On the structure of linear and cyclic codes over a finite chain ring. *

Graham H. Norton Ana Sălăgean

Algebraic Coding Research Group

Centre for Communications Research

University of Bristol, U.K.

July 19, 2001

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 a Gray map of linear codes over $\mathbb{Z}_4$,

*Research supported by the U.K. Engineering and Physical Sciences Research Council under Grant L07680. Current addresses: Dept. Mathematics, University of Queensland, Brisbane 4072, ghn @maths.uq.edu.au. The second author is now with the Department of Mathematics, Nottingham Trent University, Ana.Salagean@maths.ntu.ac.uk.
Copyright 2000, Springer-Verlag.

see [5] 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 [10]. See also [13]. 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 [7, Chapter 7].

Let R be a finite chain ring, K its residue field, γ a fixed generator of the maximal ideal of R and ν the nilpotency index of γ. The canonical projections $R[X] \to K[X]$ and $R^n \to K^n$ will be denoted by $\overline{}$.

The paper proper begins in Section 3 with more detailed versions of the structure theorems for linear codes given in [2]. We generalise these results to finite chain rings and give new, elementary proofs. To any linear code C over R, we associate the *tower of linear codes over* K

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

where $(C : r)$ denotes the submodule quotient of C by $r \in R$; see Definition 3.3. This tower plays an important role throughout the paper. We construct generator matrices for the codes in this tower given a generator matrix of C. This is then applied to give properties of C and a parity check matrix for C.

We consider cyclic codes in Section 4. Given a cyclic code C over R, we construct a unique set of polynomial generators for C. (A similar set of generators was given in [2] for $R = \mathbb{Z}_{p^a}$ using the Lasker-Noether decomposition theorem.) We relate this set of generators to a generator matrix of C and give the set of generators of the dual of C. As an application of this set of generators, we give a new characterization of cyclic codes in terms of partitions of the set of roots of $X^n - 1$ in R when R is a Galois ring.

Our proofs avoid the non-trivial Commutative Algebra invoked in [2], using instead properties

of the codes $\overline{(C:\gamma^i)}$ and the technique used in [2, Corollary to Theorem 6] for proving that $\mathbb{Z}_{p^a}[X]/(X^n-1)$ is principal. In [6] it is claimed that this technique is incorrect, by giving a 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 [2, *loc. cit.*].

There is a different set of generators which also provides a useful description of properties of a cyclic code; see [11] for codes over $\mathbb{Z}_4$ and [6] for the generalisation to $\mathbb{Z}_{p^a}$. For a discussion of the connection between these two sets of generators, see [6].

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

The structure theorems of this paper have been used to prove results on the Hamming distance of codes over a finite chain ring in [9]. A preliminary version of this paper was presented at the Workshop on Coding and Cryptography in Paris, January 1999.

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 [8].

DEFINITION 2.1 *A finite commutative ring with identity* $1 \neq 0$ *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 γ be a fixed generator of the maximal ideal of a finite chain ring R. Then γ is nilpotent and let ν be its nilpotency index i.e. the smallest positive 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 $1 \neq 0$, γ a fixed generator of the maximal ideal of R, ν the nilpotency index of γ and K the residue field of R.

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

LEMMA 2.2 ([8, P. 340]) *For any $r \in R \setminus \{0\}$ 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 onto K. Denote by $\overline{r}$ 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 ν.

LEMMA 2.4 *Let $V \subseteq R$ be a set of representatives for the equivalence classes of R under congruence modulo γ. (Equivalently, we can define V to be a maximal subset of R with the property that $\overline{r}_1 \neq \overline{r}_2$ 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 $0 \leq j \leq \nu - 1$.

PROOF. (i) We inductively construct $r_0, \ldots, r_{\nu-1} \in V$ such that $r \equiv \sum_{i=0}^{j} r_i \gamma^i \bmod \gamma^{j+1}$ for $j = 0, \ldots, \nu - 1$. Let r_0 be the unique element of V such that $\overline{r}_0 = \overline{r}$. Assuming that $j < \nu - 1$ and that we have constructed $r_0, \ldots, r_j$, we have $r - \sum_{i=0}^{j} r_i \gamma^i = v_{j+1} \gamma^{j+1}$ for some $v_{j+1} \in R$. We put r_{j+1} equal to the element in V such that $\overline{r}_{j+1} = \overline{v}_{j+1}$. Then $r \equiv \sum_{i=0}^{j+1} r_i \gamma^i \bmod \gamma^{j+2}$.

For the unicity, let $r = \sum_{i=0}^{\nu-1} r_i \gamma^i = \sum_{i=0}^{\nu-1} s_i \gamma^i$ with $r_i, s_i \in V$ for $i = 0, \ldots, \nu - 1$. Then $\sum_{i=0}^{\nu-1} (r_i - s_i) \gamma^i = 0$ and using Corollary 2.3 repeatedly we obtain $\overline{r}_i = \overline{s}_i$ for $i = 0, \ldots, \nu - 1$.

Since $r_i, s_i \in V$, this implies $r_i = s_i$ for $i = 0, \ldots, \nu - 1$.

