On the structure of linear and cyclic codes over finite chain rings

This item was submitted to Loughborough University’s Institutional Repository by the/an author.

Citation: NORTON and SALAGEAN, 2000. On the structure of linear and cyclic codes over finite chain rings. Applicable algebra in engineering, communication and computing, 10, pp. 489-506

Additional Information:

- This article was published in the journal, Applicable algebra in engineering, communication and computing [© Springer Verlag] and is also available at: http://springerlink.metapress.com/openurl.asp?genre=journal&issn=0938-1279

Metadata Record: https://dspace.lboro.ac.uk/2134/2328

Publisher: © Springer Verlag

Please cite the published version.
This item was submitted to Loughborough’s Institutional Repository by the author and is made available under the following Creative Commons Licence conditions.

![Creative Commons License](image)

**Attribution-NonCommercial-NoDerivs 2.5**

You are free:

- to copy, distribute, display, and perform the work

Under the following conditions:

**Attribution.** You must attribute the work in the manner specified by the author or licensor.

**Noncommercial.** You may not use this work for commercial purposes.

**No Derivative Works.** You may not alter, transform, or build upon this work.

- For any reuse or distribution, you must make clear to others the license terms of this work.
- Any of these conditions can be waived if you get permission from the copyright holder.

Your fair use and other rights are in no way affected by the above.

This is a human-readable summary of the Legal Code (the full license).

For the full text of this licence, please go to:
[http://creativecommons.org/licenses/by-nc-nd/2.5/](http://creativecommons.org/licenses/by-nc-nd/2.5/)
On the structure of linear and cyclic codes over finite chain rings

Graham Norton    Ana Sălăgean
Algebraic Coding Research Group
Centre for Communications Research
University of Bristol, U.K.

Abstract

We generalise structure theorems of Calderbank and Sloane for linear and cyclic codes over \( \mathbb{Z}_{p^a} \) to a finite chain ring. Our results are more detailed and do not use non-trivial results from Commutative Algebra.

Keywords: Finite chain ring, Galois ring, linear code, cyclic code.

1 Introduction

Codes over finite rings have received much attention recently after it was proved that important families of binary non-linear codes are in fact images under the Gray map of linear codes over \( \mathbb{Z}_4 \), see [HKC+94] and the references cited there.

We work with codes over a finite chain ring. Section 2 reviews finite chain and Galois rings and establishes several basic results. Examples of finite chain rings are Galois rings, and in particular \( \mathbb{Z}_{p^a} \) where \( p \) is a prime and \( a \geq 1 \). A finite chain ring is a local ring and we can define and decode alternant codes over a finite chain ring, see [NS00b]. See also [Woo99]. Galois rings are a natural setting for Reed-Solomon and generalised Reed-Muller codes. BCH codes can also be defined over Galois rings, in analogy to BCH codes over Galois fields, see [MS77, Chapter 7].

Let \( R \) be a finite chain ring, \( K \) its residue field, \( \gamma \) a fixed generator of the maximal ideal of \( R \) and \( \nu \) the nilpotency index of \( \gamma \). The canonical projections from \( R[X] \) and \( R^n \) to \( K[X] \) and \( K^n \), respectively, will be denoted by \( \overline{\cdot} \).

The paper proper begins in Section 3 with more detailed versions of the structure theorems for linear and for cyclic codes given in [CS95]. We generalise these results to finite chain rings and give new, elementary proofs. An important role is played by the tower \( \overline{C} = \overline{(C : \gamma^0)} \subseteq \ldots \subseteq \overline{(C : \gamma^n)} \) of linear/cyclic codes over \( K \) associated to any linear/cyclic code \( C \) over \( R \), see Definition 3.3. (Here \( (C : r) \) denotes the submodule quotient of \( C \) by \( r \in R \).) We construct generator matrices/ generator polynomials for these codes, given a generator matrix/ generator polynomials of \( C \). We also prove that for a cyclic code over \( R \) there is a unique set of generators of a form similar to the one given in [CS95] for \( R = \mathbb{Z}_{p^a} \).

Our proofs avoid the non-trivial Commutative Algebra invoked in [CS95], using instead properties of the codes \( \overline{(C : \gamma^i)} \) and the technique used in [CS95, Corollary to Theorem 6] for proving that \( \mathbb{Z}_{p^n}[X]/(X^n - 1) \) is principal. In [KL97] it is claimed that this technique is incorrect, by giving a

*Research supported by the U.K. Engineering and Physical Sciences Research Council under Grant L07680. A preliminary version of this paper was presented at the Workshop on Coding and Cryptography in Paris, January 1999.
counterexample. We show that their counterexample is incorrect, see Remark 4.7. The fact that for any finite chain ring $R$, $R[X]/(X^n - 1)$ is principal also follows by the technique of [CS95, loc. cit.].

There is a different set of generators which also provides a useful description of properties of a cyclic code; see [PQ96] for codes over $\mathbb{Z}_4$ and [KL97] for the generalisation to $\mathbb{Z}_{p^a}$. For a discussion of the connection between these two sets of generators, see [KL97].

When $R$ is a Galois field our results are either straightforward or reduce to classical results.

We make use of the structure theorems of this paper in [NS00a] for proving results about the Hamming distance of codes over a finite chain ring.

# 2 Preliminaries

## 2.1 Finite chain rings and Galois rings

We begin with the definition and some properties of finite chain rings and continue with Galois rings, following mainly [McD74].

**Definition 2.1** A finite commutative ring is called a finite chain ring if its ideals are linearly ordered by inclusion.

A simple example of a finite chain ring is the ring $\mathbb{Z}_{p^a}$ of integers modulo $p^a$, for some prime $p$ and $a \geq 1$. A finite chain ring is, obviously, a local ring. It is well known, and not difficult to prove that a ring is a finite chain ring if and only if it is a finite local principal ideal ring. Let $\gamma$ be a fixed generator of the maximal ideal of $R$. Then $\gamma$ is nilpotent and let $\nu$ be its nilpotency index i.e. the smallest integer such that $\gamma^\nu = 0$. Denote by $K$ the residue field $R/\gamma R$, which is finite.

Throughout this paper, $R$ denotes a finite chain ring with $1 \neq 0$, $\gamma$ a fixed generator of the maximal ideal of $R$, $\nu$ the nilpotency index of $\gamma$ and $K$ the residue field of $R$.

The ideals of $R$ are $\gamma^i R$, $i = 0, \ldots, \nu$. All the elements of the maximal ideal $R\gamma$ are nilpotent and the elements of $R \setminus R\gamma$ are units. There is a form of unique factorisation in $R$:

**Lemma 2.2 ([McD74, p. 340])** For any $r \in R$, $r \neq 0$ there is a unique integer $i$, $0 \leq i < \nu$ such that $r = u\gamma^i$, with $u$ a unit. The unit $u$ is unique modulo $\gamma^{\nu-i}$ only.

The following result will be used throughout the paper:

**Corollary 2.3** If $1 \leq i < j \leq \nu$ and $\gamma^i c \in \gamma^j R$ then $c \in \gamma^{j-i} R$. In particular, if $\gamma^i R = 0$ then $c \in \gamma^{\nu-i} R$.

There is a canonical projection homomorphism from $R$ to $K$. Denote by $\tau$ the image of an element $r \in R$ under this projection.

We now compute the cardinality $|\gamma^j R|$ of $\gamma^j R$ for $0 \leq j \leq \nu - 1$, in terms of $K$ and $\nu$.

**Lemma 2.4** Let $V \subseteq R$ be a system of representatives for the equivalence classes of $R$ under congruence modulo $\gamma$. (Equivalently, we can define $V$ to be a maximal subset of $R$ with the property that $r_1 \neq r_2$ for all $r_1, r_2 \in R$, $r_1 \neq r_2$.) Then:

(i) For all $r \in R$ there are unique $r_0, \ldots, r_{\nu-1} \in V$ such that $r = \sum_{i=0}^{\nu-1} r_i \gamma^i$.

(ii) $|V| = |K|$.

(iii) $|\gamma^j R| = |K|^{\nu-j}$ for $0 \leq j \leq \nu - 1$. 

