on repeated-root cyclic and negacyclic codes of prime power length p^s over a finite commutative chain ring R. Among other things, the nilpotency indeces of $x-1$ and $x+1$ in the ambient rings $\frac{R[x]}{\langle x^{p^s}-1\rangle}$ and $\frac{R[x]}{\langle x^{p^s}+1\rangle}$, respectively, are established.

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]

Key words: Cyclic codes, negacyclic codes, chain rings, Galois rings.
2000 AMS Classification: 94B15, 12Y05.

[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". Shannon is also credited as the founder of both digital computer and digital

landmark 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 accross 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 meassge 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 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.

---

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.

[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, 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.

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 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.

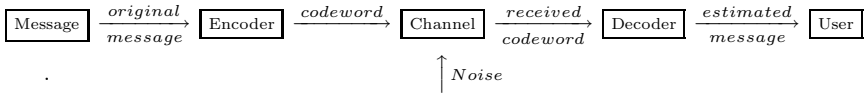
Given an alphabet $\mathcal{A}$ with q symbols, a block code C of length n over the alphabet $\mathcal{A}$ is simply a subset of $\mathcal{A}^n$. The q-ary n-tuples from C are called the codewords of the code C. One normally envisions K, the number of codewords in C, as a power of q, i.e., $K = q^k$, 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

[3]The Hamming distance is named after Richard Hamming, who first introduced it in his fundamental paper on Hamming codes in 1950 [25]. 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*.

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 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

[4]Turbo codes were first introduced and developed in 1993 by Berrou, Glavieux, and Thitimajshima. 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. Gal-

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 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 [2], 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. [3]). In 1977, Spiegel [38], [39] 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 [23, 34], 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.

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. [8]). Nechaev pointed out that the Kerdock codes are, in fact, cyclic codes over $\mathbb{Z}_4$. Furthermore, the intriguing relationship between

lager 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 memory-less 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.

[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 $\mathbb{Z}_4$.

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 [8] 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 [34, 23], this code is the unique binary code of length 16, consisting 256 codewords, and minimum distance 6. In [8] (see also [12]), 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.

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 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 $F[x]$.

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 this paper.

3. Chain Rings and Galois 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. [33], [26])[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 [6, 5, 7].

The following equivalent conditions are well-known for the class of finite commutative chain rings (cf. [20, Proposition 2.1]).

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. [33]).

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,

[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 [29], that can be represented as $R = \mathrm{GF}(4) \oplus \mathrm{GF}(4)$, where the operations $+, \cdot$ are

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

(*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. [20, 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. [33, 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. [33, Theorem XIII.4]).

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

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, [9, Theorem 4], [10, Theorem 2], [36, 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. [33, 26]):

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

(*iii*) *Each element of* $\mathrm{GR}(p^a, m)$ *can be represented as* up^k, *where* u *is a unit and* $0 \le k \le a$, *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*

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

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

Let R be a finite commutative ring. 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 $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$, 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. [17]) *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

$$f(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1} + a_k x^k,$$

then

$$f^*(x) = x^k(a_0 + a_1 x^{-1} + \cdots + a_{k-1}x^{-(k-1)} + a_k x^{-k}) = a_k + a_{k-1}x + \cdots + a_1 x^{k-1} + a_0 x^k.$$

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. [19, 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 [1], and then in the 1970s and 1980s by several authors such as Massey *et al.* [32], Falkner *et al.* [22], Roth and Seroussi [35]. However, repeated-root codes over finite fields were investigated in the most generality in the 1990s by Castagnoli *et al.* [11], and van Lint [41], 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, Blackford, Dinh [13, 14, 15, 17, 18], Ling *et al* [21, 30, 28], Sălăgean *et al* [36], 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*. In this paper, we concentrated on repaeated-root cyclic and negacyclic codes of length p^s over finite chain rings.

