Repeated-root cyclic and negacyclic codes over a finite chain ring

Ana Sălăgean

Department of Computer Science
Loughborough University, UK
A.M.Salagean@lboro.ac.uk

Abstract

We show that repeated-root cyclic codes over a finite chain ring are not principally generated. Repeated-root negacyclic codes are principally generated if the ring is a Galois ring of characteristic 2, but in other cases they are not principally generated. We also prove results on the structure, cardinality and Hamming distance of repeated root cyclic and negacyclic codes.

1 Introduction

When studying cyclic codes over finite fields, most authors assume from the outset that the length n of the code is not divisible by the characteristic p of the field. This ensures that $x^n - 1$, and therefore the generator polynomial of any cyclic code, will have no multiple factors, and hence no repeated roots in an extension field. Cyclic codes where $p|n$ were called 'repeated-root cyclic codes' and have been studied in [5] and [15] (strictly speaking, only codes where $p|n$ and the generator has multiple factors were called repeated-root codes, but we will use this term to refer to all codes with $p|n$). We will call 'simple root cyclic codes' the codes where n is not divisible by p.

Cyclic codes over a finite ring rather than a field have been studied over the last few years, motivated by the seminal paper [8]. Throughout this paper R will denote a finite chain ring, $\overline{R}$ its residue field and p the characteristic of $\overline{R}$. A cyclic code of length n over R is an ideal in $\mathcal{R} = R[x]/\langle x^n - 1\rangle$. The structure of such codes was described in [4, 9] for $R = \mathbb{Z}_{p^a}$, and in [13] for the more general case of a finite chain ring. Again, it is assumed in the aforementioned papers that n is not divisible by p i.e. we are dealing with simple root cyclic codes. The case of repeated-root cyclic codes was less studied. The structure of cyclic codes over a finite chain ring (covering both the simple-root and repeated-root case) was described in [14] and connections to Gröbner bases were made. Similar results on the structure of ideals appear in [11], but the connection with codes and Gröebner bases is not investigated. For the particular cases of $n = 2^e$ or $n = 2k$, with k odd, repeated-root cyclic codes over $\mathbb{Z}_4$ were studied in [1] and [3] respectively.

Negacyclic codes of length n over R are ideals in $\mathcal{Q} = R[x]/\langle x^n + 1\rangle$. Again, it is usually assumed that p does not divide n and we will distinguish between repeated-root and simple-root negacyclic codes according to whether p divides n or not. Simple-root negacyclic codes over $\mathbb{Z}_4$ have been studied in [16].

In this paper we are studying several issues regarding repeated-root cyclic and negacyclic codes over a finite chain ring R. In Section 3 we generalise a result of [6] and use it to show that where $p|n$, $\mathcal{R}$ is not a principal ideal ring. So in general repeated-root cyclic codes are not principally generated. This is in contrast to the situation for the simple-root cyclic codes, which are always principally generated, see [4]. The same holds for simple-root negacyclic codes. For repeated-root negacyclic codes the situation is slightly more complicated: $\mathcal{Q}$ is not a principal ideal ring when $p \neq 2$ or $p = 2 = \mathrm{char}(R)$. However, when $p = 2$ and R is a Galois ring, $\mathcal{Q}$ is a principal ideal ring.

In Section 4 we recall the structure of repeated-root cyclic codes from [14] and use it to generalise results from [12] to the case of repeated-root codes. Namely in Section 5 we determine the cardinality of a cyclic code and in Section 6 we show that the Hamming distance of a repeated-root cyclic code over R equals the Hamming distance of a certain, explicitly constructed, repeated-root cyclic code over the residue field of R.

Finally, in Section 7 we show that the results of Sections 4, 5 and 6 hold, with minor modifications, for negacyclic codes as well.

2 Notation

Throughout this paper R will denote a finite chain ring which is not a field. Recall that a finite chain ring is a finite ring whose ideals are linearly ordered. Examples of finite chain rings include $\mathbb{Z}_{p^a}$ with p a prime and $a \geq 1$ and Galois rings. The main properties of R that are used in this paper are collected below:

Proposition 2.1 *A finite chain ring R is a local principal ideal ring with maximal ideal $\mathcal{N}(R)$, the nilradical of R; the elements of $R \setminus \mathcal{N}(R)$ are units. Let γ be a fixed generator of $\mathcal{N}(R)$ and ν the nilpotency index of γ i.e. the smallest positive integer for which $\gamma^\nu = 0$.*
(i) The distinct proper ideals of R are $\langle \gamma^i \rangle$, $i = 1, \ldots, \nu - 1$.
(ii) For any element $r \in R \setminus \{0\}$ there is a unique i and a unit u such that $r = u\gamma^i$, where $0 \leq i \leq \nu - 1$ and u is unique modulo $\gamma^{\nu - i}$.
(iii) For any $r \in R$, if $r\gamma^i = 0$ then $r \in \langle \gamma^{\nu - i} \rangle$.