2
Theorem 2.6 (Hensel lifting, [McD74, Theorem XIII.4])
monic polynomials and by monic we will mean having the leading coefficient equal to 1.
written as

\[ f u + g v = 1. \]
By [McD74, Theorem XIII.6], any \( f \in R[X] \) which is not divisible by \( \gamma \) can be written as \( f = u f_1 \) where \( u \) is a unit and \( f_1 \) is monic. We will therefore restrict our attention to monic polynomials and by monic we will mean having the leading coefficient equal to 1.

\[ g \in R[X] \text{ be monic. Assume there are } f_1, \ldots, f_k \in K[X] \text{ monic, pairwise coprime such that } \bar{g} = \prod_{i=1}^{k} f_i. \]
Then there are \( g_1, \ldots, g_k \in R[X] \text{ monic, pairwise coprime such that } g = \prod_{i=1}^{k} g_i \text{ and } \bar{g}_i = f_i. \]
We do not have unique factorisation in \( R[X] \) in general; for example in \( \mathbb{Z}_p^2[X] \) we have \( X^2 = (X - p)(X + p) \). However certain non-unit polynomials do factor uniquely into irreducibles, see

The projection \( R \to K \) extends naturally to a projection \( R[X] \to K[X] \); for any \( f \in R[X] \) we denote by \( \overline{f} \) its image under this projection; also, for a set \( C \subseteq R[X] \) we define \( \overline{C} = \{ \overline{f} \mid f \in C \} \).
A polynomial \( f \in R[X] \) is a unit if and only if \( \overline{f} \) is a unit and is a zero-divisor if and only if \( \overline{f} = 0 \), by [McD74, Theorem XIII.2].
Recall that a non-unit \( f \in R[X] \) is called basic irreducible if \( f \) and \( \overline{f} \) are irreducible.

Lemma 2.5 (i) Let \( f \in R[X] \). If \( \overline{f} \) is irreducible, then \( f \) is irreducible.
(ii) For any \( l \geq 1 \) there is a basic irreducible \( f \in \mathbb{Z}_{p^l}[X] \) of degree \( l \).

Proof. (i) If \( f = f_1 f_2 \) where \( f_1, f_2 \) are non-units, then \( \overline{f} = \overline{f_1} \overline{f_2} \) where \( \overline{f_1}, \overline{f_2} \) are non-units by [McD74, Theorem XIII.2].
(ii) Let \( f \in \mathbb{Z}_p[X] \) be irreducible and of degree \( l \). Since \( \mathbb{Z}_{p^l} \) is a local ring with residue field \( \mathbb{Z}_p \), we can find a monic \( g \in \mathbb{Z}_{p^l}[X] \) with \( \bar{g} = f \). Hence \( g \) is irreducible of degree \( l \) by part (i).

For any \( l \geq 1 \), one can construct a Galois extension ring of \( \mathbb{Z}_{p^l} \) as \( GR(p^a, l) = \mathbb{Z}_{p^a}[X]/(f) \) with \( p \) a prime number, \( a \geq 1 \) and \( f \in \mathbb{Z}_{p^a}[X] \) a monic basic irreducible polynomial of degree \( l \), which exists by Lemma 2.5. The ring \( GR(p^a, l) \) is called a Galois ring and has \( p^{al} \) elements. For \( l = 1 \) we obtain the ring \( \mathbb{Z}_{p^a} \). For \( a = 1 \) we obtain the finite field with \( p^l \) elements, \( GF(p^l) \). For \( a \geq b \), there is a natural projection homomorphism (reduction modulo \( p^b \)) from \( GR(p^a, l) \) to \( GR(p^b, l) \) with kernel \( GR(p^a, l)p^b \). For any multiple \( m \) of \( l \) there is an inclusion homomorphism \( GR(p^a, l) \subseteq GR(p^a, m) \).
A Galois ring \( GR(p^a, l) \) is a finite chain ring with maximal ideal generated by \( p \), the nilpotency index of \( p \) is \( a \) and the residue field is \( GF(p^l) \).

Any finite chain ring is a certain homomorphic image of a polynomial ring \( GR(p^a, l)[X] \), see [McD74, Theorem XVII.5].

2.2 Factorisation and Hensel lifting

Hensel lifting plays a key role in the construction of cyclic codes over \( R \). Recall that two non-unit polynomials \( f, g \in R[X] \) are coprime if they generate \( R[X] \) i.e. there are \( u, v \in R[X] \) such that \( f u + g v = 1 \). By [McD74, Theorem XIII.6], any \( f \in R[X] \) which is not divisible by \( \gamma \) can be written as \( f = u f_1 \) where \( u \) is a unit and \( f_1 \) is monic. We will therefore restrict our attention to monic polynomials and by monic we will mean having the leading coefficient equal to 1.

Theorem 2.6 (Hensel lifting, [McD74, Theorem XIII.4])
Let \( g \in R[X] \) be monic. Assume there are \( f_1, \ldots, f_k \in K[X] \) monic, pairwise coprime such that \( \bar{g} = \prod_{i=1}^{k} f_i. \) Then there are \( g_1, \ldots, g_k \in R[X] \) monic, pairwise coprime such that \( g = \prod_{i=1}^{k} g_i \) and \( \bar{g}_i = f_i. \)
Theorem 2.7. A polynomial $f$ is called square-free if $g^2 | f$ implies $g$ is a unit.

**Theorem 2.7** If $g \in R[X]$ is monic and $\overline{g}$ is square-free, then $g$ factors uniquely into monic, coprime basic irreducibles.

**Proof.** By [McD74, Theorem XIII.11], $g$ factors uniquely as $g = g_1 \cdots g_k$ where $g_i$ are monic, coprime and each $(g_i)$ is a primary ideal. Since $\overline{g}$ is square-free, so are the $\overline{g}_i$. It follows from [McD74, Proposition XIII.12] that $g_i = h_i + v_i$ where $h_i$ is basic irreducible and $v_i \in (\gamma R)[X]$. Thus each $\overline{g}_i$ is irreducible and $g_i$ is also irreducible, by Lemma 2.5(i). □

We will need the following lemma for analysing cyclic codes over $R$.

**Lemma 2.8** Let $f, g \in R[X]$. Then $f, g$ are coprime if and only if $\overline{f}, \overline{g}$ are coprime.

**Proof.** Let $I$ be the ideal of $R[X]$ generated by $f$ and $g$ and $J$ be the ideal of $K[X]$ generated by $\overline{f}$ and $\overline{g}$. It is easy to show that $\overline{I} = J$. Since $h \in R[X]$ is a unit if and only if $h$ contains a unit if and only if $J$ contains a unit. □

Lemma 2.8 can also be proved constructively: given $u, v \in K[X]$ such that $\overline{f}u + \overline{g}v = 1$, a technique similar to Hensel lifting can be used to obtain $u_1, v_1 \in R[X]$ such that $fu_1 + gv_1 = 1$.

### 2.3 The module $R^n$

We extend the projection of $R$ to $K$ to a projection of $R^n$ to $K^n$. For any element $c \in R^n$ we denote by $\overline{c}$ its image under this projection. For a set $C \subseteq R^n$, we define $\overline{C} = \{ \overline{c} \mid c \in C \}$.

For any constant $r \in R$ and any $c \in R^n$ we denote by $rc$ the usual multiplication of a vector by a scalar. Also, for a set $C \subseteq R^n$ we write $rC$ for the set $\{ rc \mid c \in C \}$. We will say that a vector is divisible by a constant $r \in R$ if all its entries are divisible by $r$. For any $c \in R^n$ there is a unique $i$ such that $c = \gamma^i e$, $0 \leq i \leq \nu - 1$ and $e \in R^n$ is not divisible by $\gamma$. As in Corollary 2.3, if $1 \leq i \leq j \leq \nu$ and $\gamma^j e \in \gamma^i R^n$ then $c \in \gamma^{i-j} R^n$. In particular, if $\gamma^j c = 0$ then $c \in \gamma^{\nu-i} R^n$. Thus for any $i$ with $0 \leq i \leq \nu - 1$ we easily obtain a well-defined $R$-homomorphism $\varphi : \gamma^i R^n \to (R/\gamma^{\nu-i} R)^n$ given by $\varphi(\gamma^i c) = (c_1 + \gamma^{\nu-i} R, \ldots, c_\nu + \gamma^{\nu-i} R)$ for any $c = (c_1, \ldots, c_\nu) \in R^n$. Indeed, $\varphi$ is an isomorphism. Now $\gamma^i R^n$ is also an $(R/\gamma^{\nu-i} R)$-module (with $(r + \gamma^{\nu-i} R) \cdot \gamma^i c = r \gamma^i c$ in the usual way) and it is easy to check that $\varphi$ is also an $(R/\gamma^{\nu-i} R)$-homomorphism.

