Available online at www.sciencedirect.com

SCIENCE DIRECT®

Discrete Applied Mathematics 154 (2006) 413–419

DISCRETE APPLIED MATHEMATICS

www.elsevier.com/locate/dam

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

Ana Sălăgean*

*Department of Computer Science, Loughborough University, Loughborough, Leics LE11 3TU, UK*

Received 11 September 2003; received in revised form 5 March 2004; accepted 21 March 2005
Available online 21 September 2005

**Abstract**

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


*Keywords:* Repeated-root cyclic codes; Finite chain ring; Principal ideal ring

## 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 [7,20,12] (strictly speaking, only the codes where $p|n$ and the generator polynomial has multiple factors were called repeated-root codes, but here we will use this term to refer to all codes with $p|n$). We will call "simple-root cyclic codes" the codes with $n$ not divisible by $p$.

Cyclic codes over a finite ring rather than a field have been extensively studied over the last few years, motivated by [10]. Throughout this paper $R$ will denote a finite chain ring (e.g. $\mathbb{Z}_{p^a}$, the ring of integers modulo a power of a prime $p$, or a Galois 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 $\mathscr{R} = R[x]/\langle x^n - 1\rangle$. The structure of such codes was described in [6,11] for $R = \mathbb{Z}_{p^a}$, and in [17] 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. All proofs make essential use of this assumption and the proof techniques cannot be directly adapted to the case when $p|n$.

Repeated-root cyclic codes over finite rings have been less studied. The structure of cyclic codes over a finite chain ring (covering both the simple-root and repeated-root case) was derived in [19] using Gröbner bases techniques. Similar results on the structure of ideals in $R[x]$ were proven in [14,15] using different techniques. Repeated-root cyclic codes over $\mathbb{Z}_4$ for different particular cases of $n$ were studied in [1,2,4].

* Tel.: 44 1509 228 237; Fax: 44 1509 211 586
*E-mail address:* A.M.Salagean@lboro.ac.uk.

0166-218X/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.dam.2005.03.016

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. For $R = \mathbb{Z}_4$, simple-root negacyclic codes have been studied in [21] and repeated-root negacyclic codes in [5].

In this paper, we are studying several issues regarding repeated-root cyclic and negacyclic codes over a finite chain ring $R$. The main result is in Section 3, Theorem 3.4. We show that when $p|n$, $\mathcal{R}$ is not a principal ideal ring, which means that for any $n$ a multiple of $p$ there exist repeated-root cyclic codes of length $n$ which are not principally generated. This is in contrast to the situation for the simple-root cyclic codes, which are always principally generated, see [6]. Simple-root negacyclic codes too are always principally generated. For repeated-root negacyclic codes the situation is slightly more complicated: we show that $\mathcal{Q}$ is a principal ideal ring when $R$ is a Galois ring and $p = 2$, but in all other cases it is not principal. The main ingredient in the proof of these results is a theorem of [8,9], which we recall in a slightly generalised form and with a simplified proof. For the particular case of codes of even length over $R = \mathbb{Z}_4$ our results show that repeated-root negacyclic codes are always principal, whereas repeated-root cyclic codes are not. We retrieve thus results of [1,2,4,5].

In the remainder of the sections, the results on the structure, cardinality and Hamming distance of simple-root cyclic codes described in [19] (see also [6,11]) are generalised to include both simple-root and repeated-root cyclic codes. Namely in Section 5 we determine a generator matrix and 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 $R$. In proving these results we make use of the Gröbner basis of a cyclic code derived in [19] and recalled in Section 4. The canonical generating systems described in [14,15] could also be used.

Finally, in Section 7 we show that the results of Sections 4–6 hold for negacyclic codes as well.

