G-codes over Formal Power Series Rings and Finite Chain Rings

Steven T. Dougherty
Department of Mathematics
University of Scranton
Scranton, PA 18510
USA
Joe Gildea, Adrian Korban
Department of Mathematical and Physical Sciences
Thornton Science Park, Pool Ln
Chester CH2 4NU
England

October 14, 2019

Abstract

In this work, we define G-codes over the infinite ring R_∞ as ideals in the group ring $R_\infty G$. We show that the dual of a G-code is again a G-code in this setting. We study the projections and lifts of G-codes over the finite chain rings and over the formal power series rings respectively. We extend known results of constructing γ-adic codes over R_∞ to γ-adic G-codes over the same ring. We also study G-codes over principal ideal rings.

Key Words: G-codes, finite chain rings, formal power series rings, γ-adic codes.

1 Introduction

One of the most widely studied families of codes is the family of cyclic codes. One reason for this, is that cyclic codes over a Frobenius ring R have an algebraic description as ideals in the polynomial ring $R[x]/\langle x^n - 1\rangle$ where n is the length of the code. To classify cyclic codes, it is simply a matter of finding ideals in this ring via a factorization of $x^n - 1$ over R. Another very important reason is that cyclic codes are held invariant by the action of the cyclic shift. This, in turn, means that their automorphism group must contain the cyclic group of order n as a subgroup. This gives a structure to these codes which is highly useful in applications both in and out of mathematics.

Cyclic codes were first studied over finite fields and later were studied over Frobenius rings, especially for chain rings and principal ideal rings. In [1], Calderbank and Sloane made a more unified approach to studying cyclic codes over the rings $\mathbb{Z}_{p^e}$ by studying cyclic codes over over the p-adic numbers. This approach implied results for cyclic codes over $\mathbb{Z}_{p^e}$ for all $e > 0$ by considering these rings as projections of the p-adic ring. This work has been generalized to study codes over arbitrary chain rings by S.T. Dougherty and Y.H. Park in [6]. In [4], γ-adic codes are defined over a formal power series ring which are then used to study codes over finite chain rings. Also, cyclic codes over formal power series rings are studied in [5].

Recently, G-codes have been defined as codes that are ideals in the group ring RG, where R is a finite commutative Frobenius ring and G is a finite group of order n. This gives an alternative view of cyclic codes as ideals in the group ring RC_n where C_n is the cyclic group of order n. Moreover, it generalizes the notion of cyclic codes by considering codes whose automorphism group contains the arbitrary group G as a subgroup. In [3], parallels between cyclic codes and G-codes are drawn. For example, it is shown that the dual of a G-code is also a G-code, as in the case of cyclic codes, namely that the dual of a cyclic codes is also a cyclic code. Moreover, constructions of these codes are given as well as algebraic properties of their structure.

In this work, we generalize these ideas to study G-codes in a very broad sense. Namely, we study G-codes over formal power series rings and use that canonical projection to study G-codes over finite chain rings. This allows for a construction of infinite families of G-codes from a single code and helps to determine their minimum weight and structural properties.

2 Preliminaries

We begin by recalling some standard definitions from the theory of rings and the theory of codes.

2.1 Codes

We shall give the definitions for codes over rings. For a complete description of algebraic coding theory in this setting, see [2]. Let R be a commutative ring. Note that we are not necessarily assuming that the ring is finite. A code of length n over R is a subset of R^n and a code is linear if it is a submodule of the ambient space R^n. We assume that all finite rings we use as alphabets are Frobenius, where a Frobenius ring is characterized by the following. Let $\widehat{R}$ be the character module of the ring R. For a finite ring R the following are equivalent:

- R is a Frobenius ring.
- As a left module, $\widehat{R} \cong {}_RR$.
- As a right module, $\widehat{R} \cong R_R$.

The *Hamming weight* of a vector is the number of non-zero coordinates in that vector and the minimum weight of a code is the smallest weight of all non-zero vectors in the code.

We define the standard inner-product on the ambient space, namely

$$[\mathbf{v}, \mathbf{w}] = \sum v_i w_i.$$

We define the orthogonal with respect to this inner-product as:

$$\mathcal{C}^\perp = \{\mathbf{v} \in R^n \mid [\mathbf{v}, \mathbf{w}] = 0, \forall \mathbf{w} \in \mathcal{C}\}.$$

The code $\mathcal{C}^\perp$ is linear, whether or not $\mathcal{C}$ is. If R is a finite Frobenius ring, then we have that $(\mathcal{C}^\perp)^\perp = \mathcal{C}$ for all linear codes $\mathcal{C}$ over R. However, if R is infinite this is not always true, which prompts the following definition.