**Lemma 2.9** Let $0 \leq i \leq \nu - 1$. The map $\varphi : \gamma^i R^n \to (R/\gamma^{\nu-i} R)^n$ given by $\varphi(\gamma^i c) = (c_1 + \gamma^{\nu-i} R, \ldots, c_\nu + \gamma^{\nu-i} R)$ for any $c = (c_1, \ldots, c_\nu) \in R^n$ is an isomorphism of $R$ and of $(R/\gamma^{\nu-i} R)$-modules. In particular $\varphi : \gamma^{\nu-1} R^n \to K^n$ given by $\varphi(\gamma^{\nu-1} c) = \overline{c}$ is an isomorphism of $K$-vector spaces.

### 3 The structure of linear codes over $R$

Recall that a linear code of length $n$ over $R$ is an $R$-submodule of $R^n$. From now on, by “code” we mean “linear code”. For $R = \mathbb{Z}_p$, the structure of codes is described in [CS95, p.22] We will now give more detailed versions of these theorems, generalised to a finite chain ring. We will also give new proofs.

#### 3.1 Generator matrices

For $k > 0$, $I_k$ denotes the $k \times k$ identity matrix.
Definition 3.1 (Generator matrix) Let $C$ be a code over $R$. A matrix $G$ is called a generator matrix for $C$ if $C = \text{rowspan}_{R}(G)$ and none of the rows of $G$ can be written as a linear combination of the other rows.

We say that $G$ is a generator matrix in standard form if after a suitable permutation of the coordinates,

$$G = \begin{pmatrix}
I_{k_0} & A_0 & A_{01} & A_{02} & \cdots & A_{0,\nu-1} & A_{0,\nu} \\
0 & \gamma I_{k_1} & \gamma A_{12} & \gamma A_{13} & \cdots & \gamma A_{1,\nu-1} & \gamma A_{1,\nu} \\
0 & 0 & \gamma^2 I_{k_2} & \gamma^2 A_{23} & \cdots & \gamma^2 A_{2,\nu-1} & \gamma^2 A_{2,\nu} \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \cdots & \gamma^{\nu-1} I_{k_{\nu-1}} & \gamma^{\nu-1} A_{\nu-1,\nu} \\
\end{pmatrix}$$

say, where the columns are grouped into blocks of sizes $k_0, k_1, \ldots, k_{\nu-1}, n - \sum_{i=0}^{\nu-1} k_i$ with $k_i \geq 0$. We associate to $G$ the matrix

$$A = \begin{pmatrix}
A_0 \\
\vdots \\
A_{\nu-1} \\
\end{pmatrix}.$$ 

Of course, if $k_i = 0$, the matrices $\gamma^i A_i$ and $A_i$ are suppressed in $G$ and $A$ respectively. For a given $G$ and $1 \leq i \leq \nu - 1$, the matrices $A_i$ are unique modulo $\gamma^{\nu-i}$ only (Lemma 2.2) and therefore the $A_i$ are unique.

Proposition 3.2 Any code has a generator matrix in standard form.

Proof. Given an arbitrary set of generators for a code, we obtain a generator matrix $G$ by successively eliminating from the set those elements that can be written as a linear combination of the other elements currently in the set.

To bring $G$ to standard form, we apply column permutations and elementary row operations: permuting rows, dividing a row by a unit, adding to a row another row multiplied by an element of $R$. Performing these operations on $G$ as for Gaussian elimination (with the restriction of not dividing by non-units) reduces $G$ to standard form.

For any code $C$ and any $r \in R$, $(C : r)$ is the submodule quotient $(C : r) = \{e \in R^n \mid re \in C\}$.

Definition 3.3 To any code $C$ over $R$ we associate the tower of codes

$$C = (C : \gamma^0) \subseteq \ldots \subseteq (C : \gamma^1) \subseteq \ldots \subseteq (C : \gamma^{\nu-1})$$

over $R$ and its projection to $K$,

$$\overline{C} = (\overline{C} : \gamma^0) \subseteq \ldots \subseteq (\overline{C} : \gamma^1) \subseteq \ldots \subseteq (\overline{C} : \gamma^{\nu-1}).$$

For $\mathbb{Z}_4$, the codes $\overline{C} = (\overline{C} : \gamma^0)$ and $\overline{C} = (\overline{C} : \gamma^1)$ were introduced in [CS93] (denoted there $C^{(1)}$ and $C^{(2)}$). The tower of codes over $K$ will play an important role throughout this paper.

The following result appears in [CS93, p. 34] for the particular case $R = \mathbb{Z}_4$.

Lemma 3.4 (i) Let $C$ be a code with generator matrix $G$ in standard form and $A$ as in (2). Then for $0 \leq i \leq \nu - 1$, $(C : \gamma^i)$ has generator matrix

$$\begin{pmatrix}
\overline{A}_0 \\
\vdots \\
\overline{A}_i \\
\end{pmatrix}.$$
and \( \dim((C : \gamma^i)) = k_0 + \ldots + k_i \).

(ii) If \( E_0 \subseteq E_1 \subseteq \ldots \subseteq E_{\nu - 1} \) are codes of length \( n \) over \( K \), then there is a code \( C \) of length \( n \) over \( R \) such that \( (C : \gamma^i) = E_i \) for \( i = 0, \ldots, \nu - 1 \).

**Proof.** (i) It is easy to check that the row span of the given matrix is contained in \((C : \gamma^i)\). Let \( e \in (C : \gamma^i) \) and let \( g \in (C : \gamma^i) \) be such that \( \bar{g} = e \). Since \( \gamma^i g \in C \) and \( G \) is a generating matrix for \( C \), there are \( v_j \in R^k \) such that

\[
\gamma^i g = (v_0, v_0 A_0 + \gamma v_1, \ldots, v_0 A_{0, \nu - 1} + v_1 \gamma A_{1, \nu - 1} + \ldots + \gamma^{\nu - 1} v_{\nu - 1}, v_0 A_{0, \nu} + \ldots + \gamma^{\nu - 1} v_{\nu - 1} A_{\nu - 1, \nu}).
\]

Since \( \gamma^i g \) is divisible by \( \gamma^i \), we must have \( v_0 = \gamma^i w_0 \) for some \( w_0 \in R^{k_0} \). The second block of entries of \( \gamma^i g \) becomes \( \gamma^i w_0 A_0 + \gamma w_1 \), hence \( v_1 = \gamma^{i - 1} w_1 \) for some \( w_1 \in R^{k_1} \). Continuing we obtain \( v_j = \gamma^{i-j} w_j \) for \( j = 0, \ldots, i \). Therefore \( \gamma^i g = \sum_{j=0}^{i} \gamma^i w_j A_j + \gamma^{i-1} v_{\nu - 1} A_{\nu - 1} \) and \( g \equiv \sum_{j=0}^{i} w_j A_j + \sum_{j=i+1}^{\nu - 1} v_j \gamma^{j-i} A_j \pmod{\gamma^{\nu-i}} \) by Corollary 2.3. Hence \( e = \bar{g} = \sum_{j=0}^{i} w_j A_j \) i.e. \((C : \gamma^i)\) is generated by the required matrix. The rows of this matrix are obviously linearly independent over \( K \), hence \( \dim((C : \gamma^i)) = k_0 + \ldots + k_i \).

(ii) Let \( l_i = \dim(E_i) \). After suitably permuting the coordinates we may assume that each \( E_i \) is generated by an \( l_i \times n \) matrix

\[
\begin{pmatrix}
L_0 \\
\vdots \\
L_i
\end{pmatrix}
\]

such that the square submatrix consisting of the first \( l_i \) columns is \( I_{l_i} \). We then choose matrices \( A_i \) over \( R \) such that \( A_i = L_i \) and define \( C \) to be the code with generator matrix

\[
\begin{pmatrix}
A_0 \\
\vdots \\
\gamma^{i-1} A_{\nu - 1}
\end{pmatrix}.
\]

Note that the code \( C \) is not unique as it depends on the choice of the \( A_i \).

\[ \square \]

**Theorem 3.5** Let \( C \) be a code of length \( n \) over \( R = GR(p^a, l) \). Then:

(i) The parameters \( k_0, \ldots, k_{\nu - 1} \) are the same for any generator matrix \( G \) in standard form for \( C \).