## 2. Notation

Throughout this paper $R$ will denote a commutative 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 $\mathbb{Z}_{p^a}$ (the ring of integer residues modulo a prime $p$, with $a$ an integer, $a \geqslant 1$) and Galois rings. The main properties of $R$ that are used in this paper are collected below (see for example [13,22]):

**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 $R\backslash\mathcal{N}(R)$ are units. Let $\gamma$ be a fixed generator of $\mathcal{N}(R)$ and $v$ the nilpotency index of $\gamma$ i.e. the smallest positive integer for which $\gamma^v = 0$.*

(i) *The distinct proper ideals of $R$ are $\langle\gamma^i\rangle$, $i = 1, \ldots, v-1$.*
(ii) *For any element $r \in R\backslash\{0\}$ there is a unique $i$ and a unit $u$ such that $r = u\gamma^i$, where $0 \leqslant i \leqslant v-1$ and $u$ is unique modulo $\gamma^{v-i}$.*
(iii) *For any $r \in R$, if $r\gamma^i = 0$ then $r \in \langle\gamma^{v-i}\rangle$.*

From now on, $\gamma$ and $v$ will be as in Proposition 2.1. We will denote by $\overline{R} = R/\langle\gamma\rangle$ 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 $\gamma = p$, $v = a$, $\overline{R} = \mathbb{Z}_p$ 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 $\gamma = p$, $v = a$, $\overline{R} = \mathrm{GF}(p^m)$ 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 over a finite chain ring are not principally generated

Cyclic and negacyclic codes over a field (regardless of being simple-root or repeated-root) are always principal ideals and admit as generator a divisor of $x^n - 1$ (or $x^n + 1$, respectively).

It was shown in [6, Corollary of Theorem 6] that simple-root cyclic codes over $\mathbb{Z}_{p^a}$ are always principal ideals but they do not always admit as generator a divisor of $x^n - 1$. Using the same technique the result can be generalised as follows ([17, Theorem 4.6], cf. also [8]):

**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 cyclic codes it was proven in [1,4] that for $R = \mathbb{Z}_4$ and $n = 2^e$ or $n = 2k$ with $k$ odd, $\mathscr{R}$ is not a principal ideal ring.

To examine the general case we will need the following theorem, which is a generalisation of [8, Theorem 4]; see also [9, Theorem 2]. We simplified the proof and included it in the appendix for completeness.

**Theorem 3.2** (*cf. Cazaran and Kelarev [8,9]*). *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 $f = gh + \gamma u$ 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.*

Note that in the original theorems [8, Theorem 4, 9, Theorem 2] the polynomials $g, h, u$ are constructed in a unique way and the construction relies on the structure of the particular ring, whereas here we allow any choice for the polynomials $g, h, u$, provided they satisfy the looser properties mentioned in the theorem.

**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 $\overline{d}\,\overline{(f_1 - gh_1)} = 0$, which implies $\overline{(f_1 - gh_1)} = 0$, since $\overline{d} \neq 0$. Hence 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, as 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.** *Let $R$ be a finite chain ring and $p$ the characteristic of its residue filed. Let $\mathscr{R} = R[x]/\langle x^n - 1\rangle$ and $\mathscr{Q} = R[x]/\langle x^n + 1\rangle$. If $p|n$ then*:

(i) *$\mathscr{R}$ is not a principal ideal ring.*
(ii) *If $p > 2$ or if $p = 2$ and $R$ is not a Galois ring then $\mathscr{Q}$ is not a principal ideal ring.*
(iii) *If $p = 2$ and $R$ is a Galois ring then $\mathscr{Q}$ is a principal ideal ring.*

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

$$x^{kp^b} - 1 = (x^k - 1)^{p^b},$$

$$x^{kp^b} + 1 = (x^k + 1)^{p^b}$$

since $\binom{p^b}{i} \equiv 0 (\mathrm{mod}\ p)$ 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, $\mathscr{R}$ is not a principal ideal ring.

(ii) and (iii) 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 $\overline{f}$.

Consider first the case $p > 2$. 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 $\mathscr{Q}$ is not a principal ideal ring.

Now assume $p = 2$. There is a $u \in R[x]$ such that $f = gh + \gamma u$. We determine $\gamma u$:

$$\gamma u = f - gh = x^{k2^b} + 1 - (x^k + 1)^{2^b} = -\sum_{i=1}^{2^b - 1} \binom{2^b}{i} x^{ki}.$$

By Kummer's Theorem we know that all $\binom{2^b}{i}$ with $i = 1, \ldots, 2^b - 1$ are divisible by 4, except for $\binom{2^b}{2^{b-1}}$, which is divisible by 2 but not by 4. Hence: $\gamma u = 2tx^{k2^{b-1}} + 4w$ for some odd integer $t$ and some $w \in R[x]$. If $R$ is a Galois ring then $\gamma = 2$ so $\overline{u} = x^{k2^{b-1}}$. Obviously $\overline{u}$ is coprime to $\overline{h}$, hence by Theorem 3.2, $\mathscr{Q}$ is a principal ideal ring.