From now on, γ and ν will be as in Proposition 2.1. We will denote by $\overline{R} = R/\mathcal{N}(R)$ the residue field of R and by the prime number p the characteristic of $\overline{R}$. Recall that the characteristic of R will then be a power of p.

We will also denote by $\overline{r}$ the image of an element $r \in R$ under the canonical projection from R to $\overline{R}$. This projection extends naturally to a projection from $R[x]$ to $\overline{R}[x]$.

Example 2.2 *(i) For $R = \mathbb{Z}_{p^a}$ we have $\gamma = p$, $\nu = a$, $\overline{R} = \mathbb{Z}_p$ and $\overline{r} = r \bmod p$.*
(ii) If R is a Galois ring $R = \mathrm{GR}(p^a, m) = \mathbb{Z}_{p^a}[x]/\langle t \rangle$ with t a basic irreducible polynomial of degree m, then $\gamma = p$, $\nu = a$, $\overline{R} = \mathrm{GF}(p^m)$ and $\overline{r} = r \bmod p$.

A cyclic code of length n over R is an ideal in $\mathcal{R} = R[x]/\langle x^n - 1 \rangle$. A negacyclic code of length n over R is an ideal in $\mathcal{Q} = R[x]/\langle x^n + 1 \rangle$.

A polynomial over a field is called square-free if it has no multiple irreducible factors in its decomposition. The square-free part of a polynomial over a field is the product of all its distinct irreducible factors.

3 Repeated-root cyclic codes are not principally generated

It was shown in [4, Corollary of Theorem 6] that simple-root cyclic codes over $\mathbb{Z}_{p^a}$ are always principal ideals. Using the same technique the result can be generalised as follows ([13, Theorem4.6], cf. also [6]):

Theorem 3.1 *Let $f \in R[x]$ be a monic polynomial such that $\overline{f}$ is square-free. Then $R[x]/\langle f \rangle$ is a principal ideal ring.*

Hence simple-root cyclic and negacyclic codes over R are principally generated.

For repeated-root codes cyclic codes it was proven in [1] and [3] that for $R = \mathbb{Z}_4$ and $n = 2^e$ or $n = 2k$ with k odd, the codes are not principally generated.

To examine the general case we will need the following theorem, which is a modified version of [6, Theorem 4], generalised from $R = \mathbb{Z}_{p^a}$ to R a finite chain ring. The proof is similar and has been included in the Appendix for completeness.

Theorem 3.2 *(cf. [6]) Let $f \in R[x]$ be a monic polynomial which 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 $f = gh + \gamma u$ with $u \in R[x]$. Then $R[x]/\langle f \rangle$ is a principal ideal ring iff $\overline{u} \neq 0$ and $\overline{u}$ and $\overline{h}$ are coprime.*

Corollary 3.3 *With the notations of Theorem 3.2, if f and h have a non-trivial common factor as polynomials in $R[x]$, then $R[x]/\langle f \rangle$ is not a principal ideal ring.*

PROOF. If $\overline{u} = 0$, by Theorem 3.2, $R[x]/\langle f \rangle$ is not a principal ideal ring. So let us assume $\overline{u} \neq 0$. Let $d \in R[x]$ be the non-trivial common divisor of f and h. Write $f = df_1$ and $h = dh_1$ with $f_1, h_1 \in R[x]$. We have $df_1 = gdh_1 + \gamma u$, hence $\gamma u = d(f_1 - gh_1)$. This means $\overline{d(f_1 - gh_1)} = 0$, which implies $\overline{(f_1 - gh_1)} = 0$, since $\overline{d} \neq 0$. Hence all coefficients of $f_1 - gh_1$ are divisible by γ so we can write $f_1 - gh_1 = \gamma u_1$ for some $u_1 \in R[x]$. Then $\gamma u = \gamma d u_1$, so $\overline{u} = \overline{d}\overline{u_1}$. Hence $\overline{u}$ and $\overline{h}$ are not coprime, since they have $\overline{d}$ as a common factor. By Theorem 3.2 we can now infer that $R[x]/\langle f \rangle$ is not a principal ideal ring. □

Theorem 3.4 *Assume $p|n$. Then:*
(i) $\mathcal{R}$ is not a principal ideal ring.
(ii) If $p \neq 2$ or if $p = 2$ and $\mathrm{char}(R) = 2$ then $\mathcal{Q}$ is not a principal ideal ring.
(iii) If $\gamma = p = 2$ (in particular if R is a Galois ring with $p = 2$) then $\mathcal{Q}$ is a principal ideal ring.