(ii) Any codeword \( c \in C \) can be uniquely written as \( c = (v_0, v_1, \ldots, v_{\nu - 1}) G \) where \( v_i \in (R/\gamma^{\nu-i} R)^{k_i} \cong (\gamma^i R)^{k_i} \).

(iii) \( |C| = |K|^{\sum_{i=0}^{\nu - 1} (\nu - i) k_i} \).

**Proof.** (i) The unicity of the \( k_i \)'s follows from the fact that \( k_0 = \dim(C) \) and \( k_i = \dim((C : \gamma^i)) - \dim((C : \gamma^{i-1})) \), for \( i = 1, \ldots, \nu - 1 \), by Lemma 3.4.

(ii) Put \( k = \sum_{i=0}^{\nu - 1} k_i \). Since \( G \) is a generator matrix for \( C \) the encoding map \( \text{enc}_G : R^k \to R^n \) defined by \( \text{enc}_G(v) = v G \) has the image \( \text{enc}_G(R^k) = C \). We prove that the kernel of this map is \( \prod_{i=0}^{\nu - 1} \gamma^{\nu-i} R^{k_i} \). Let \( v = (v_0, \ldots, v_{\nu - 1}) \) be such that \( v_i \in R^{k_i} \) and \( \text{enc}_G(v) = (v_0, v_0 A_0 + \gamma v_1, \ldots, v_0 A_{0, \nu - 1} + v_1 \gamma A_{1, \nu - 1} + \ldots + \gamma^{\nu - 1} v_{\nu - 1}, v_0 A_{0, \nu} + \ldots + \gamma^{\nu - 1} v_{\nu - 1} A_{\nu - 1, \nu}) = 0 \). Then \( v_0 = 0 \) and the second block of entries becomes \( v_1 \) and has to be 0, hence \( v_1 \in \gamma^{\nu-i} R^{k_i} \), as in Corollary 2.3. Continuing this way we obtain \( v_i \in \gamma^{\nu-i} R^{k_i} \) for all \( i = 0, \ldots, \nu - 1 \). Hence

\[
C \cong R^k / \prod_{i=0}^{\nu - 1} \gamma^{\nu-i} R^{k_i} \cong \prod_{i=0}^{\nu - 1} (R/\gamma^{\nu-i} R^{k_i})^{k_i} \cong \prod_{i=0}^{\nu - 1} (\gamma^i R)^{k_i}.
\]
which also gives $|C|$, using Lemma 2.4. 

The previous theorem justifies the following definition:

**Definition 3.6** For any code $C$ over $R$ we define $k(C)$ to be the numver of rows in a generator matrix in standard form of $C$. We also define $k_i(C)$, $i = 0, \ldots, \nu - 1$ as being the number of rows divisible by $\gamma_i$ but not by $\gamma_{i+1}$ in a generator matrix in standard form for $C$. (Equivalently we define \(k_0(C) = \dim(C)\) and \(k_i(C) = \dim((C : \gamma_i^r)) - \dim((C : \gamma_i^{r-1}))\) for $1 \leq i \leq \nu - 1$.)

Clearly $k(C) = \sum_{i=0}^{\nu-1} k_i(C)$.

**Corollary 3.7** If $C, D$ are codes of length $n$ over $R$ such that $C \subset D$ and $k_i(C) = k_i(D)$ for $i = 0, \ldots, \nu - 1$, then $C = D$.

Since finite products and finite direct sums coincide, we have also proved the following known result (see [McD74, Problem II, p.60 and Exercise XII.15]).

**Corollary 3.8** Any $R$-submodule $C$ of $R^n$ can be uniquely decomposed as a direct sum:

$$C \cong \bigoplus_{i=0}^{\nu-1} (R/\gamma_i^r R)^{k_i(C)} \cong \bigoplus_{i=0}^{\nu-1} \gamma_i^r R^{k_i(C)}$$

for some $k_i(C) \geq 0$.

**Corollary 3.9** Let $C$ be an $R$-submodule of $R^n$. If $G \subset R^n$ is such that $C = \text{rowspan}(G)$ and $C \neq \text{rowspan}(G')$ for any proper subset $G'$ of $G$, then $|G| = k(C)$.

### 3.2 The dual code

We will examine now the structure of the dual of a code $C$, denoted, as usual, $C^\perp$.

**Theorem 3.10** Let $C$ be a code with generator matrix $G$ in standard form as in (1). Then

(i) If for $0 \leq i < j \leq \nu$, $B_{i,j} = -\sum_{k=i+1}^{j-1} B_{i,k} A_{\nu-j,\nu-k} - A_{\nu-j,\nu-i}^r$, then

$$H = \begin{pmatrix}
B_{0,\nu} & B_{0,\nu-1} & \cdots & B_{0,1} & I_{n-k(C)} \\
g_{B_{1,\nu}} & g_{B_{1,\nu-1}} & \cdots & g_{k_{\nu-1}(C)} & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
g_{\nu-1} B_{\nu-1,a} & g_{\nu-1} I_{k_1(C)} & \cdots & 0 & 0 \\
\end{pmatrix}
\begin{pmatrix}
B_0 \\
g_B \\
\vdots \\
g_{\nu-1} B_{\nu-1} \\
\end{pmatrix}
$$

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

(ii) For $i = 0, \ldots, \nu - 1$, $(C^\perp : \gamma_i^r) = ((C : \gamma_i^{r-1}))^\perp$. Also $k_0(C^\perp) = n - k(C)$ and $k_i(C^\perp) = k_{\nu-1}(C)$, for $i = 1, \ldots, \nu - 1$.

(iii) $|C^\perp| = |R^n|/|C|$ and $(C^\perp)^\perp = C$.

**Proof.** (i) It is straightforward to check that $HG^\text{tr} = 0$. Let $D$ be the $R$-module generated by $H$. We have $k_0(D) = n - k(C)$, $k_i(D) = k_{\nu-1}(C)$ for $i = 1, \ldots, \nu - 1$ and $D$ is orthogonal to $C$, hence $D \subset C^\perp$. The equality $D = C^\perp$ will follow from Corollary 3.7 after proving that $k_i(C^\perp) = k_i(D)$ for $i = 0, \ldots, \nu - 1$.

(ii) We prove first that $(C^\perp : \gamma_i^r) \perp (C : \gamma_i^{r-1})$. Let $b \in (C^\perp : \gamma_i^r)$ and $e \in (C : \gamma_i^{r-1})$. Then $\gamma^r b \in C^\perp$ and $\gamma_i^{r-1} e \in C$ and $\gamma_i^{r-1} be^r = 0$ i.e. $b e^r = 0$. For vector spaces, we know that
the sum of the dimensions of two orthogonal subspaces of $K^n$ cannot exceed the dimension of the whole space. Since $D \subseteq C^\perp$, we have $(D : \gamma^i) \subseteq (C^\perp : \gamma^i)$ for all $i$, and so

$$
n \geq \dim((C : \gamma^{\nu-i-1})) + \dim((C^\perp : \gamma^i))
\geq \dim((C : \gamma^{\nu-i-1})) + \dim((D : \gamma^i))
= k_0(C) + \ldots + k_{\nu-i-1}(C) + k_0(D) + \ldots + k_i(D)
= k_0(C) + \ldots + k_{\nu-i-1}(C) + n - k(C) + k_{\nu-i}(C) + \ldots + k_{\nu-1}(C) = n.
$$

Hence $\dim((C^\perp : \gamma^i)) = \dim((D : \gamma^i)) = n - \dim((C : \gamma^{\nu-i-1}))$, which implies \((C^\perp : \gamma^i) = ((C : \gamma^{\nu-i-1}))^\perp\) and $k_i(C^\perp) = k_i(D)$ for $i = 0, \ldots, \nu - 1$.

(iii) Easy consequence of (ii).