Assume now $R$ is not a Galois ring. By [13, Lemma XVII.4], any finite chain ring $R$ contains a Galois ring $T = \mathrm{GR}(p^a, r)$ and $\gamma^s = pv$ for some $s \geqslant 1$ and $v \in T[x]$ a unit. Moreover, when $R$ is not a Galois ring one can show that $s \geqslant 2$. We have $p = 2 = \gamma^s v^{-1}$ and so $\gamma u = \gamma^s v^{-1} t x^{k2^{b-1}} + \gamma^{2s} v^{-2} w$. Hence $\overline{u} = 0$ and by Theorem 3.2, $\mathscr{Q}$ is not a principal ideal ring. □

For the important particular case $R = \mathbb{Z}_4$, Theorem 3.4 becomes:

**Corollary 3.5.** *If $n$ is even then $\mathbb{Z}_4[x]/\langle x^n + 1\rangle$ is a principal ideal ring and $\mathbb{Z}_4[x]/\langle x^n - 1\rangle$ is not a principal ideal ring.*

Hence all repeated-root negacyclic codes over $\mathbb{Z}_4$ are principal. For any even $n$ there are repeated-root cyclic codes over $\mathbb{Z}_4$ which are not principal. We retrieved therefore results of [1,2,4,5].

## 4. Generators of cyclic codes over a finite chain ring

Generators of a particular form for ideals in $R[x]$ were described in [14,15]. The structure of minimal Gröbner bases for ideals in $R[x]$ was described in [19]. It turns out that the two notions coincide.

We recall below [19, Theorem 4.2], which describes Gröbner bases for cyclic codes over $R$. As usual, elements of $\mathscr{R}$ are identified with polynomials of degree less than $n$.

**Theorem 4.1.** *Let $C \subset \mathscr{R}$ 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* $0 \leqslant s \leqslant v - 1$ *and*

(i) $0 \leqslant j_0 < \cdots < j_s \leqslant v - 1$
(ii) $g_i$ *monic for* $i = 0, \ldots, s$,
(iii) $n > \deg(g_0) > \deg(g_1) > \cdots > \deg(g_s)$,
(iv) $\gamma^{j_{i+1}} g_i \in \langle \gamma^{j_{i+1}} g_{i+1}, \ldots \gamma^{j_s} g_s \rangle$ *in* $R[x]$, *for* $i = 0, \ldots, s - 1$,
(v) $\gamma^{j_0}(x^n - 1) \in \langle \gamma^{j_0} g_0, \ldots, \gamma^{j_s} g_s \rangle$ *in* $R[x]$.

*Moreover this set of generators is a strong Gröbner basis.*

The following is an immediate consequence of [18, Theorem 7.5]:

**Proposition 4.2.** *Let $C \subset \mathcal{R}$ be a non-zero cyclic code. A Gröbner basis of $C$ as described in Theorem* 4.1 *is not necessarily unique. However, the cardinality of the basis, the degrees of its polynomials and the exponents $j_0, \ldots, j_s$ are unique.*

**Remark 4.3.** Note that Theorem 4.1 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 [19, 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 [6,17]. 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 [19, Example 3.3]).

## 5. The generator matrix and the cardinality of cyclic codes over a finite chain ring

In [17, Theorem 4.5] we determine a generator matrix and 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 set of generators as in Theorem* 4.1. *Denote $d_i = \deg(g_i)$ for $i = 0, \ldots, s$ and $d_{-1} = n$. Then*

(i) *The matrix consisting of the rows corresponding to the codewords $\gamma^{j_i} x^k g_i$ with $i = 0, \ldots, s$ and $k = 0, \ldots, d_{i-1} - d_i - 1$ is a generator matrix for $C$.*
(ii) $|C| = |\overline{R}|^{\sum_{i=0}^{s} (v-j_i)(d_{i-1}-d_i)}$.