Part (ii) is easy. For part (iii), note that in the representation given by (i) we have $|V| = |K|$ possibilities for each of $r_0, \ldots, r_{\nu-1}$ and that $\sum_{i=0}^{\nu-1} r_i \gamma^i \in \gamma^j R$ if and only if $r_0 = \ldots = r_{j-1} = 0$.

$\square$

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 $\overline{C} = \{\overline{f} \mid f \in C\}$.

We say that a polynomial $f \in R[X]$ is *monic* if its leading coefficient is 1. A polynomial $f \in R[X]$ is a unit if and only if $\overline{f}$ is a unit and f is a zero-divisor if and only if $\overline{f} = 0$, by [8, Theorem XIII.2]. Recall that a non-unit $f \in R[X]$ is called *basic irreducible* if both f and $\overline{f}$ are irreducible. We observe that $R[X]$ is a Noetherian ring only, whereas $K[X]$ is a Euclidean ring, so that for $f \in R[X]$, the consequences of $\overline{f}$ being irreducible are much stronger.

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 $f \in \mathbb{Z}_{p^a}[X]$ 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 [8, Theorem XIII.2].

(ii) Let $f \in \mathbb{Z}_p[X]$ be irreducible and of degree l. Since $\mathbb{Z}_{p^a}$ is a local ring with residue field $\mathbb{Z}_p$, we can find a monic $g \in \mathbb{Z}_{p^a}[X]$ with $\overline{g} = f$. Hence g is irreducible of degree l by part (i). $\square$

For any $l \geq 1$, one can construct a Galois extension ring of $\mathbb{Z}_{p^a}$ as $\mathrm{GR}(p^a, l) = \mathbb{Z}_{p^a}[X]/(f)$ where p is a prime number, $a \geq 1$ and $f \in \mathbb{Z}_{p^a}[X]$ is a monic basic irreducible polynomial of degree l, which exists by Lemma 2.5. The ring $\mathrm{GR}(p^a, l)$ 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, $\mathrm{GF}(p^l)$. For $a \geq b$, there is a natural projection homomorphism (reduction modulo p^b) of $\mathrm{GR}(p^a, l)$ to $\mathrm{GR}(p^b, l)$ with kernel $\mathrm{GR}(p^a, l)p^b$. For any multiple m of l there is an inclusion homomorphism $\mathrm{GR}(p^a, l) \subseteq \mathrm{GR}(p^a, m)$.

A Galois ring $\mathrm{GR}(p^a, l)$ is a finite chain ring with maximal ideal generated by p, the nilpotency index of p is a and the residue field is $\mathrm{GF}(p^l)$. Any finite chain ring is a certain homomorphic image of a polynomial ring $\mathrm{GR}(p^a, l)[X]$, see [8, 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-invertible polynomials (or two non-units) $f, g \in R[X]$ are *coprime* if they generate $R[X]$, i.e. there are $u, v \in R[X]$ such that $fu + gv = 1$. By [8, Theorem XIII.6], any $f \in R[X]$ which is not divisible by γ can be written as $f = uf_1$ where $u \in R[X]$ is a unit and f_1 is monic. We will therefore restrict our attention to monic polynomials.

THEOREM 2.6 (HENSEL LIFTING, [8, 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 $\overline{g} = \prod_{i=1}^{k} f_i$. Then there are $g_1, \ldots, g_k \in R[X]$ monic, pairwise coprime such that $g = \prod_{i=1}^{k} g_i$ and $\overline{g_i} = f_i$.*

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 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 [8, Theorem XIII.11], g factors uniquely as $g = g_1 \cdots g_k$ where the g_i are pairwise coprime, and each g_i is monic and generates a primary ideal. Since $\overline{g}$ is square-free, so are the $\overline{g}_i$. It follows from [8, 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 so each g_i is irreducible by Lemma 2.5(i). $\square$

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 $\overline{h}$ is a unit, I contains a unit if and only if J contains a unit. $\square$

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 onto K to a projection of the free R-module R^n onto K^n. Abusing terminology, we shall refer to an n-tuple in R^n as a "vector".

For any vector $c \in R^n$ we denote the image of c under the projection $R^n \to K^n$ by $\overline{c}$, and for a subset C of R^n, we define $\overline{C} = \{\overline{c} |\ c \in C\}$.

For any constant $r \in R$ and any vector $c \in R^n$ 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 $\{rc |\ c \in C\}$. We will say that a vector is divisible by a constant $r \in R$ if all its entries contain r as a factor. 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 γ. As in Corollary 2.3, if $1 \leq i \leq j \leq \nu$ and $\gamma^i c \in \gamma^j R^n$ then $c \in \gamma^{j-i} R^n$. In particular, if $\gamma^i c = 0$ 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 $\varphi(\gamma^i c) = (c_1 + \gamma^{\nu-i}R, \ldots, c_n + \gamma^{\nu-i}R)$ for any $c = (c_1, \ldots, c_n) \in R^n$. Indeed, φ is an isomorphism. Now $\gamma^i R^n$ is also an $(R/\gamma^{\nu-i}R)$-module (with $(r + \gamma^{\nu-i}R) \circ \gamma^i c = r\gamma^i c$ in the usual way) and it is easy to check that φ 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 $\varphi(\gamma^i c) = (c_1 + \gamma^{\nu-i}R, \ldots, c_n + \gamma^{\nu-i}R)$ for any $c = (c_1, \ldots, c_n) \in R^n$ 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 $R = \mathbb{Z}_{p^a}$, the structure of codes is described in [2, p.22] We will now give more detailed versions of these theorems, generalised to a finite chain ring. We 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 the rows of G span C and none of them can be written as a linear combination of the other rows of G.*