We associate the matrix

$$
B = \begin{pmatrix}
B_0 \\
\vdots \\
B_{\nu-1}
\end{pmatrix}
$$

of Theorem 3.10 to $H$. As in (2), $B$ is not unique: for example we could choose $B_{i,i+1} = -A_{\nu-i-1,\nu-i} + \gamma V$ with $V$ an arbitrary $k_{\nu-i-1}(C) \times k_{\nu-i}(C)$ matrix.

**Corollary 3.11** Let $C$ be a code with generator matrix $G$ as in (1), parity check matrix $H$ as in (3) and let $A, B$ be associated to $G, H$ as in (2) and (4). Then $\overline{C}$ has generator matrix $\overline{A}_0$ and parity check matrix $\overline{B}$.

**Proof.** Use the fact that $(\overline{C})^\perp = ((C : \gamma^0))^\perp = (C^\perp : \gamma^{\nu-1})$. \qed

### 3.3 Free codes

**Definition 3.12** We say that a code over $R$ is free if it is a free $R$-module.

Obviously, over a field any code is free. The following characterisations of a free code are immediate:

**Proposition 3.13** Let $C$ be a code over $R$. The following assertions are equivalent:

(i) $C$ is a free code.

(ii) If $G$ is a generator matrix for $C$ in standard form, then $G = (I \ M)$ for some matrix $M$.

(iii) $k(C) = k_0(C)$.

(iv) $\overline{C} = (C : \gamma) = \ldots = (C : \gamma^{\nu-1})$.

(v) $C^\perp$ is a free code.

(vi) $\overline{C}$ has generator matrix $\overline{G}$ and parity check matrix $\overline{H}$.

For other characterisations of free codes over a finite chain ring see also [NS00a, Corollary 3.12].

### 4 The structure of cyclic codes

The structure of cyclic codes over $\mathbb{Z}_{p^e}$ was presented in [CS95, Theorem 6]. Their proof uses Lasker-Noether decomposition of ideals and the construction of an idempotent. We prefer an
elementary approach which does not appeal to Commutative Algebra and which generalises easily to finite chain rings. An alternative description of the structure of cyclic codes over \( \mathbb{Z}_p \), as well as its connection to [CS95] appears in [KL97].

Recall that a code is cyclic if a cyclic shift of any codeword is a codeword. We assume that \( n \) is not divisible by the characteristic of \( K \) so that \( X^n - 1 \) is square-free in \( K[X] \) and by Theorem 2.7 it has a unique decomposition into distinct monic basic irreducible factors in \( R[X] \). We write \( R_n \) for the quotient ring of \( R[X] \) by the ideal generated by \( X^n - 1; K_n \) is similarly defined. As usual, we identify \((R^n, +) \) and \((R_n, +) \). If \( f \in R[X] \) has degree \( n - 1 \) or less, we identify \( f \) and its quotient class in \( R_n \). A code \( C \) of length \( n \) is cyclic if and only if it is an ideal of \( R_n \). Clearly if \( C \) is cyclic so is \( \overline{C} \). For a cyclic code \( C \), \( (C : \gamma^i) = \{e \in R_n | \gamma^i e \in C \} \) is the ideal quotient of \( C \) by \( \gamma^i \) in \( R_n \); in particular, \( (C : \gamma^i) \) is cyclic for \( 0 \leq i \leq \nu - 1 \). The ideal generated by \( f_1, \ldots, f_s \in R_n \) or \( f_1, \ldots, f_s \in K_n \) will be denoted by \( \text{id}(f_1, \ldots, f_s) \).

### 4.1 Generating sets in standard form

**Definition 4.1 (Generating set in standard form)** We say that the set \( S = \{\gamma^{a_0} g_{a_0}, \gamma^{a_1} g_{a_1}, \ldots, \gamma^{a_s} g_{a_s} \} \) is a generating set in standard form for the cyclic code \( C = \text{id}(S) \) if \( 0 \leq s < \nu \), \( 0 \leq a_0 < a_1 < a_2 < \cdots < a_s < \nu \), and \( g_i \in R[X] \) are monic, \( \deg(g_i) > \deg(g_{i+1}) \) for \( i = 0, \ldots, s - 1 \) and \( g_{a_s} | g_{a_{s-1}} | \cdots | g_{a_0} | X^n - 1 \).

We will use the following lemmas to construct a unique generating set in standard form for a non-zero cyclic code.

**Lemma 4.2** If \( C \) is a non-zero cyclic code, then \( (C : \gamma^{\nu-1}) \neq \{0\} \).

**Proof.** Let \( c \in C, c \neq 0 \). By Lemma 2.2, we can write \( c = \gamma^i u \) for some \( i, 0 \leq i \leq \nu - 1 \) and unit \( u \). Since \( C \) is an ideal, \( \gamma^{\nu-1} u \in C \) i.e. \( u \in (C : \gamma^{\nu-1}) \) and \( 0 \neq \pi \in (C : \gamma^{\nu-1}) \). \( \square \)

**Lemma 4.3** Let \( S = \{\gamma^{a_0} g_{a_0}, \gamma^{a_1} g_{a_1}, \ldots, \gamma^{a_s} g_{a_s} \} \) be a generating set in standard form for \( C = \text{id}(S) \). If \( i < a_0 \) then \( (C : \gamma^i) = \{0\} \), otherwise \( (C : \gamma^i) = \text{id}(\overline{g_{a_i}}) \) where \( j \) is maximal with the property \( a_j \leq i \).

**Proof.** Let \( e \in (C : \gamma^i) \). There is a \( g \in (C : \gamma^i) \) such that \( \overline{g} = e \). Since \( \gamma^i g \in \text{id}(S) \), we can write \( \gamma^i g = \sum_{k=0}^{s} h_{a_k} \gamma^{a_k} g_{a_k} \pmod{\gamma^{\nu-i}} \), hence \( e = \overline{g} = 0 \) and we are done. Otherwise, let \( j \) be maximal such that \( a_j \leq i \). Since \( g_{a_j} | g_{a_{j-1}} | \cdots | g_{a_0} \), we can write \( \gamma^i g = h_{a_j} g_{a_j} + \sum_{k=j+1}^{s} h_{a_k} \gamma^{a_k} g_{a_k} \) for some \( h \in R[X] \). Now both \( \gamma^i g \) and \( \sum_{k=j+1}^{s} h_{a_k} \gamma^{a_k} g_{a_k} \) are divisible by \( \gamma^i \) and \( g_{a_j} \) is monic, so \( h \) must be divisible by \( \gamma^i \) i.e. \( h = \gamma^t h \) for some \( t \in R[X] \). Hence \( e = \overline{g} = \overline{h_{a_j}} \) i.e. \( (C : \gamma^i) \subseteq \text{id}(\overline{g_{a_j}}) \). The other inclusion is immediate. \( \square \)

For any \( f \in K[X] \) such that \( f | X^n - 1 \), Theorems 2.7 and 2.6 imply the existence and unicity of a polynomial \( g \in R[X] \) such that \( \overline{g} = f \) and \( g | X^n - 1 \), since \( X^n - 1 \) is square-free in \( K[X] \). The polynomial \( g \) will be called the Hensel lift of \( f \).

**Theorem 4.4** (cf. [CS95, Theorem 6]) Any non-zero cyclic code \( C \) over \( R \) has a unique generating set in standard form.

**Proof.** We first prove the existence. From Lemma 4.2, \( (C : \gamma^{\nu-1}) \neq \{0\} \) and we can define \( 0 \leq s < \nu, 0 \leq a_0 < a_1 < a_2 < \cdots < a_s < \nu \) by requiring that the inclusions \( \{0\} \subset (C : \gamma^{a_0}) \subset (C : \gamma^{a_1}) \subset \cdots \subset (C : \gamma^{a_s}) \) are strict and \( s \) is maximal.
Since $C$ is cyclic, the $(C : \gamma^t)$'s are cyclic codes over $K$. Choose $f_{a_j} \in R[X]$ monic such that $\gamma^{a_j} f_{a_j} \in C$ and $\overline{f}_{a_j}$ is the unique monic generator polynomial of $(C : \gamma^{a_j})$. Let $g_{a_j}$ be the Hensel lift of $\overline{f}_{a_j}$. It is easy to check that $S = \{ \gamma^{a_0} g_{a_0}, \gamma^{a_1} g_{a_1}, \ldots, \gamma^{a_s} g_{a_s} \}$ is a generating set in standard form for $D = \text{id}(S)$.