PROOF. Since $p|n$, we can write n as $n = kp^b$ for some $b \geq 1$ and $p \not| k$. In $\overline{R}[x]$ we have:

$$\begin{aligned} x^{kp^b} - 1 &= (x^k - 1)^{p^b} \\ x^{kp^b} + 1 &= (x^k + 1)^{p^b} \end{aligned}$$

since $\begin{pmatrix} p^b \\ i \end{pmatrix} \equiv 0 \bmod p$ for all $0 < i < p^b$ and $(-1)^{p^b} = -1$ if p is odd and $(-1)^{p^b} = 1 = -1$ if $p = 2$.

(i) Putting $f = x^n - 1$, $g = x^k - 1$ and $h = (x^k - 1)^{p^b - 1}$ with $f, g, h \in R[x]$ we have that $\overline{f} = \overline{g}\overline{h}$ and $\overline{g}$ is the square-free part of $\overline{f}$. Note that $x^k - 1$ divides $f = x^{kp^b} - 1$ in $R[x]$.

Hence $x^k - 1$ is a common factor of f and h, so by Corollary 3.3 $\mathcal{R}$ is not a principal ideal ring.

(ii) If $p \neq 2$, put $f = x^n + 1$, $g = x^k + 1$ and $h = (x^k + 1)^{p^b - 1}$ with $f, g, h \in R[x]$. We have that $\overline{f} = \overline{g}\overline{h}$ and $\overline{g}$ is the square-free part of $\overline{f}$. Since p^b is odd, $x^k + 1$ is a factor of $f = x^{kp^b} + 1$. Hence $x^k + 1$ is a common factor of f and h, so by Corollary 3.3 $\mathcal{Q}$ is not a principal ideal ring. Now assume $p = 2$ and $\mathrm{char}(R) = p = 2$. Then $1 = -1$ in R, so $R[x]/\langle x^n + 1\rangle = R[x]/\langle x^n - 1\rangle$ in this case, i.e. $\mathcal{Q} = \mathcal{R}$ is not a principal ideal ring.

(iii) Now $p = 2$ and $\gamma = p = 2$. We put $f = x^n + 1$, $g = x^k + 1$ and $h = (x^k + 1)^{2^b - 1}$ with $f, g, h \in R[x]$. We have that $\overline{f} = \overline{g}\overline{h}$ and $\overline{g}$ is the square-free part of $\overline{f}$. There is a $u \in R[x]$ such that $f = gh + 2u$. We will determine now $\overline{u}$. We have:

$$-2u = gh - f = (x^k + 1)^{2^b} - (x^{k2^b} + 1) = \sum_{i=1}^{2^b - 1} \begin{pmatrix} 2^b \\ i \end{pmatrix} x^{ki}$$

By Kummer's Theorem we know that all $\begin{pmatrix} 2^b \\ i \end{pmatrix}$ with $i = 1, \ldots, 2^b - 1$ are divisible by 4, except for $\begin{pmatrix} 2^b \\ 2^{b-1} \end{pmatrix}$, which is divisible by 2 but not by 4. Hence: $\overline{u} = x^{k2^{b-1}}$. Obviously $\overline{u}$ is coprime to $\overline{h}$, hence by Corollary 3.3 $\mathcal{Q}$ is a principal ideal ring. □

4 Generators for repeated-root cyclic codes

We recall below [14, Theorem 4.2]. As usual, elements of $\mathcal{R}$ are identified with polynomials of degree less than n.