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

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

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

$$A = \begin{pmatrix} A_0 \\ \vdots \\ A_{\nu-1} \end{pmatrix}. \tag{2}$$

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

$\overline{A_i}$'s 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. $\square$

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*

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

over R and its projection to K,

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

For $\mathbb{Z}_4$, the codes $\overline{C} = \overline{(C : \gamma^0)}$ and $\overline{(C : \gamma^1)}$ were introduced in [4] (denoted there as $C^{(1)}$ and $C^{(2)}$). The tower of codes over K will play an important role throughout this paper.

The following result appears in [4, 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 let A be as in (2). Then for $0 \leq i \leq \nu - 1$, $\overline{(C : \gamma^i)}$ has generator matrix*

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

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

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

PROOF. (i) It is easy to check that $\overline{(C:\gamma^i)}$ contains the module spanned by the rows of the given matrix. Let $e \in \overline{(C:\gamma^i)}$ and let $g \in (C:\gamma^i)$ be such that $\overline{g} = e$. As $\gamma^i g \in C$ and G is a generating matrix for C, there are $v_j \in R^{k_j}$ such that

$$\gamma^i g = (v_0, v_0A_{01} + \gamma v_1, \ldots, v_0A_{0,\nu-1} + v_1\gamma A_{1,\nu-1} + \cdots + \gamma^{\nu-1}v_{\nu-1}, v_0A_{0,\nu} + \cdots + \gamma^{\nu-1}v_{\nu-1}A_{\nu-1,\nu}).$$

Also $\gamma^i g$ is divisible by γ^i, so 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 $\gamma^i w_0 A_{01} + \gamma v_1$, hence $v_1 = \gamma^{i-1} w_1$ for some $w_1 \in R^{k_1}$. Continuing, we obtain $v_j = \gamma^{i-j} w_j$ where $w_j \in R^{k_j}$ for $j = 0, \ldots, i$. Therefore $\gamma^i g = \sum_{j=0}^{i} \gamma^i w_j A_j + \sum_{j=i+1}^{\nu-1} v_j \gamma^j A_j$ 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 $e = \overline{g} = \sum_{j=0}^{i} \overline{w_j}\,\overline{A_j}$ i.e. $\overline{(C:\gamma^i)}$ is generated by the required matrix. The rows of this matrix are obviously linearly independent over K, hence $\dim(\overline{(C:\gamma^i)}) = k_0 + \cdots + k_i$.

(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 $\overline{A_i} = L_i$ and define C to be the code with generator matrix

$$\begin{pmatrix} A_0 \\ \gamma A_1 \\ \vdots \\ \gamma^{\nu-1} A_{\nu-1} \end{pmatrix}.$$

Note that the code C is not unique as it depends on the choice of the A_i's. $\square$

THEOREM 3.5 *Let C be a code of length n. 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 written uniquely 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 $k_0 = \dim(\overline{C})$ and $k_i = \dim(\overline{(C:\gamma^i)}) - \dim(\overline{(C:\gamma^{i-1})})$, 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 $enc_G : R^k \to R^n$ defined by $enc_G(v) = vG$ has the image $enc_G(R^k) = C$. 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 $enc_G(v) = (v_0, v_0A_{01} + \gamma v_1, \ldots, v_0A_{0,\nu-1} + v_1\gamma A_{1,\nu-1} + \cdots + \gamma^{\nu-1}v_{\nu-1}, v_0A_{0,\nu} + \cdots + \gamma^{\nu-1}v_{\nu-1}A_{\nu-1,\nu}) = 0$. Then $v_0 = 0$ and the second block of entries becomes γv_1 and has to be 0, hence $v_1 \in \gamma^{\nu-1}R^{k_1}$, 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. □

Proposition 3.2 and the previous theorem justify the following definition:

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

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 $C \subseteq D$ 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 [8, 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:*

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

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

COROLLARY 3.9 *If C is an R-submodule of R^n, then any generator matrix for C has $k(C)$ rows.*

3.2 The dual code

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

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

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

$$H = \begin{pmatrix} B_{0,\nu} & B_{0,\nu-1} & \cdots & B_{0,1} & I_{n-k(C)} \\ \gamma B_{1,\nu} & \gamma B_{1,\nu-1} & \cdots & \gamma I_{k_{\nu-1}(C)} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ \gamma^{\nu-1} B_{\nu-1,a} & \gamma^{\nu-1} I_{k_1(C)} & \cdots & 0 & 0 \end{pmatrix} = \begin{pmatrix} B_0 \\ \gamma B_1 \\ \vdots \\ \gamma^{\nu-1} B_{\nu-1} \end{pmatrix} \tag{3}$$