For proving $D = C$, we first prove that $\gamma^{a_j} g_{a_j} \in C$ for $j = 0, 1, \ldots, s$. (The technique is similar to the one used in [CS95, Corollary of Theorem 6].) Since $\overline{g}_{a_j} = \overline{f}_{a_j}$, there are polynomials $h_{a_j} \in R[X]$ such that $\gamma h_{a_j} := f_{a_j} - g_{a_j}$. Let $v_{a_j} := (X^n - 1)/g_{a_j}$. We have $\gamma^{a_j} f_{a_j} v_{a_j} = \gamma^{a_j} (g_{a_j} + h_{a_j}) v_{a_j} = \gamma^{a_j + 1} h_{a_j} v_{a_j}$ in $R[X]/(X^n - 1)$. Hence $\gamma^{a_j + 1} h_{a_j} v_{a_j} \in C$. Now $\overline{v}_{a_j}$ and $\overline{f}_{a_j}$ are coprime in $R[X]$ since $\overline{v}_{a_j} = (X^n - 1)/g_{a_j}$ and $\overline{f}_{a_j} = \overline{g}_{a_j}$. Hence $v_{a_j}$ and $f_{a_j}$ are also coprime in $R[X]$ by Lemma 2.8 if there are monomials $u$ and $v$ such that $v_{a_j} v + f_{a_j} u = 1$. Multiplying this relation by $\gamma^{a_j + 1} h_{a_j}$, we obtain $\gamma^{a_j + 1} h_{a_j} v_{a_j} v + \gamma^{a_j + 1} h_{a_j} f_{a_j} u = \gamma^{a_j + 1} h_{a_j}$. Since $\gamma^{a_j + 1} h_{a_j} v_{a_j} \in C$ and $\gamma^{a_j} f_{a_j} \in C$, we obtain $\gamma^{a_j + 1} h_{a_j} \in C$ and therefore $\gamma^{a_j} g_{a_j} = \gamma^{a_j} f_{a_j} - \gamma^{a_j + 1} h_{a_j} \in C$. Thus $D \subseteq C$. We chose $f_{a_j}$ such that $(C : \gamma^t) = \text{id}(\overline{f}_{a_j}) = \text{id}(\overline{g}_{a_j})$ for $a_j \leq i < a_{j+1}$. On the other hand, by Lemma 4.3(i), $(D : \gamma^t) = \text{id}(\overline{g}_{a_j})$ for $a_j \leq i < a_{j+1}$. Therefore $(C : \gamma^t) = (D : \gamma^t)$ for $i = 0, \ldots, \nu - 1$, which implies $k_i(C) = k_i(D)$ and, by Corollary 3.7, $C = D$.

Next we prove the unicity of the generating set in standard form for $C$. Let $\{ \gamma^{b_0} h_{a_0}, \gamma^{b_1} h_{a_1}, \ldots, \gamma^{b_s} h_{a_s} \}$ be another generating set in standard form for $C$. By Lemma 4.3 and since $\overline{h}_{a_s}$ is a strict divisor of $\overline{h}_{a_j}$, the inclusions $\{0\} \subset (C : \gamma^{b_0}) \subset (C : \gamma^{b_1}) \subset \ldots \subset (C : \gamma^{b_s})$ are strict and $t$ is maximal. Hence $t = s$ and $b_j = a_j$ for $j = 0, 1, \ldots, s$. Also, $(C : \gamma^{a_j}) = \text{id}(\overline{g}_{a_j}) = \text{id}(\overline{h}_{a_j})$, so $\overline{g}_{a_j} = \overline{h}_{a_j}$ as they are both monic divisors of $X^n - 1$. Finally $g_{a_j}$ and $h_{a_j}$ are equal as they are the Hensel lift of $g_{a_j} = h_{a_j}$.

Henceforth all cyclic codes will be non-zero. Next we relate generating sets in standard form to generator matrices.

**Theorem 4.5** Let $S = \{ \gamma^{a_0} g_{a_0}, \gamma^{a_1} g_{a_1}, \ldots, \gamma^{a_s} g_{a_s} \}$ be a generating set in standard form for the code $C$ = $\text{id}(S)$. Then:

(i) If $T = \bigcup_{i=0}^{s} \{ \gamma^{a_i} g_{a_i} X^{d_i - d_{i+1}}, \ldots, \gamma^{a_i} g_{a_i} X, \gamma^{a_i} g_{a_i} \}$ where $d_i = \text{deg}(g_{a_i})$ for $i = 0, \ldots, s$ and by convention $d_{-1} = n, d_{s+1} = 0$, then $T$ defines a generator matrix for $C$.

(ii) Any $c \in C$ can be uniquely written as $c = \sum_{j=0}^{s} h_j g_{a_j} \gamma^{a_j}$ with $h_j \in (R/R\gamma^{a_j})[X]$ and $\text{deg}(h_j) < d_{j-1} - d_j$.

(iii) $k_i(C) = d_{j-1} - d_j$ if $i = a_j$ for some $j$, $k_i(C) = 0$ otherwise, and $|C| = |K| \sum_{j=0}^{s} (\nu - a_j) (d_{j-1} - d_j)$.

**Proof.** (i) As in the case of cyclic codes over a finite field, $C = \text{rowspan}(U)$, where

$$U = \bigcup_{j=0}^{s} \{ \gamma^{a_j} g_{a_j} X^{n - d_j - 1}, \ldots, \gamma^{a_j} g_{a_j} X, \gamma^{a_j} g_{a_j} \}.$$

Some of these polynomials can be removed from $U$ because they are linear combinations of the others. For example, since $g_{a_0}$ divides $g_{a_0}$, we can put $g_{a_0}/g_{a_0} = X^{d_0 - d_1} + h$ with $\text{deg}(h) < d_0 - d_1$. Then $X^{n-1-d_1} g_{a_1} = X^{n-1-d_1} g_{a_0} + X^{n-1-d_1} h g_{a_1}$, hence $X^{n-1-d_1} g_{a_1}$ can be removed from $U$. Similarly we can remove $X^{n-2-d_2} g_{a_2}, \ldots, X^{d_0-d_1} g_{a_1}, X^{d_1-d_2} g_{a_2},$ and so on. Finally, only the elements of $T$ remain in $U$. Since the polynomials in $T$ have distinct leading terms, none of them can be written as a linear combination of the others, and hence $T$ defines a generator matrix for $C$.

(ii) By (i), any $c \in C$ can be written as a linear combination of the elements of $T$ i.e. for $j = 0, \ldots, s$ there are $h_j \in R[X]$ such that $\text{deg}(h_j) < d_{j-1} - d_j$ and $c = \sum_{j=0}^{s} h_j \gamma^{a_j} g_{a_j} = \sum_{j=0}^{s} (h_j \text{mod } \gamma^{\nu-a_j}) \gamma^{a_j} g_{a_j}$. 


(iii) By Lemma 4.3(i), \( \dim((C : \gamma^i)) = 0 \) if \( i < a_0 \), otherwise \( \dim((C : \gamma^i)) = n - d_j \) where \( j \) is maximal such that \( a_j \leq i \). Then \( k_i(C) \) are computed using Definition 3.6 and \( |C| \) using Theorem 3.5(iii).

\[ \square \]

**Corollary 4.6 (cf. [CS95, Corollary to Theorem 6])** The ring \( R_n \) is principal.

**Proof.** Let \( C \) be an ideal of \( R_n \). As in the proof of [CS95, Corollary to Theorem 6], one shows that if \( \{ \gamma^{a_0}g_0, \gamma^{a_1}g_1, \ldots, \gamma^{a_s}g_s \} \) is a generating set in standard form for \( C \) then \( C = \id(\sum_{j=0}^{s} \gamma^{a_j}g_j) \).

**Remark 4.7** In the proof of Theorem 4.4 and Corollary 4.6 we used the technique of [CS95, Corollary to Theorem 6] for proving that \( \mathbb{Z}_p[X]/(X^n - 1) \) is principal. In [KL97] it is claimed that the proof of [CS95, loc. cit.] is incorrect, without indicating where the logical mistake is. Instead, [KL97, Example 3.1] is given, for which it is claimed that the single generator constructed by [CS95, loc. cit.] fails to generate a certain element of the ideal. We show below that this generator does in fact generate that particular element, so the counterexample is incorrect.