5. Repeated-root cyclic and negacyclic codes of length p^s over a finite chain ring

Let R be a finite chain ring of characteristic p^a that has maximal ideal $\langle\gamma\rangle$. Let N_γ denote the nilpotency index of γ. Cyclic and negacyclic codes of length p^s over R are the ideals of the ambient rings

$$\mathcal{R}_1 = \frac{R[x]}{\langle x^{p^s}-1\rangle}, \quad \mathcal{R}_{-1} = \frac{R[x]}{\langle x^{p^s}-1\rangle}.$$

Each element $r \in R$ can be written as $r = w\gamma^i$, where w is a unit of R and $0 \le i \le N^\gamma$. Thus, each codeword $\mathbf{c}$ of a cyclic code of length p^s over R has its polynomial representation $c(x) \in \mathcal{R}_1$ expressed as

$$c(x) = \sum_{i=0}^{p^s-1} w_i\gamma^{k_i}(x-1)^i = w_0\gamma^{k_0} + (x-1)\sum_{i=1}^{p^s-1} w_i\gamma^{k_i}(x-1)^{i-1},$$

where w_i's are units of R, and $0 \le k_i \le N_\gamma$. Since both $x-1$ and γ are nilpotent in $\mathcal{R}_1$, $c(x)$ is invertible in $\mathcal{R}_1$ if and only if $k_0 = 0$. That means $\langle x-1, \gamma\rangle$ is the set of all non-invertible elements of $\mathcal{R}_1$. Therefore, $\mathcal{R}_1$ is a local ring with maximal ideal $\langle x-1, \gamma\rangle$. Similarly, $\mathcal{R}_{-1}$ is a local ring with maximal ideal $\langle x+1, \gamma\rangle$. We summarize that in the following proposition.

Proposition 5.1. *Let R be a finite chain ring of characteristic p^a and maximal ideal $\langle\gamma\rangle$. The ambient rings $\mathcal{R}_1$ and $\mathcal{R}_{-1}$ are local rings with maximal ideals $\langle x-1, \gamma\rangle$, $\langle x+1, \gamma\rangle$, respectively.*

In light of Proposition 2.1, and [36, Theorem 3.4], we have:

Proposition 5.2. *Let R be a finite chain ring of characteristic p^a and maximal ideal $\langle\gamma\rangle$. Then*

- *$\mathcal{R}_1$ is not a chain ring.*
- *$\mathcal{R}_{-1}$ is a chain ring if and only if $p = 2$, and the ring R is a Galois ring.*

When R is a Galois ring and $p = 2$, $R = \mathrm{GR}(2^a, m)$, and the negacyclic codes of length 2^s over $\mathrm{GR}(2^a, m)$ are ideals of the chain ring $\mathcal{R}_{-1}$. [13] studied this class of code. It is shown that the chain ring $\mathcal{R}_{-1}$ has maximal ideal $\langle x+1\rangle$, and $x+1$ has nilpotency index $2^s a$. From that the structure of all such negacyclic codes were given. Furthermore, this structure is used to give the Hamming distance of all negacyclic codes in [13, 16, 18].

When $p \neq 2$, $\mathcal{R}_1$ and $\mathcal{R}_{-1}$ are local ring with maximal ideals $\langle x-1, \gamma\rangle$ and $\langle x+1, \gamma\rangle$, but they are not chain rings. While the nilpotency index N_γ of the generator γ is given, it is important to find the nilpotency index of the other generator $x-1$ (in $\mathcal{R}_1$), and $x+1$ (in $\mathcal{R}_{-1}$). These nilpotency indeces are significant to obtain the structure of ideals of the ambient rings $\mathcal{R}_1$ and $\mathcal{R}_{-1}$. We process to establish them in the next section.

6. Nilpotency indeces of $x-1$ and $x+1$ in $\mathcal{R}_1$ and $\mathcal{R}_{-1}$

Throughout this section, R is a finite commutative chain ring of characteristic p^a, and $\mathcal{R}_1$ and $\mathcal{R}_{-1}$ are the ambient rings as defined in Section 5. We first recall an important fact in number theory proven by Kummer[8].

Theorem 6.1. (Kummer's Theorem) *For any prime p and integers $n \geq m \geq 0$, the highest power to which p divides the binomial coefficient $\binom{n}{m}$ is equal to the numbers of carries when adding $n-m$ and m in base p.*

Kummer's Theorem easily implies the following result.