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

(ii) For $i = 0, \ldots, \nu - 1$, $\overline{(C^\perp : \gamma^i)} = (\overline{(C : \gamma^{\nu-1-i})})^\perp$, $k_0(C^\perp) = n - k(C)$ and $k_i(C^\perp) = k_{\nu-i}(C)$, 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 $HG^{tr} = 0$. Let D be the R-module generated by H. We have $k_0(D) = n - k(C)$, $k_i(D) = k_{\nu-i}(C)$ for $i = 1, \ldots, \nu - 1$ and D is orthogonal to C, hence

$D \subseteq C^\perp$. 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 first prove that $\overline{(C^\perp : \gamma^i)} \perp \overline{(C : \gamma^{\nu-i-1})}$. Let $b \in (C^\perp : \gamma^i)$ and $e \in (C : \gamma^{\nu-i-1})$. Then $\gamma^i b \in C^\perp$ and $\gamma^{\nu-i-1} e \in C$, so $\gamma^{\nu-1} b e^{tr} = 0$ i.e. $\overline{b}\overline{e}^{tr} = 0$. 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 $\overline{(D : \gamma^i)} \subseteq \overline{(C^\perp : \gamma^i)}$ for all i, and so

$$\begin{aligned} n &\geq \dim(\overline{(C : \gamma^{\nu-i-1})}) + \dim(\overline{(C^\perp : \gamma^i)}) \\ &\geq \dim(\overline{(C : \gamma^{\nu-i-1})}) + \dim(\overline{(D : \gamma^i)}) \\ &= k_0(C) + \cdots + k_{\nu-i-1}(C) + k_0(D) + \cdots + k_i(D) \\ &= k_0(C) + \cdots + k_{\nu-i-1}(C) + n - k(C) + k_{\nu-i}(C) + \cdots + k_{\nu-1}(C) = n. \end{aligned}$$

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

(iii) Easy consequence of (ii). □

We associate the matrix

$$B = \begin{pmatrix} B_0 \\ \vdots \\ B_{\nu-1} \end{pmatrix} \tag{4}$$

of Theorem 3.10 to H. As in (2), B is not unique: for example we could choose $B_{i,i+1} = -A^{tr}_{\nu-i-1,\nu-i} + \gamma V$ with V an arbitrary $k_{\nu-i}(C) \times k_{\nu-i-1}(C)$ 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 Lemma 3.4 and the fact that $(\overline{C})^\perp = (\overline{(C : \gamma^0)})^\perp = \overline{(C^\perp : \gamma^{\nu-1})}$. □

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) $\overline{C} = \overline{(C : \gamma)} = \cdots = \overline{(C : \gamma^{\nu-1})}$;

(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 [9, Corollary 3.12].

4 The structure of cyclic codes

The structure of cyclic codes over $\mathbb{Z}_{p^a}$ was presented in [2, 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 $\mathbb{Z}_{p^a}$, as well as its connection to [2], appears in [6].

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 over R 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 γ^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 $\mathrm{id}(f_1, \ldots, f_s)$.

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* $C = \mathrm{id}(S)$ *if* $0 \leq s < \nu$ *and*

(i) $0 \leq a_0 < a_1 < a_2 < \cdots < a_s < \nu$;

(ii) $g_{a_i} \in R[X]$ *is monic for* $i = 0, \ldots, s$;

(iii) $\deg(g_{a_i}) > \deg(g_{a_{i+1}})$ *for* $i = 0, \ldots, s-1$;

(iv) $g_{a_s} | g_{a_{s-1}} | \cdots | g_{a_0} | X^n - 1$.

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 code, then* $\overline{(C : \gamma^{\nu-1})} \neq \{0\}$.

PROOF. Let $c \in C$, $c \neq 0$. By Lemma 2.2, we can write $c = \gamma^i u$ for some i, $0 \leq i \leq \nu - 1$ with i maximal. Since C is an ideal, $\gamma^{\nu-1} u \in C$ i.e. $u \in (C : \gamma^{\nu-1})$ and $0 \neq \overline{u} \in \overline{(C : \gamma^{\nu-1})}$. □

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* $C = \mathrm{id}(S)$. *If* $i < a_0$ *then* $\overline{(C : \gamma^i)} = \{0\}$, *otherwise* $\overline{(C : \gamma^i)} = \mathrm{id}(\overline{g}_{a_j})$ *where j is maximal with the property* $a_j \leq i$.