In \( \mathbb{Z}_8[X] \), \( X^7 - 1 = g_1g_2g_3 \) where \( g_1 = X - 1 \), \( g_2 = X^3 + 6X^2 + 5X + 7 \) and \( g_3 = X^3 + 3X^2 + 2X + 7 \). Let \( C = \id(f_0, 2f_1, 2^2f_2) \) where \( f_0 = g_2, f_1 = f_2 = 1 \). By [CS95, loc. cit.], \( g = f_0 + 2f_1 + 2^2f_2 = g_2 + 6 \) generates \( C \). Now, it is stated in [KL97, Example 3.1], that \( g \) does not generate \( C \) since \( f \notin \id(g) \) where \( f = g_2 + 2g_1g_3 \in C \). We will explicitly construct a polynomial \( h \) such that \( f = hg \). Indeed, division gives \( f = g(2X + 1) + 4(X^2 + 1) \). As in the proof of [CS95, loc. cit.], we show that \( 4 \in \id(g) \). We have \( 3g_1g_3g = 3g_1g_3(g_2 + 6) = 2g_1g_3 \) (mod \( X^7 - 1 \)) and \( 4g = 4g_2g \). Since \( g_2g \) and \( g_1g_3g \) are coprime, there are \( u, v \in R[X] \) such that \( g_2u + g_3g = 0 \), by Lemma 2.8. Hence \( 4 = 4g_2u + 4g_1g_3v = 4gu + 6g_1g_3v = g(4u + 6g_1g_3v) \) and consequently \( f = g(2X + 1 + (4u + 6g_1g_3v)(X^2 + 1)) \in \id(g) \).

### 4.2 The dual code

**Proposition 4.8** The dual of a cyclic code over \( R \) is cyclic.

**Proof.** Let \( C \) be cyclic and \( \pi : R^n \to R^n \) be the shift operator. If \( u \in C^\perp \) then for any \( c \in C \),

\[ \pi(u) \cdot c = \pi(u) \cdot \pi(\pi^{-1}(c)) = u \cdot \pi^{-1}(c) = 0. \]

So \( C^\perp \) is cyclic.

In particular, the dual of a cyclic code has a unique generating set in standard form, which we now construct. First recall that the reciprocal of a non-zero polynomial \( f(X) \) is \( f^*(X) = X^{\deg(f)}f(1/X) \). For a polynomial \( f \in R[X] \) whose constant term is a unit, we define \( f^\# \) to be equal to \( f^* \) divided by the leading coefficient of \( f^* \). In particular, the constant term of any divisor of \( X^n - 1 \) is a unit.

**Theorem 4.9** Let \( C \) be a cyclic code over \( R \) with \( \{ \gamma^{a_0}g_0, \gamma^{a_1}g_1, \ldots, \gamma^{a_s}g_s \} \) a generating set in standard form. Put \( a_{s+1} = \nu \) and for \( j = -1 \), \( g_a = X^{n-1} \). For \( j = 0, \ldots, s + 1 \), let \( b_j = \nu - a_{s+1-j} \) and \( h_{b_j} = ((X^n-1)/g_{a_{s+1-j}})^\# \). Then \( \{ \gamma^{b_0}h_{b_0}, \gamma^{b_1}h_{b_1}, \ldots, \gamma^{b_{s+1}}h_{b_{s+1}} \} \) is the generating set in standard form for \( C^\perp \).

**Proof.** Let \( S = \{ \gamma^{b_0}h_{b_0}, \gamma^{b_1}h_{b_1}, \ldots, \gamma^{b_{s+1}}h_{b_{s+1}} \} \) and let \( D = \id(S) \). It is straightforward to check that \( S \) is a generating set in standard form and that \( D \subseteq C^\perp \). We show that \( k_i(D) = k_{\nu-i}(C) \), which implies that \( D = C^\perp \) by Corollary 3.7 and Theorem 3.10(ii). From Theorem 4.5(iii) we have \( k_i(D) = \deg(h_{b_{s+1-j}}) - \deg(h_{b_j}) \) if \( i = b_j \) for some \( j \) and \( k_i(D) = 0 \) otherwise, which the reader may check is \( k_{\nu-i}(C) \).

\[ \square \]
4.3 The Hensel lift of a cyclic code

A natural way of constructing a cyclic code over $R$ is by lifting the generator polynomial of a cyclic code over $K$, as in [CS95]. See also [Sha79].

**Definition 4.10 (Hensel lift of a cyclic code)** Let $f \in K[X]$ be monic such that $f|X^n - 1$. The cyclic code $\text{id}(g)$ where $g$ is the Hensel lift of $f$ is called the Hensel lift of the cyclic code $\text{id}(f)$.

If $C$ is the Hensel lift of $E$ then $\overline{C} = E$, but $C$ is not the only cyclic code whose projection is $E$.

**Proposition 4.11** Let $C$ be a code over $R$. The following properties are equivalent:

(i) $C$ is the Hensel lift of a cyclic code.

(ii) $C$ is cyclic and free.

(iii) There is a $g \in R[X]$ such that $C = \text{id}(g)$ and $g|X^n - 1$.

(iv) There is a monic $g \in R[X]$ such that $\{g\}$ is the generating set in standard form for $C$.

(v) $C^\perp$ is the Hensel lift of a cyclic code.

**Remark 4.12** All the results on cyclic codes proved so far in this section also hold, with similar proofs, with $X^n - 1$ replaced by any polynomial $f$ of degree $n$ such that $\overline{f}$ is square-free in $K[X]$. We are then working with codes which are ideals in $R[X]/(f)$. For the particular case $f = X^n + 1$ we obtain negacyclic codes and for $f = X^n - c$, with $c \in R$, $c \neq 0$ we obtain constacyclic codes (see [Ber68, p. 303]).

4.4 Cyclic codes defined by roots of unity

For the case when $R$ is a Galois ring we give an alternative definition of cyclic codes in terms of the zeros of their codewords in a suitable extension ring.

Let $R = GR(p^a, l)$ and let $m \in \mathbb{N}$ be such that $l|m$ and $n|p^m - 1$. The ring $GR(p^a, m)$ is an extension of $R$ in which $X^n - 1$ has $n$ roots. By [McD74, Lemma XV.1], we can lift uniquely a primitive root of $X^n - 1$ from $GF(p^m)$ to a root $\xi$ of $X^n - 1$ in $GR(p^a, m)$. By [NS00b, Theorem 2.9], $\xi$ will also be primitive. For $0 \leq i \leq n - 1$ denote by $m_i \in K[X]$ the unique monic minimal polynomial of $\overline{\xi}^i$. Let $U$ be a set of representatives for the conjugacy classes of $\overline{\xi}$, i.e. a maximal subset of $\{0, \ldots, n - 1\}$ such that $m_i \neq m_j$ for all $i, j \in U$, $i \neq j$. It is well known that $X^n - 1 = \prod_{i \in U} m_i$. Denote by $M_i$ the Hensel lift of $m_i$, for $i = 0, \ldots, n - 1$. By Theorem 2.7, the $M_i$ are monic basic irreducible polynomials. We will need the following properties of the $M_i$.

**Lemma 4.13**

(i) For $i = 0, \ldots, n - 1$, $\{j \in \{0, \ldots, n - 1\} \mid M_i(\xi^j) = 0\} = \{j \in \{0, \ldots, n - 1\} \mid m_i(\overline{\xi}) = 0\}$

(ii) For $i = 0, \ldots, n - 1$, $M_i$ is the minimal polynomial of $\xi^i$.

(iii) $U$ is a set of representatives for the conjugacy classes of $\xi$.

(iv) Let $f \in R[X]$ and let $\{i_1, \ldots, i_v\} \subseteq U$. If $f(\xi^{i_j}) = 0$ for $j = 1, \ldots, v$ then $\prod_{j=1}^v M_{i_j}|f$.

(v) Let $f \in R[X]$ so that $f|X^n - 1$ and let $L \subseteq U$. Then $f = \prod_{i \in L} M_i$ if $L = \{i \in U \mid f(\xi^i) = 0\}$.