**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 $\gamma^{v-j_i}$ for $i = 0, \ldots, s$. There are therefore $|\overline{R}|^{(v-j_i)(d_{i-1}-d_i)}$ possibilities of choosing each $v_i$. □

The formula for the cardinality of the code, as well as the size of the generator matrix in the theorem above, do not depend on the choice of minimal Gröbner basis, as $s$, $d_i$ and $j_i$ are unique by Proposition 4.2.

**Remark 5.2.** Note that a generator matrix for a cyclic code $C$ cannot be directly constructed from an arbitrary (non-Gröbner basis) set of generators of $C$. Another advantage of describing $C$ by a Gröbner basis rather than an arbitrary set of generators is that we have an immediate method for error detection. Namely, a polynomial of degree smaller than $n$ represents a codeword if and only if it strongly reduces to 0 with respect to the Gröbner basis. Equivalently, one can use for error detection a parity check matrix derived from a generator matrix. However, as noted earlier, we would need a Gröbner basis in the first place for deriving a generator matrix.

## 6. The Hamming distance of cyclic codes over a finite chain ring

For simple-root cyclic codes over $R$ it was shown in [16] that their Hamming distance coincides with the Hamming distance of certain, explicitly constructed, simple-root cyclic codes over $\overline{R}$. Here we will extend this result to include 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.** As in [16, Theorem 4.2] one can show that $\mathrm{d}_H(C) = \mathrm{d}_H(C \cap \langle\gamma^{v-1}\rangle) = \mathrm{d}_H(\overline{(C : \gamma^{v-1})})$ where $(C : \gamma^{v-1})$ is the ideal quotient $(C : \gamma^{v-1}) = \{g \in \mathcal{R} | \gamma^{v-1} g \in C\}$ . (The main idea in the proof of this result is that multiplying a

codeword by $\gamma$ decreases its weight, so when looking for words of minimum Hamming weight in $C$ is suffices to look in $C \cap \langle \gamma^{v-1} \rangle$. The second equality follows from the fact that for any $g \in \mathscr{R}$, both $\gamma^{v-1} g$ and $\overline{g}$ have non-zero coefficients exactly in those positions where $g$ has unit coefficients, and so $\mathrm{wt}_H(\gamma^{v-1} g) = \mathrm{wt}_H(\overline{g})$.)

We have $C \cap \langle \gamma^{v-1} \rangle = \langle \gamma^{v-1} g_s \rangle$ as the set of generators in Theorem 4.1 is also a strong Gröbner basis and we can reduce any element of $C \cap \langle \gamma^{v-1} \rangle$ to 0 using only $\gamma^{j_s} g_s$. Hence $(C : \gamma^{v-1}) = \{g \in \mathscr{R} | \gamma^{v-1} g \in \langle \gamma^{v-1} g_s \rangle\} = \langle g_s, \gamma \rangle$ and so $\overline{(C : \gamma^{v-1})} = \langle \overline{g_s} \rangle$. We have therefore $\mathrm{d}_H(C) = \mathrm{d}_H(\overline{(C : \gamma^{v-1})}) = \mathrm{d}_H(\langle \overline{g_s} \rangle)$ 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 [12,7,20] concerning the Hamming distance apply.

## 7. Negacyclic codes

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

## Appendix

**Proof of Theorem 3.2.** It is known that a finite ring is principal iff its radical is principal (see [3, Propositions 8.7 and 8.8] and also [9, Lemma 3]). The ring $R[x]/\langle f \rangle$ is finite. It is easy to see that $\mathscr{N}(\overline{R}[x]/\langle f \rangle) = \langle \overline{g} \rangle$ and $\mathscr{N}(R[x]/\langle f \rangle) = \langle g, \gamma \rangle$, where $\mathscr{N}(\,)$ denotes the nilradical. Hence it suffices to prove that $\langle g, \gamma \rangle$ is principal iff $\overline{u} \neq 0$ and $\overline{u}$ and $\overline{h}$ are coprime.