PROOF. Let $e \in \overline{(C : \gamma^i)}$. There is a $g \in (C : \gamma^i)$ such that $\overline{g} = e$. Since $\gamma^i g \in \mathrm{id}(S)$, we can write $\gamma^i g = \sum_{k=0}^{s} h_{a_k} \gamma^{a_k} g_{a_k}$ for some polynomials h_{a_k}. If $i < a_0$ then $g \equiv \sum_{k=0}^{s} h_{a_k} \gamma^{a_k - i} g_{a_k} \pmod{\gamma^{\nu-i}}$, 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 $\gamma^i g = hg_{a_j} + \sum_{k=j+1}^{s} h_{a_k}\gamma^{a_k}g_{a_k}$ 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 γ^i and g_{a_j} is monic, so h must be divisible by γ^i i.e. $h = \gamma^i t$ for some $t \in R[X]$. Hence $e = \overline{g} = \overline{t}\overline{g}_{a_j}$ i.e. $\overline{(C:\gamma^i)} \subseteq \mathrm{id}(\overline{g}_{a_j})$. 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. [2, 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, $\overline{(C:\gamma^{\nu-1})} \neq \{0\}$ 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 $\{0\} \subset \overline{(C:\gamma^{a_0})} \subset \overline{(C:\gamma^{a_1})} \subset \cdots \subset \overline{(C:\gamma^{a_s})}$ are *strict* and that s is maximal.

Since C is cyclic, the $\overline{(C:\gamma^i)}$'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 $\overline{(C:\gamma^{a_j})}$. 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 $D = \mathrm{id}(S)$.

For proving $D = C$, we first prove that $\gamma^{a_j}g_j \in C$ for $j = 0, 1, \ldots, s$. (The technique is similar to the one used in [2, 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 $\gamma^{a_j}f_{a_j}v_{a_j} = \gamma^{a_j}(g_{a_j} + \gamma h_{a_j})v_{a_j} = \gamma^{a_j+1}h_{a_j}v_{a_j}$ 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 $K[X]$ since $\overline{v}_{a_j} = (X^n - 1)/\overline{g}_{a_j}$ 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 i.e. there are polynomials 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 $\overline{(C:\gamma^i)} = \mathrm{id}(\overline{f}_{a_j}) = \mathrm{id}(\overline{g}_{a_j})$ for $a_j \leq i < a_{j+1}$. On the other hand, by Lemma 4.3(i),

$\overline{(D:\gamma^i)} = \mathrm{id}(\overline{g}_{a_j})$ for $a_j \leq i < a_{j+1}$. Therefore $\overline{(C:\gamma^i)} = \overline{(D:\gamma^i)}$ for $i = 0, \ldots, \nu - 1$, which implies that $k_i(C) = k_i(D)$ and so $C = D$ by Corollary 3.7.

Next we prove the unicity of a generating set in standard form for C. Suppose that we have another generating set in standard form $\{\gamma^{b_0} h_{b_0}, \gamma^{b_1} h_{b_1}, \ldots, \gamma^{b_t} h_{b_t}\}$ for C. By Lemma 4.3 and since $\overline{h}_{b_{j+1}}$ is a strict divisor of $\overline{h}_{b_j}$, the inclusions $\{0\} \subset \overline{(C:\gamma^{b_0})} \subset \overline{(C:\gamma^{b_1})} \subset \cdots \subset \overline{(C:\gamma^{b_t})}$ are strict and t is maximal. Hence $t = s$ and $b_j = a_j$ for $j = 0, \ldots, s$. Also, $\overline{(C:\gamma^{a_j})} = \mathrm{id}(\overline{g}_{a_j}) = \mathrm{id}(\overline{h}_{a_j})$, 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 monic Hensel lift of $\overline{g}_{a_j} = \overline{h}_{a_j}$. $\square$

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 $C = \mathrm{id}(S)$. Then*

(i) if $T = \bigcup_{i=0}^{s} \{\gamma^{a_i} g_{a_i} X^{d_{i-1}-d_i-1}, \ldots, \gamma^{a_i} g_{a_i} X, \gamma^{a_i} g_{a_i}\}$ where $d_i = \deg(g_{a_i})$ 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 $h_j \in (R/R\gamma^{\nu-a_i})[X] \cong (R\gamma^{a_i})[X]$ and $\deg(h_j) < d_{j-1} - d_j$;

(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 is spanned by 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 $g_{a_1} | g_{a_0}$, we can put $g_{a_0}/g_{a_1} = X^{d_0-d_1} + h$ with $\deg(h) < d_0 - d_1$. Then $X^{n-1-d_1} g_{a_1} = X^{n-1-d_0} g_{a_0} + X^{n-1-d_0} h g_{a_1}$ and $X^{n-1-d_1} g_{a_1}$ can be removed from U. Similarly we can remove $X^{n-2-d_1} g_{a_1}, \ldots, X^{d_0-d_1} g_{a_1}$. Using then the fact that $g_{a_2} | g_{a_1}$ we remove $X^{n-1-d_2} g_{a_2}, \ldots, X^{d_1-d_2} g_{a_2}$, and so on. Finally, only the elements of T remain in U. Since the

polynomials in T have distinct degrees, none of them can be written as a linear combination of the others, so that 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 $\deg(h_j) < d_{j-1} - d_j$ and $c = \sum_{j=0}^{s} h_j \gamma^{a_j} g_{a_j} = \sum_{j=0}^{s} (h_j \bmod \gamma^{\nu - a_j}) \gamma^{a_j} g_{a_j}$.