Proposition 6.2. *Let p be a prime.*

(a) *Assume that $t < p^n$, and m is the largest integer such that $p^m | t$. Then $p^{n-m} | \binom{p^n}{t}$, and $p^{n-m+1} \nmid \binom{p^n}{t}$.*

(b) *For any i with $1 \leq i \leq p-1$, $p | \binom{p^s}{ip^{s-1}}$, and $p^2 \nmid \binom{p^s}{ip^{s-1}}$.*

Proof. Since m is the largest integer with $p^m | t$, the sum of $p^n - t$ and t in base p has $n-m$ carries. Therefore, (a) follows from Kummer's Theorem. (b) is just a straightforward implication of (a). □

[8]Ernst Eduard Kummer (29 January 1810 - 14 May 1893) was a German mathematician. Kummer made several contributions to mathematics in different areas. Kummer also proved Fermat's last theorem for a considerable class of prime exponents. He studied what were later called Kummer extensions of fields, that is, extensions generated by adjoining an nth root to a field already containing a primitive nth root of unity. This is a significant extension of the theory of quadratic extensions, and the genus theory of quadratic forms (linked to the 2-torsion of the class group). It is considered as foundation for class field theory.

Proposition 6.3. *Let $k \geq 0$. Then in $\mathcal{R}_1$, there exist elements $\alpha_k(x)$, $\beta_k(x)$ such that $\alpha_k(x)$ is invertible, $p^{k+2}|\beta_k(x)$, and*

$$(x-1)^{p^s+k(p-1)p^{s-1}} = p^{k+1}\alpha_k(x)(x-1)^{p^{s-1}} + \beta_k(x).$$

Proof. We proceed by induction on k. When $k = 0$, we have

$$\begin{aligned} 0 &= x^{p^s} - 1 \\ &= [(x-1)+1]^{p^s} - 1 \\ &= \sum_{i=1}^{p^s} \binom{p^s}{i} (x-1)^i. \end{aligned}$$

Therefore,

$$\begin{aligned} (x-1)^{p^s} &= -\sum_{i=1}^{p^s-1} \binom{p^s}{i} (x-1)^i \\ &= -\sum_{i=1}^{p-1} \binom{p^s}{ip^{s-1}} (x-1)^{ip^{s-1}} - \sum_{i=1,\, p^{s-1} \not| i}^{p^s-1} \binom{p^s}{i} (x-1)^i \\ &= p\alpha_0(x)(x-1)^{p^{s-1}} + \beta_0(x), \end{aligned}$$

where

$$\alpha_0(x) = -\frac{1}{p} \sum_{i=1}^{p-1} \binom{p^s}{ip^{s-1}} (x-1)^{(i-1)p^{s-1}},$$

and

$$\beta_0(x) = -\sum_{i=1,\, p^{s-1} \not| i}^{p^s-1} \binom{p^s}{i} (x-1)^i.$$

By Proposition 6.2, $\alpha_0(x)$ is invertible, and $p^2|\beta_0(x)$. Thus the assertion is true for $k = 0$. Now, assume that the assertation is true for any integer up to k, we

need to show that it is true for $k+1$. We have

$$\begin{aligned}
(x-1)^{p^s+(k+1)(p-1)p^{s-1}} &= (x-1)^{p^s+k(p-1)p^{s-1}}(x-1)^{(p-1)p^{s-1}} \\
&= \left[p^{k+1}\alpha_k(x)(x-1)^{p^{s-1}} + \beta_k(x)\right](x-1)^{(p-1)p^{s-1}} \\
&= p^{k+1}\alpha_k(x)(x-1)^{p^s} + \beta_k(x)(x-1)^{(p-1)p^{s-1}} \\
&= p^{k+1}\alpha_k(x)\left[p\alpha_0(x)(x-1)^{p^{s-1}} + \beta_0(x)\right] + \beta_k(x)(x-1)^{(p-1)p^{s-1}} \\
&= p^{k+2}\alpha_k(x)\alpha_0(x)(x-1)^{p^{s-1}} + p^{k+1}\alpha_k(x)\beta_0(x) + \beta_k(x)(x-1)^{(p-1)p^{s-1}} \\
&= p^{k+2}\left[\alpha_k(x)\alpha_0(x) + \frac{\beta_k(x)}{p^{k+2}}(x-1)^{(p-2)p^{s-1}}\right](x-1)^{p^{s-1}} + p^{k+1}\alpha_k(x)\beta_0(x) \\
&= p^{k+2}\alpha_{k+1}(x)(x-1)^{p^{s-1}} + \beta_{k+1}(x),
\end{aligned}$$

where

$$\alpha_{k+1}(x) = \alpha_k(x)\alpha_0(x) + \frac{\beta_k(x)}{p^{k+2}}(x-1)^{(p-2)p^{s-1}},$$

and

$$\beta_{k+1}(x) = p^{k+1}\alpha_k(x)\beta_0(x).$$

Since $\alpha_0(x)$ and $\alpha_k(x)$ are invertible, it is easy to see that α_{k+1} is also invertible. As $p^2|\beta_0(x)$, $p^{k+3}|\beta_{k+1}(x)$. □