Assume first that $\overline{u} \neq 0$ and $\overline{u}$ and $\overline{h}$ are coprime. We will show that $\langle g, \gamma \rangle$ is principal, namely it is generated by $v = g + \gamma b$ where $b \in R[x]$ is such that $\overline{b} = \overline{g} / \gcd(\overline{g}, \overline{u})$. In $R[x]/\langle f \rangle$ we have $vh = (g + \gamma b)h = gh + \gamma bh = \gamma(bh - u)$. Note that $\overline{bh - u}$ and $\overline{f}$ are coprime, since any factor of $\overline{f}$ is either a factor of $\overline{u}$ or a factor of $\overline{bh}$ but not both. By [13, Theorem XIII.4], $f$ and $u - bh$ are coprime so $u - bh$ is invertible in $R[x]/\langle f \rangle$. Hence $\gamma = vh(bh - u)^{-1} \in \langle v \rangle$ and therefore $g = v - \gamma b \in \langle v \rangle$, so $\langle g, \gamma \rangle = \langle v \rangle$.

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 may 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 $\gamma = Af + Bv$ in $R[x]$. Hence $0 = \overline{Af} + \overline{Bv} = \overline{Agh} + \overline{Bg} = \overline{g}(\overline{Ah} + \overline{B})$. We have therefore that $B = -Ah + \gamma c$ for some $c \in R[x]$. Now $\gamma = Af + Bv$ becomes $\gamma = A(gh + \gamma u) + (-Ah + \gamma c)(g + \gamma w) = \gamma(Au - Ahw + gc) + \gamma^2 cw$. Therefore $1 = \overline{A(u - hw)} + \overline{gc}$ i.e. $\overline{u - hw}$ and $\overline{g}$ are coprime in $\overline{R}[x]$. Since all irreducible factors of $\overline{h}$ are factors of $\overline{g}$, it follows that $\overline{u} \neq 0$ and $\overline{h}$ and $\overline{u}$ are coprime, as required. □

## References


[1] T. Abualrub, 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, 2001, pp. 15–21. http://www.elsevier.nl:80/inca/publications/store/5/0/5/6/0/9/.

[2] T. Abualrub, R. Oehmke, On the generators of $\mathbb{Z}_4$ cyclic codes of length $2^e$, IEEE Trans. Inform. Theory 49 (2003) 2126–2133.

[3] M. Atiyah, I. McDonald, Introduction to Commutative Algebra, Longman Higher Education, New York, 1969.

[4] 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, 2001, pp. 83–92, http://www.elsevier.nl:80/inca/publications/store/5/0/5/6/0/9/.

[5] T. Blackford, Negacyclic codes over $\mathbb{Z}_4$ of even length, IEEE Trans. Inform. Theory 49 (2003) 1417–1424.

[6] A.R. Calderbank, N.J.A. Sloane, Modular and $p$-adic codes, Designs Codes Cryptogr. 6 (1995) 21–35.

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

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

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

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

[11] P. Kanwar, S.R. López-Permouth, Cyclic codes over the integers modulo $\mathbb{Z}_{p^m}$, Finite Fields Appl. 3 (1997) 334–352.

[12] J.L. Massey, D.J. Costello, J. Justesen, Polynomial weights and code constructions, IEEE Trans. Inform. Theory 19 (1973) 101–110.

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

[14] A.A. Nechaev, Linear recurrence sequences over commutative rings, Discrete Math. Appl. 2 (6) (1992) 659–683.

[15] A.A. Nechaev, D.A. Mikhailov, Canonical generating system of a monic polynomial ideal over a commutative artinian chain ring, Discrete Math. Appl. 11 (2001) 545–586.
[16] G.H. Norton, A. Sălăgean, On the Hamming distance of linear codes over finite chain rings, IEEE Trans. Inform. Theory 46 (2000) 1060–1067.
[17] G.H. Norton, A. Sălăgean, On the structure of linear and cyclic codes over finite chain rings, Appl. Algebra Engng. Comm. Comput. 10 (2000) 489–506.
[18] G.H. Norton, A. Sălăgean, Strong Gröbner bases for polynomials over a principal ideal ring, Bull. Austr. Math. Soc. 64 (2001) 505–528.
[19] G.H. Norton, A. Sălăgean, Cyclic codes and minimal strong Gröbner bases over a principal ideal ring, Finite Fields Appl. 9 (2003) 237–249.
[20] J.H. van Lint, Repeated-root cyclic codes, IEEE Trans. Inform. Theory 37 (1991) 343–345.
[21] J. Wolfmann, Negacyclic and cyclic codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 45 (1999) 2527–2532.
[22] O. Zariski, P. Samuel, Commutative Algebra, Springer, Berlin, 1979.