(iii) By Lemma 4.3(i), $\dim(\overline{(C : \gamma^i)}) = 0$ if $i < a_0$, otherwise $\dim(\overline{(C : \gamma^i)}) = n - d_j$ 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). □

COROLLARY 4.6 (CF. [2, COROLLARY TO THEOREM 6]) *The ring R_n is principal.*

PROOF. Let C be an ideal of R_n. As in the proof of [2, Corollary to Theorem 6], one shows that if $\{\gamma^{a_0} g_{a_0}, \gamma^{a_1} g_{a_1}, \ldots, \gamma^{a_s} g_{a_s}\}$ is a generating set in standard form for C then $C = \mathrm{id}(\sum_{j=0}^{s} \gamma^{a_j} g_{a_j})$. □

REMARK 4.7 *In the proof of Theorem 4.4 and Corollary 4.6 we used the technique of [2, Corollary to Theorem 6] for proving that $\mathbb{Z}_{p^a}[X]/(X^n - 1)$ is principal. In [6] it is claimed that the proof of [2,* loc. cit.*] is incorrect, without indicating where the logical mistake is. Instead, [6, Example 3.1] is given, for which it is claimed that the single generator constructed by [2,* loc. cit.*] fails to generate a certain element of the ideal. We will show that this generator does in fact generate that particular element, so the counterexample is incorrect.*

In $\mathbb{Z}_8[X]$, $X^7 - 1 = g_1 g_2 g_3$ where $g_1 = X - 1$, $g_2 = X^3 + 6X^2 + 5X + 7$ and $g_3 = X^3 + 3X^2 + 2X + 7$. Let $C = \mathrm{id}(f_0, 2f_1, 2^2 f_2)$ where $f_0 = g_2$, $f_1 = f_2 = 1$. By [2, loc. cit.*], $g = f_0 + 2f_1 + 2^2 f_2 = g_2 + 6$ generates C. Now, it is stated in [6, Example 3.1], that g does not generate C since $f \notin \mathrm{id}(g)$ where $f = g_2 + 2g_1 g_3 \in C$. 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 [2,* loc. cit.*], we show that $4 \in \mathrm{id}(g)$. We have $3g_1 g_3 g = 3g_1 g_3 (g_2 + 6) = 2g_1 g_3 \pmod{X^7 - 1}$ and $4g = 4g_2$. Since $\overline{g_2}$ and $\overline{g_1 g_3}$ are coprime,*

there are $u, v \in R[X]$ *such that* $g_2u + g_1g_3v = 1$, *by Lemma 2.8. Hence* $4 = 4g_2u + 4g_1g_3v = 4gu + 6g_1g_3gv = g(4u + 6g_1g_3v)$ *and consequently* $f = g(2X + 1 + (4u + 6g_1g_3v)(X^2 + 1)) \in \mathrm{id}(g)$.

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 $u \cdot c$ denotes the dot product of $u \in C^\perp$ and $c \in C$, then $\pi(u) \cdot c = \pi(u) \cdot \pi(\pi^{-1}(c)) = u \cdot \pi^{-1}(c) = 0$ and so $C^\perp$ is also 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 f_0 is a unit, we define $f^\#$ to be f^* divided by f_0. 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* $\{\gamma^{a_0} g_{a_0}, \gamma^{a_1} g_{a_1}, \ldots, \gamma^{a_s} g_{a_s}\}$ *a generating set in standard form. Put* $a_{s+1} = \nu$ *and* $g_{a_{-1}} = X^n - 1$. *For* $j = 0, \ldots, s+1$, *let* $b_j = \nu - a_{s+1-j}$ *and* $h_{b_j} = ((X^n - 1)/g_{a_{s-j}})^\#$. *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 $D = \mathrm{id}(S)$. 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 $k_i(D) = \deg(h_{b_{j-1}}) - \deg(h_{b_j})$ if $i = b_j$ for some j and $k_i(D) = 0$ otherwise, which the reader may check is $k_{\nu-i}(C)$. □

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 [2]. See also [12].

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* $\mathrm{id}(g)$ *where g is the Hensel lift of f is called the* Hensel lift *of the cyclic code* $\mathrm{id}(f)$.

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 $C = \mathrm{id}(g)$ 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 [1, p. 303]).*

4.4 Cyclic codes defined by roots of unity

In this subsection, we give an alternative definition of cyclic codes (in terms of the zeroes of their codewords in a suitable extension ring) when R is a Galois ring.

Let $R = \mathrm{GR}(p^a, l)$ and let $m \in \mathbb{N}$ be such that $l|m$ and $n|p^m - 1$. The ring $\mathrm{GR}(p^a, m)$ is an extension of R in which $X^n - 1$ has n roots. By [8, Lemma XV.1], we can lift uniquely a primitive root of $X^n - 1$ from $\mathrm{GF}(p^m)$ to a root ξ of $X^n - 1$ in $\mathrm{GR}(p^a, m)$. By [10, Theorem 2.9], ξ 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 $\overline{\xi}$ over K*, 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 $i = 0, \ldots, n-1$, $\{j \in \{0, \ldots, n-1\} \mid M_i(\xi^j) = 0\} = \{j \in \{0, \ldots, n-1\} \mid m_i(\overline{\xi}^j) = 0\}$.

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

(iii) U is a set of representatives for the conjugacy classes of ξ over R.