Theorem 4.1 *Let $C \subset \mathcal{R}$ be a non-zero cyclic code. Then C admits a set of generators*

$$C = \langle \gamma^{j_0} g_0, \ldots, \gamma^{j_s} g_s \rangle$$

where $0 \leq s \leq \nu - 1$ and
(i) $0 \leq j_0 < \cdots < j_s \leq \nu - 1$
(ii) g_i monic for $i = 0, \ldots, s$,
(iii) $n > \deg(g_0) > \deg(g_1) > \ldots > \deg(g_s)$,
(iv) $\gamma^{j_{i+1}} g_i \in \langle \gamma^{j_{i+1}} g_{i+1}, \ldots \gamma^{j_s} g_s \rangle$ for $i = 0, \ldots, s-1$.
(v) $\gamma^{j_0}(x^n - 1) \in \langle \gamma^{j_0} g_0, \ldots, \gamma^{j_s} g_s \rangle$
Moreover this set of generators is also a strong Gröbner basis.

Remark 4.2 *Note that this is a structure theorem for both simple-root and repeated-root cyclic codes. Conditions (iv) and (v) imply that $\overline{g}_s | \overline{g}_{s-1} | \ldots | \overline{g}_0 | \overline{x^n - 1}$. For the simple root case we show in [14, Theorem 4.3] that conditions (iv) and (v) can be replaced by the stronger condition $g_s | g_{s-1} | \ldots | g_0 | x^n - 1$ retrieving thus the structure theorems of [4] and [13]. For repeated-root codes, conditions (iv) and (v) cannot be improved in general: there are codes for which no set of generators of the form given in Theorem 4.1 has the property $g_s | g_{s-1} | \ldots | g_0 | x^n - 1$ (see [14, Example 3.3]).*

5 The cardinality of cyclic codes over a finite chain ring

In [13, Theorem 4.5] we determine the cardinality of a simple-root cyclic code over a finite chain ring. The result can be generalised to arbitrary cyclic codes (repeated-root or simple root) as follows:

Theorem 5.1 *Let C be a cyclic code given by a system of generators as in Theorem 4.1. Then*

$$|C| = |\overline{R}|^{\sum_{i=0}^{s}(\nu-j_i)(d_{i-1}-d_i)}$$

where $d_i = \deg(g_i)$ for $i = 0, \ldots, s$ and $d_{-1} = n$.

PROOF. By Theorem 4.1, the set of generators $G = \{\gamma^{j_0}g_0, \ldots, \gamma^{j_s}g_s\}$ is also a strong Gröbner basis. Hence for any $g \in R[x]$ with $\deg(g) < n$ we have that g represents a codeword in C iff g strongly reduces to 0 w.r.t. G. Let g be such a polynomial. No matter what polynomial in G is used at each reduction step, the final result of reducing g will still be 0. We can therefore impose that we will always use $\gamma^{j_i}g_i$ with minimum possible i. The reduction becomes then unique and yields polynomials $v_0, \ldots, v_s \in R[x]$ with $g = \sum_{i=0}^{s} v_i\gamma^{j_i}g_i$, $\deg(v_i) < d_{i-1} - d_i$ and v_i unique modulo $\gamma^{\nu-j_i}$ for $i = 0, \ldots, s$. There are therefore $|\overline{R}|^{(\nu-j_i)(d_{i-1}-d_i)}$ possibilities of choosing each v_i. □

6 The Hamming distance of repeated-root cyclic codes over a finite chain ring

For simple-root cyclic codes over R it was shown in [12] that their Hamming distance coincides with the Hamming distance of certain, explicitly constructed, simple-root cyclic codes over $\overline{R}$. Here we will show that the same happens for repeated-root cyclic codes.

We will denote by $\mathrm{d}_H()$ and $\mathrm{wt}_H()$ the Hamming distance and Hamming weight, respectively.

Theorem 6.1 *Let C be a cyclic code given by a set of generators as in Theorem 4.1. We have: $\mathrm{d}_H(C) = \mathrm{d}_H(\langle\overline{g_s}\rangle)$.*

PROOF. By [12, Theorem 4.2] we know that $\mathrm{d}_H(C) = \mathrm{d}_H(C \cap \langle\gamma^{\nu-1}\rangle) = \mathrm{d}_H(\overline{(C:\gamma^{\nu-1})})$ where $(C:\gamma^{\nu-1})$ is the ideal quotient $(C:\gamma^{\nu-1}) = \{g \in \mathcal{R} | \gamma^{\nu-1}g \in C\}$. (The main idea in the proof of this result is that multiplying a codeword by γ decreases its weight, so when looking for words of minimum Hamming weight in C is suffices to look in $C \cap \langle\gamma^{\nu-1}\rangle$. The second equality follows from the fact that for any $g \in \mathcal{R}$, both $\gamma^{\nu-1}g$ and $\overline{g}$ have non-zero coefficients exactly in those positions where g has unit coefficients, and so $\mathrm{wt}_H(\gamma^{\nu-1}g) = \mathrm{wt}_H(\overline{g})$.)