(vi) For $k = 1, \ldots, a - 1$, $M_i \mod p^k \in (R/p^k R)[X] \cong GR(p^k, l)[X]$, is the minimal polynomial of $\overline{\xi^i} \mod p^k$.

**Proof.** (i) All the roots of $m_i$ are powers of $\overline{\xi}$ and all the roots of $M_i$ are powers of $\xi$. If $M_i(\overline{\xi}) = 0$ then of course $\overline{M_i}(\overline{\xi}) = m_i(\overline{\xi}) = 0$. Conversely, let $\overline{\xi}^i$ be a root of $m_i$. Since $m_i$ has no multiple
roots, by [McD74], the root \( \xi^j \) of \( m_i \) can be uniquely lifted to a root of \( M_i \), say \( \xi^k \) such that \( \overline{\xi^k} = \overline{\xi^j} \). Since \( \overline{\xi} \) has order \( n \), it follows that \( k = j \).

(ii) and (iii) are immediate consequences of (i).

(iv) We use induction on \( v \). First consider \( v = 1 \) and assume that \( f \) is not divisible by \( M_i \). So dividing \( f \) by \( M_i \), we obtain \( f = qM_i + p^kr \) with \( q, r \in R[X] \), \( r \neq 0 \), \( \deg(r) < \deg(M_i) \), \( 0 \leq k \leq a - 1 \) and \( p \notdivide r \). Since \( p^kr(\xi^j) = 0 \), we obtain \( \tau(\xi^i) = 0 \) (applying Lemma 2.3 if \( k > 0 \)). This means that \( \tau \) is divisible by \( m_i \), the minimal polynomial of \( \xi^i \), which is impossible as \( \deg(\tau) < \deg(M_i) = \deg(m_i) \) since \( M_i \) is monic.

Next, assume \( v \geq 2 \). As above, there is some \( g \in R[X] \) such that \( f = M_i \cdot g \). From the definition of \( U \) follows that for \( j = 1, \ldots, v - 1 \), \( M_i(\xi^{jv}) = m_i(\xi^{jv}) \neq 0 \), hence \( M_i(\xi^{jv}) \) is a unit. So, for \( j = 1, \ldots, v - 1 \), \( f(\xi^jv) = 0 \) implies \( g(\xi^jv) = 0 \). Applying the induction hypothesis, \( \prod_{j=1}^{v-2} M_i \cdot g \).

(v) Use (iv) and the fact that any root of \( f \) is a power of \( \xi \).

(vi) Apply (ii) in the ring \( GR(p^k, l)[X] \), as \( M_i \mod p^k \) is obtained by Hensel lifting \( m_i \) to \( GR(p^k, l)[X] \). \( \square \)

Any set of roots \( \{\xi^1, \ldots, \xi^k\} \) defines a cyclic code \( \{c \in R_n \mid c(\xi^j) = 0, j = 1, \ldots, k\} \). The generator polynomial of this code is the product of the distinct elements in the set \( \{M_i, \ldots, M_k\} \) and a parity check matrix is

\[
H = \begin{pmatrix}
1 & \xi^1 & \xi^{2i_1} & \cdots & \xi^{(n-1)i_1} \\
\vdots & \vdots & \vdots & & \vdots \\
1 & \xi^{i_k} & \xi^{2i_k} & \cdots & \xi^{(n-1)i_k}
\end{pmatrix}
\]

This construction is described in [Sha79]. The more general case of codes with several generator polynomials appears implicitly in [HKC+94] and [CMKH96] for codes over \( \mathbb{Z}_4 \). We generalise their construction and relate it to generating sets in standard form.

**Proposition 4.14** Let \( s \geq 0 \), \( 0 \leq a_0 < a_1 < \ldots < a_s < a_{s+1} = a \) and let \( L_{a_j} \) for \( j = 0, \ldots, s+1 \) be a partition of \( U \). Then \( C = \{c \in R_n \mid p^{a_j}c(\xi^i) = 0, i_j \in L_{a_j}, j = 0, \ldots, s+1\} \) is a cyclic code with parity check matrix

\[
H = \begin{pmatrix}
H_{a_{s+1}} \\
p^{a_{s+1}} H_{a_s} \\
\vdots \\
p^{a_0} H_{a_0}
\end{pmatrix}
\]

where \( H_{a_j} = \begin{pmatrix}
1 & \xi^{l_{j,1}} & \cdots & \xi^{(n-1)l_{j,1}} \\
\vdots & \vdots & & \vdots \\
1 & \xi^{l_{j,m_j}} & \cdots & \xi^{(n-1)l_{j,m_j}}
\end{pmatrix} \) and \( L_{a_j} = \{l_{j,1}, \ldots, l_{j,m_j}\} \).

**Theorem 4.15** (i) If \( C \) is a cyclic code having \( \{p^{a_0}g_{a_0}, p^{a_1}g_{a_1}, \ldots, p^{a_s}g_{a_s}\} \) as generating set in standard form, then \( C = \{c \in R_n \mid p^{a_j}c(\xi^i) = 0, i_j \in L_{a_j}, j = 0, \ldots, s+1\} \), where \( L_{a_j} = \{i \in U \mid t_{a_j}(\xi^i) = 0\} \), \( t_{a_j} = g_{a_j-1}/g_{a_j} \) with the conventions \( a_{s+1} = a, g_{a_{s+1}} = 1 \) and \( g_{a_j} = X^n - 1 \) for \( j = 1 \).

(ii) Conversely, if \( C = \{c \in R_n \mid p^{a_j}c(\xi^i) = 0, i_j \in L_{a_j}, j = 0, \ldots, s+1\} \) is a cyclic code as in Proposition 4.14, then \( C \) has the generator set in standard form \( \{p^{a_0}t_{a_0}, p^{a_1}t_{a_1}, \ldots, p^{a_{s+1}}t_{a_{s+1}}\} \) where \( t_{a_j} = \prod_{i_j \in L_{a_j}} M_{i_j} \).

**Proof.** (i) Since \( t_{a_j} \mid X^n - 1 \), for \( j = 0, \ldots, s+1 \), by Lemma 4.13(v) we have that \( t_{a_j} = \prod_{i_j \in L_{a_j}} M_{i_j} \).

The \( t_{a_j} \) are pairwise coprime and \( \prod_{j=0}^{s+1} t_{a_j} = X^n - 1 \), so the \( L_{a_j} \) are a partition of \( U \). Put \( D = \{c \in R_n \mid p^{a_j}c(\xi^i) = 0, i_j \in L_{a_j}, j = 0, \ldots, s+1\} \). It is easy to check from the definitions that \( C \subseteq D \).
Now let $c \in D$. Since $c(\xi^{i+1}) = 0$ for all $i+1 \in L_{a+1}$, by Lemma 4.13(iv) we deduce that $t_{a+1}|c$ i.e. $c = t_{a+1}c_{a+1}$ for some $c_{a+1} \in R[X]$. Further, $p^{a-a}t_{a+1}(\xi^i)c_{a+1}(\xi^i) = 0$ for all $i \in L_a$. Since $t_{a+1}(\xi^i) \neq 0$, we deduce $t_{a+1}(\xi^i) \neq 0$ by Lemma 4.13(i), so $t_{a+1}(\xi^i)$ is a unit. Thus $p^{a-a}t_{a+1}(\xi^i)c_{a+1} \mod p^{a-a} = 0$ as in Lemma 2.3. Hence $(t_a \ mod p^{a-a})$ divides $(c_{a+1} \ mod p^{a-a})$ by Lemma 4.13(iv) and (vi), i.e. $c_{a+1} = t_a c_a + p^{a-a}h_a$, for some $c_a, h_a \in R[X]$ and therefore $c = g_{a+1}c_a + p^{a-a}h_a$. Continuing this way we obtain $c = g_{a+1}c_a + \sum p^{a-a}g_a h_a$, for some $h_a \in R[X]$. As $g_a t_a = 0 \mod (X^a - 1)$, it follows that $c = \sum p^{a-a}g_a h_a \in C$.

The proof of part (ii) is similar.

Acknowledgement. The authors gratefully acknowledge financial support from the U.K. Engineering and Physical Sciences Research Council (EPSRC). The second author was supported by EPSRC Grant L07680.

References