(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 $f = \prod_{i \in L} M_i$ iff $L = \{i \in U | f(\xi^i) = 0\}$.

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

PROOF. (i) The roots of m_i are powers of $\overline{\xi}$ and the roots of M_i are powers of ξ. If $M_i(\xi^j) = 0$ then of course $\overline{M_i(\xi^j)} = m_i(\overline{\xi}^j) = 0$. Conversely, let $\overline{\xi}^j$ be a root of m_i. Since m_i has no multiple roots, by [8], the root $\overline{\xi^j}$ of m_i can be uniquely lifted to a root of M_i, say ξ^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 induct on v. First consider $v = 1$ and assume that f is not divisible by M_{i_1}. Then dividing f by M_{i_1} we obtain $f = qM_{i_1} + p^k r$ with $q, r \in R[X]$, $r \neq 0$, $\deg(r) < \deg(M_{i_1})$, $0 \leq k \leq a-1$ and p does not divide r. Since $p^k r(\xi^{i_1}) = 0$, we obtain $\overline{r}(\overline{\xi}^{i_1}) = 0$ (applying Lemma 2.3 if $k > 0$). This means that $\overline{r}$ is divisible by m_{i_1}, the minimal polynomial of $\overline{\xi}^{i_1}$, which is impossible as $\deg(\overline{r}) \leq \deg(r) < \deg(M_{i_1}) = \deg(m_{i_1})$ since M_{i_1} is monic.

Next, assume $v \geq 2$. As above, there is some $g \in R[X]$ such that $f = M_{i_v} g$. From the definition of U, it follows that for $j = 1, \ldots, v-1$, $\overline{M_{i_v}(\xi^{i_j})} = m_{i_v}(\overline{\xi}^{i_j}) \neq 0$, and so $M_{i_v}(\xi^{i_j})$ is a unit. Thus for $j = 1, \ldots, v-1$, $f(\xi^{i_j}) = 0$ implies that $g(\xi^{i_j}) = 0$. Applying the inductive hypothesis, $\prod_{j=1}^{v-1} M_{i_j} | g$.

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

(vi) Since M_i mod p^k is obtained by Hensel lifting of m_i to $\mathrm{GR}(p^k, l)[X]$, we can apply (ii) in the ring $\mathrm{GR}(p^k, l)[X]$. $\square$

Any set of roots $\{\xi^{i_1}, \ldots, \xi^{i_k}\}$ defines a cyclic code $\{c \in R_n |\ c(\xi^{i_j}) = 0, j = 1, \ldots, k\}$. The generator polynomial of this code is the product of those minimal polynomials $M_{i_1}, \ldots, M_{i_k}$ which are distinct, and a parity check matrix is

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

This construction is described in [12]. The more general case of codes with several generator polynomials appears implicitly in [3] and [5] for codes over $\mathbb{Z}_4$.

We now generalise this construction to cyclic codes over $R = \mathrm{GR}(p^a, l)$ using the generating set in standard form of a cyclic code.

Recall that U is a set of representatives for the conjugacy classes of $\overline{\xi}$ over K. Lemma 4.13 shows that U is a also set of representatives for the conjugacy classes of ξ over R.

THEOREM 4.14 *Let C be an R-submodule of R^n. Then C is a cyclic code if and only if there are integers $0 \leq a_0 < \cdots < a_s < a_{s+1} = a$ and a partition $\{L_{a_j} |\ j = 0, \ldots, s+1\}$ of U with*

$$C = \{c \in R_n |\ p^{a-a_j} c(\xi^{i_j}) = 0, i_j \in L_{a_j}, j = 0, \ldots, s+1\}.$$

PROOF. Let C be a cyclic code. By Theorem 4.4, C has a generating set in standard form, $\{p^{a_0} g_{a_0}, p^{a_1} g_{a_1}, \ldots, p^{a_s} g_{a_s}\}$ say. We adopt the conventions $g_{a_{-1}} = X^n - 1$ and $g_{a_{s+1}} = 1$. For $j = 0, \ldots, s+1$, we define $t_{a_j} = g_{a_{j-1}}/g_{a_j}$ and $L_{a_j} = \{i \in U | t_{a_j}(\xi^i) = 0\}$. Now Lemma 4.13(v) implies that $t_{a_j} = \prod_{i_j \in L_{a_j}} M_{i_j}$ since $t_{a_j} | X^n - 1$ for $j = 0, \ldots, s+1$. Also, the construction of the t_{a_j} gives $X^n - 1 = \prod_{j=0}^{s+1} t_{a_j}$, so that the t_{a_j} are pairwise coprime and the L_{a_j} form a partition of U.