We have $C \cap \langle\gamma^{\nu-1}\rangle = \langle\gamma^{\nu-1}g_s\rangle$ as the set of generators in Theorem 4.1 is also a strong Gröbner basis and we can reduce any element of $C \cap \langle\gamma^{\nu-1}\rangle$ to 0 using only $\gamma^{j_s}g_s$. Hence $(C:\gamma^{\nu-1}) = \{g \in \mathcal{R} | \gamma^{\nu-1}g \in \langle\gamma^{\nu-1}g_s\rangle\} = \langle g_s, \gamma\rangle$ and $\overline{(C:\gamma^{\nu-1})} = \langle\overline{g_s}\rangle$. We have therefore $\mathrm{d}_H(C) = \mathrm{d}_H(\overline{(C:\gamma^{\nu-1})}) = \mathrm{d}_H(\langle\overline{g_s}\rangle)$ as required. □

Hence if C is a repeated-root cyclic code, its Hamming distance equals the Hamming distance of $\langle\overline{g_s}\rangle$. The latter is a repeated-root cyclic code over the finite field $\overline{R}$ for which the results of [5] and [15] concerning the Hamming distance apply.

7 Negacyclic codes

The results in Sections 4, 5 and 6 also hold for negacyclic codes, reformulated accordingly. We obtain valid theorems if we replace "C is a cyclic code" by "C is a negacycyclic code" and $x^n - 1$ by $x^n + 1$ in Theorems 4.1, 5.1 and 6.1.

8 Appendix

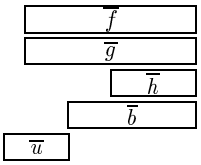
Proof of Theorem 3.2

It is known that a finite ring is principal iff its radical is principal (see [2, Propositions 8.7 and 8.8] and also [7, Lemma 3]). The ring $R[x]/\langle f\rangle$ is finite.

It is easy to see that $\mathcal{N}(\overline{R}[x]/\langle f\rangle) = \langle\overline{g}\rangle$ and $\mathcal{N}(R[x]/\langle f\rangle) = \langle g, \gamma\rangle$.

Assume first that $\overline{u} \neq 0$ and $\overline{u}$ and $\overline{h}$ are coprime. We will show that the radical is principal, namely $\langle g, \gamma\rangle = \langle v\rangle$ where $v = g + \gamma b$ and $b \in R[x]$ is such that $\overline{b} = \overline{g}/\gcd(\overline{g}, \overline{u})$.

To visualise the divisibility relationships between different polynomials in this proof, the following diagram may be useful. The regions that overlap (viewed vertically) represent common factors.



We have that $\overline{g}$ and $\overline{u} - \overline{bh}$ are coprime, since any factor of $\overline{g}$ is either a factor of $\overline{u}$ or a factor of $\overline{bh}$ but not both. By [10, Theorem XIII.4], g and $u - bh$ are coprime so there are polynomials $A, B, w \in R[x]$ such that $1 = Ag + B(u - bh)$. Multiplying by γ we obtain

$$\begin{aligned}\gamma &= \gamma Ag + \gamma B(u - bh)\\ &= \gamma A(v - \gamma b) + B(\gamma u - \gamma bh)\\ &= \gamma Av + B(f - gh - (v - g)h) - \gamma^2 Ab\\ &= v(\gamma A - Bh) - \gamma^2 Ab\end{aligned}$$

Multiplying the last equation by $\gamma^{\nu-2}, \gamma^{\nu-1}, \ldots, 1$ and using each result in the next equation we obtain, successively:

$$\begin{aligned}\gamma^{\nu-1} &= \gamma^{\nu-2}v(\gamma A - Bh) - \gamma^{\nu} Ab = \gamma^{\nu-2}v(\gamma A - Bh) \in \langle v\rangle\\ \gamma^{\nu-2} &= \gamma^{\nu-3}v(\gamma A - Bh) - \gamma^{\nu-1} Ab \in \langle v\rangle\\ &\vdots\\ \gamma &= v(\gamma A - Bh) - \gamma^2 Ab \in \langle v\rangle\end{aligned}$$

We proved therefore that $\gamma \in \langle v\rangle$ and now $g \in \langle v\rangle$ immediately follows. Hence $\langle g, \gamma\rangle = \langle v\rangle$.