Theorem 6.4. *In $\mathcal{R}_1$, $x-1$ is nilpotent with nipotency index $ap^s-(a-1)p^{s-1}$.*

Proof. Using $k = a-1$ in Proposition 6.3, it follows that in $\frac{R[x]}{\langle x^{p^s}-1\rangle}$, there exists $\alpha_{a-1}(x), \beta_{a-1}(x)$ such that $\alpha_{a-1}(x)$ is invertible, $p^{a+1}|\beta_{a-1}(x)$, and

$$(x-1)^{p^s+(a-1)(p-1)p^{s-1}} = p^a\alpha_{a-1}(x)(x-1)^{p^{s-1}} + \beta_{a-1}(x) = 0.$$

Thus the nilpotency index of $x-1$ is less than or equal to $p^s + (a-1)(p-1)p^{s-1} = ap^s - (a-1)p^{s-1}$. We complete the proof by showing that $(x-1)^{ap^s-(a-1)p^{s-1}-1} \neq 0$. Making use of Proposition 6.3 for $k = a-2$, we get that there exists $\alpha_{a-2}(x), \beta_{a-2}(x)$ such that $\alpha_{a-2}(x)$ is invertible, $p^a|\beta_{a-2}(x)$, and

$$(x-1)^{p^s+(a-2)(p-1)p^{s-1}} = p^{a-1}\alpha_{a-2}(x)(x-1)^{p^{s-1}} + \beta_{a-2}(x) = p^{a-1}\alpha_{a-2}(x)(x-1)^{p^{s-1}}.$$

Therefore,

$$\begin{aligned}
(x-1)^{ap^s-(a-1)p^{s-1}-1} &= (x-1)^{p^s+(a-1)(p-1)p^{s-1}-1} \\
&= (x-1)^{p^s+(a-2)(p-1)p^{s-1}+(p-1)p^{s-1}-1} \\
&= (x-1)^{p^s+(a-2)(p-1)p^{s-1}}(x-1)^{(p-1)p^{s-1}-1} \\
&= p^{a-1}\alpha_{a-2}(x)(x-1)^{p^{s-1}}(x-1)^{(p-1)p^{s-1}-1} \\
&= p^{a-1}\alpha_{a-2}(x)(x-1)^{p^s-1} \neq 0. \ \square
\end{aligned}$$

Theorem 6.5. *The followings hold true.*

(a) *If p is odd, then in $\mathcal{R}_{-1}$, there exist elements $\alpha_k(x)$, $\beta_k(x)$ such that $\alpha_k(x)$ is invertible, $p^{k+2}|\beta_k(x)$, and*

$$(x+1)^{p^s+k(p-1)p^{s-1}} = p^{k+1}\alpha_k(x)(x+1)^{p^{s-1}} + \beta_k(x).$$

Moreover, in $\frac{R[x]}{\langle x^{p^s}+1\rangle}$, $x+1$ is nilpotent with nipotency index $ap^s-(a-1)p^{s-1}$.

(b) *If $p=2$, then for any positive integer n, there exists an unit $\alpha_n(x) \in \frac{R[x]}{\langle x^{2^s}+1\rangle}$ such that $(x+1)^{2^n} = x^{2^n}+1+2\alpha_n(x)$. In particular, $x+1$ is nilpotent in $\frac{R[x]}{\langle x^{2^s}+1\rangle}$ with nilpotency index $2^s a$.*

Proof. For (a), note that when p is odd, the map $\phi : \mathcal{R}_1 \longrightarrow \mathcal{R}_{-1}$ that sends x to $-x$ is a ring isomorphism. Therefore, the results from Proposition 6.3 and Theorem 6.4 hold for $\mathcal{R}_{-1}$ when we replace x by $-x$.