Now let $D = \{c \in R_n |\ p^{a-a_j} c(\xi^{i_j}) = 0, i_j \in L_{a_j}, j = 0, \ldots, s+1\}$. We will show that $C = D$. It is easy to check from the definitions that $C \subseteq D$. Suppose that $c \in D$. Since $c(\xi^{i_{s+1}}) = 0$ for all $i_{s+1} \in L_{a_{s+1}}$, Lemma 4.13(iv) implies that $t_{a_{s+1}} | c$ i.e. $c = t_{a_{s+1}} c_{a_{s+1}}$ for some $c_{a_{s+1}} \in R[X]$. Further, $p^{a-a_s} t_{a_{s+1}}(\xi^{i_s}) c_{a_{s+1}}(\xi^{i_s}) = 0$ for all $i_s \in L_{a_s}$. Since $t_{a_{s+1}}(\xi^{i_s}) \neq 0$, we deduce that $\overline{t}_{a_{s+1}}(\overline{\xi}^{i_s}) \neq 0$ from Lemma 4.13(i), so $t_{a_{s+1}}(\xi^{i_s})$ is a unit. Thus $p^{a-a_s} c_{a_{s+1}}(\xi^{i_s}) = 0$ for all $i_s \in L_{a_s}$ which implies that $c_{a_{s+1}}(\xi^{i_s}) \bmod p^{a_s} = 0$ as in Lemma 2.3. Hence $(t_{a_s} \bmod p^{a_s})$ divides $(c_{a_{s+1}} \bmod p^{a_s})$ by Lemma 4.13(iv) and (vi), i.e. $c_{a_{s+1}} = t_{a_s} c_{a_s} + p^{a_s} h_{a_s}$ for some $c_{a_s}, h_{a_s} \in R[X]$. Therefore $c = g_{a_{s-1}} c_{a_s} + p^{a_s} g_{a_s} h_{a_s}$. Continuing in this way, we obtain $c = g_{a_0} t_{a_0} c_{a_0} + \sum_{j=0}^{s} p^{a_j} g_{a_j} h_{a_j}$ for some $h_{a_j} \in R[X]$. As $g_{a_0} t_{a_0} = 0 \bmod (X^n - 1)$, it follows that $c = \sum_{j=0}^{s} p^{a_j} g_{a_j} h_{a_j} \in C$.

Conversely, suppose we have integers $0 \leq a_0 < \cdots < a_s < a_{s+1} = a$ and a partition $\{L_{a_j} |\ j = 0, \ldots, s+1\}$ of U. Put $C = \{c \in R_n |\ p^{a-a_j} c(\xi^{i_j}) = 0, i_j \in L_{a_j}, j = 0, \ldots, s+1\}$. It is easy to check that C is a cyclic code. In fact, we can give the generator set in standard form of C explicitly. If we set

$$t_{a_j} = \prod_{i_j \in L_{a_j}} M_{i_j} \text{ and } g_{a_{j-1}} = \prod_{k=j}^{s+1} t_{a_k}$$

for $j = 1, \ldots, s+1$, then as in the first part, $C = \mathrm{id}(\{p^{a_0} g_{a_0}, p^{a_1} g_{a_1}, \ldots, p^{a_s} g_{a_s}\})$. □

The proof of the last result is straightforward and omitted.

PROPOSITION 4.15 *If C is a cyclic code as in Theorem 4.14 and $L_{a_j} = \{l_{j,1}, \ldots, l_{j,m_j}\}$ for $j = 0, \ldots, s+1$, then a parity check matrix for C is given by*

$$H = \begin{pmatrix} H_{a_{s+1}} \\ p^{a-a_s} H_{a_s} \\ \vdots \\ p^{a-a_0} H_{a_0} \end{pmatrix} \quad \textit{where} \quad H_{a_j} = \begin{pmatrix} 1 & \xi^{l_{j,1}} & \ldots & \xi^{(n-1)l_{j,1}} \\ \vdots & \vdots & & \vdots \\ 1 & \xi^{l_{j,m_j}} & \ldots & \xi^{(n-1)l_{j,m_j}} \end{pmatrix}.$$

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. We thank the referee for useful comments and suggestions.

References

[1] E. R. Berlekamp. *Algebraic Coding Theory.* Series in Systems Science. McGraw Hill, New York-Toronto, 1968.

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

[3] A.R. Calderbank, G. McGuire, P.V. Kumar, and T. Helleseth. Cyclic codes over $\mathbb{Z}_4$, locator polynomials, and Newton's identities. *IEEE Trans. Inform. Theory*, 42(1):217–226, 1996.

[4] J. H. Conway and N. J. A. Sloane. Self-dual codes over the integers modulo 4. *J. Combinat. Theory*, A 62:30–45, 1993.

[5] 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.

[6] 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.

[7] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-correcting Codes.* North Holland, Amsterdam, 1977.

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

[9] G. H. Norton and A. Sălăgean. On the Hamming distance of linear codes over finite chain rings. *IEEE Trans. Inform. Theory*, 1999. To Appear.

[10] G. H. Norton and A. Sălăgean. On the key equation over a commutative ring. *Designs, Codes and Cryptography*, 1999. In Press.

[11] V. S. Pless and Z. Qian. Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$. *IEEE Trans. Inform. Theory.*, 42(5):1594–1600, 1996.

[12] P. Shankar. On BCH codes over arbitrary integer rings. *IEEE Trans. Inform. Theory*, 25(4):480–483, 1979.

[13] J.A. Wood. Duality for modules over finite rings and applications to coding theory. *American J. Mathematics*, 1999. To appear.