For the converse result, assume that $\langle g, \gamma\rangle$ is a principal ideal and let v be its generator. Since $\overline{\langle g, \gamma\rangle} = \langle\overline{g}\rangle = \langle\overline{v}\rangle$ we can assume that $\overline{v} = \overline{g}$. Write v as $v = g + \gamma w$ for some $w \in R[x]$. Since $\gamma \in \langle v\rangle$, there are $A, B \in R[x]$ such that $\gamma = Af + Bv$. Hence $0 = \overline{Af} + \overline{Bv} =$

$\overline{Agh} + \overline{Bg} = \overline{g}(\overline{Ah} + \overline{B})$. We have therefore that $\overline{B}$ is divisible by $\overline{h}$ i.e. there are B_1, c such that $B = hB_1 + \gamma c$. Now $\gamma = Af + Bv$ becomes $\gamma = A(gh + \gamma u) + (hB_1 + \gamma c)v = h(Ag + b_1 v) + \gamma(Au + cv)$. So $\overline{h}$ divides $\overline{1 - Au + cv} = \overline{1 - Au + cg}$. By definition, $\overline{h}$ divides $\overline{g}$, so $\overline{h}$ divides $\overline{1 - Au}$. If $\overline{u}$ was zero, then we would have that $\overline{h}$ divides 1, which is a contradiction. Also, if there was a non-trivial common factor of $\overline{h}$ and $\overline{u}$, that common factor would be a factor of 1, which is again a contradiction. Hence we obtained that $\overline{u} \neq 0$ and $\overline{u}$ and $\overline{h}$ are coprime, as required.

References

[1] T. Abualrub and R. Oehmke. Cyclic codes of length 2^e over $\mathbb{Z}_4$. In *Proceedings of the Workshop on Coding and Cryptography, Paris*, Electronic Notes in Discrete Mathematics, pages 15–21, 2001. http://www.elsevier.nl:80/inca/publications/store/5/0/5/6/0/9/.

[2] M. Atiyah and I. McDonald. *Introduction to Commutative Algebra.* Longman Higher Education, 1969.

[3] T. Blackford. Cyclic codes over $\mathbb{Z}_4$ of oddly even length. In *Proceedings of the Workshop on Coding and Cryptography, Paris*, Electronic Notes in Discrete Mathematics, pages 83–92, 2001. http://www.elsevier.nl:80/inca/publications/store/5/0/5/6/0/9/.

[4] A. R. Calderbank and N. J. A. Sloane. Modular and p-adic codes. *Designs, Codes and Cryptography*, 6:21–35, 1995.

[5] G. Castagnoli, J.L. Massey, P.A. Schoeller, and N. von Seemann. On repeated-root cyclic codes. *IEEE Trans on Information Theory*, 37:337–342, 1991.

[6] J. Cazaran and A.V. Kelarev. Generators and weights of polynomial codes. *Archiv der Mathematik*, 69:479–486, 1997.

[7] J. Cazaran and A.V. Kelarev. On finite principal ideal rings. *Acta Math. Univ. Comenianae*, LXVIII:77–84, 1999.

[8] 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*, 40:301–319, 1994.

[9] P. Kanwar and S. R. López-Permouth. Cyclic codes over the integers modulo $\mathbb{Z}_{p^m}$. *Finite Fields and Their Applications*, 3:334–352, 1997.

[10] B. R. McDonald. *Finite Rings with Identity.* Marcel Dekker, New York, 1974.

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

[12] G.H. Norton and A. Sălăgean. On the Hamming distance of linear codes over finite chain rings. *IEEE Trans on Information Theory*, 46:1060–1067, 2000.

[13] G.H. Norton and A. Sălăgean. On the structure of linear and cyclic codes over finite chain rings. *Applicable algebra in engineering, communication and computing*, 10:489–506, 2000.

[14] G.H. Norton and A. Sălăgean. Cyclic codes and minimal strong Gröbner bases over a principal ideal ring. *Finite Fields and Applications*, 2002. to appear.

[15] J.H. van Lint. Repeated-root cyclic codes. *IEEE Trans on Information Theory*, 37:343–345, 1991.

[16] J. Wolfmann. Negacyclic and cyclic codes over $\mathbb{Z}_4$. *IEEE Trans. in Information Theory*, 45:2527–2532, 1999.