We prove (b) by induction on n. For $n=1$, $(x+1)^2 = x^2+1+2x$, $\alpha_1(x)=x$, and hence obviously, $\alpha_1(x)=x$ is a unit in $\frac{R[x]}{\langle x^{2^s}+1\rangle}$. Assume $n>1$ and the conclusion is true for all positive integer less than n. Then

$$\begin{aligned}(x+1)^{2^n} &= [(x+1)^{2^{(n-1)}}]^2 \\ &= [x^{2^{(n-1)}}+1+2\alpha_{n-1}(x)]^2 \\ &= x^{2^n}+1+4\alpha_{n-1}^2(x)+2x^{2^{n-1}}+4\alpha_{n-1}(x)+4x^{2^{n-1}}\alpha_{n-1}(x) \\ &= x^{2^n}+1+2\alpha_n(x),\end{aligned}$$

where $\alpha_n(x) = 2\alpha_{n-1}^2(x)+x^{2^{n-1}}+2\alpha_{n-1}(x)+2x^{2^{n-1}}\alpha_{n-1}(x)$. To show that $\alpha_n(x)$ is a unit in $\frac{R[x]}{\langle x^{2^s}+1\rangle}$, we note that x is invertible, and so $x^{2^{n-1}}$ is also invertible in $\frac{R[x]}{\langle x^{2^s}+1\rangle}$. As 2 is nilpotent in $\frac{R[x]}{\langle x^{2^s}+1\rangle}$, it follows that $\alpha_n(x)$ has the form $\alpha_n(x) = x^{2^{n-1}}(1+y)$, where y is nilpotent in $\frac{R[x]}{\langle x^{2^s}+1\rangle}$. Choose k to be an odd integer such that $y^k=0$, we have

$$1 = 1+y^k = (1+y)(1-y+y^2-\cdots+y^{k-1}),$$

which means $1+y$ is invertible in $\frac{R[x]}{\langle x^{2^s}+1\rangle}$, and therefore $\alpha_n(x) = x^{2^{(n-1)}}(1+y)$ is a unit in $\frac{R[x]}{\langle x^{2^s}+1\rangle}$. Finally, using $n=s$, we have in $\frac{R[x]}{\langle x^{2^s}+1\rangle}$

$$(x+1)^{2^s} = x^{2^s}+1+2\alpha_s(x) = 2\alpha_s(x),$$

for some unit $\alpha_s(x)$. Therefore, the nilpotency index of $x+1$ is $2^s a$. □

References

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

[2] I.F. Blake, *Codes over certain rings*, Inform. and Control **20** (1972), 396-404.

[3] I.F. Blake, *Codes over Integer Residue Rings*, Inform. and Control **29** (1975), 295-300.

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

[5] 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, (2001) 323-332.

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

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

[8] 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** (1993), 218-222.

[9] J. Cazaran and A.V. Kelarev, *Generators and weights of polynomial codes*, Arch. Math. **69** (1997), 479 - 486.

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

[11] G. Castagnoli, J.L. Massey, P.A. Schoeller, and N. von Seemann, *On repeated-root cyclic codes*, IEEE Trans. Inform. Theory **37** (1991), 337-342.

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

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

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

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

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

[17] 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).

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

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

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

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

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

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

[24] 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** (1999), 2522-2524.

[25] R.W. Hamming, *Error detecting and error correcting codes*, Bell Sys. Tech. J. **29** (1950), 147-160.

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

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

[28] H.M. Kiah, K.H. Leung, and S. Ling, *Cyclic codes over* $\mathrm{GR}(p^2, m)$ *of length* p^k, Finite Fields & Appl. **14** (2008), 834-846.

[29] E. Kleinfeld, *Finite Hjelmslev planes*, Illinois J. Math. **3** (1959), 403-407.

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

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

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

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

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

[35] R.M. Roth and G. Seroussi, *On cyclic MDS codes of length* q *over* $\mathrm{GF}(q)$, IEEE Trans. Inform. Theory **32** (1986), 284-285.

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

[37] C.E. Shannon, *A mathematical theory of communication*, Bell System Tech. J. **27** (1948), 379-423, 623-656. Reprinted in: *A mathematical theory of communication*, (Eds. C.E. Shannon and W. Weaver), Univ. of Illinois Press, Urbana, IL, 1963.

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

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

[40] J.H. van Lint, *Kerdock and Preparata codes*, Congressus Numerantium **39** (1983), 25-41.

[41] J.H. van Lint, *Repeated-root cyclic codes*, IEEE Trans. Inform. Theory **37** (1991), 343-345.