Definition 1. *A linear code $\mathcal{C}$ over an infinite ring R is called basic if $\mathcal{C} = (\mathcal{C}^\perp)^\perp$.*

Not all linear codes are basic. For example, consider the code over the p-adic integers of length 2 given by $\mathcal{C} = \langle (p, p) \rangle$. Here $\mathcal{C}^\perp = \langle (1, -1) \rangle$. However, $\langle (1, -1) \rangle^\perp = \langle (1, 1) \rangle$ which strictly contains the code $\mathcal{C}$. Therefore, this code is not basic.

2.2 Finite Chain Rings and Formal Power Series Rings

We recall the definitions and properties of a finite chain ring R and the formal power series ring R_∞. We refer the reader to [4] and [5] for details and further explanations. In this paper, we assume that all rings have a multiplicative identity and that all rings are commutative.

A ring is called a *chain ring* if its ideals are linearly ordered by inclusion. In particular, this means that any finite chain ring has a unique maximal ideal. Let R be a finite chain ring. Denote the unique maximal ideal of R by $\mathfrak{m}$, and let $\tilde{\gamma}$ be the generator of the unique maximal ideal $\mathfrak{m}$. This gives that $\mathfrak{m} = \langle\tilde{\gamma}\rangle = R\tilde{\gamma}$, where $R\tilde{\gamma} = \langle\tilde{\gamma}\rangle = \{\beta\tilde{\gamma} \mid \beta \in R\}$. We have the following chain of ideals:

$$R = \langle\tilde{\gamma}^0\rangle \supseteq \langle\tilde{\gamma}^1\rangle \supseteq \cdots \supseteq \langle\tilde{\gamma}^i\rangle \supseteq \cdots . \tag{1}$$

The chain in (1) can not be infinite, since R is finite. Therefore, there exists i such that $\langle\tilde{\gamma}^i\rangle = \{0\}$. Let e be the minimal number such that $\langle\tilde{\gamma}^e\rangle = \{0\}$. The number e is called the nilpotency index of $\tilde{\gamma}$. This gives that for a finite chain ring we have the following:

$$R = \langle\tilde{\gamma}^0\rangle \supseteq \langle\tilde{\gamma}^1\rangle \supseteq \cdots \supseteq \langle\tilde{\gamma}^e\rangle. \tag{2}$$

If the ring R is infinite then the chain in Equation 1 is also infinite. Consider, for example, the infinite chain in the p-adic integers:

$$\langle 1\rangle \supseteq \langle p\rangle \supseteq \langle p^2\rangle \supseteq \langle p^3\rangle \cdots . \tag{3}$$

Let $R^\times$ denote the multiplicative group of all units in the ring R. Let $\mathbb{F} = R/\mathfrak{m} = R/\langle\tilde{\gamma}\rangle$ be the residue field with characteristic p, where p is a prime number, then $|\mathbb{F}| = q = p^r$ for some integers q and r. We know that $|\mathbb{F}^\times| = p^r - 1$. We now state two well-known lemmas for which the proofs can be found in [10].

Lemma 2.1. *For any $0 \neq r \in R$ there is a unique integer i, $0 \leq i < e$ such that $r = \mu\tilde{\gamma}^i$, with μ a unit. The unit μ is unique modulo $\tilde{\gamma}^{e-i}$.*

Lemma 2.2. *Let R be a finite chain ring with maximal ideal $\mathfrak{m} = \langle\tilde{\gamma}\rangle$, where $\tilde{\gamma}$ is a generator of $\mathfrak{m}$ with nilpotency index e. Let $V \subseteq R$ be a set of representatives for the equivalence classes of R under congruence modulo $\tilde{\gamma}$. Then*

(i) for all $r \in R$ there are unique $r_0, \cdots, r_{e-1} \in V$ such that $r = \sum_{i=0}^{e-1} r_i\tilde{\gamma}^i$;

(ii) $|V| = |\mathbb{F}|$;

(iii) $|\langle\tilde{\gamma}^j\rangle| = |\mathbb{F}|^{r-j}$ for $0 \leq j \leq e-1$.

From Lemma 2.2, we know that any element $\tilde{a}$ of R can be written uniquely as

$$\tilde{a} = a_0 + a_1\tilde{\gamma} + \cdots + a_{e-1}\tilde{\gamma}^{e-1},$$

where the a_i can be viewed as elements in the field $\mathbb{F}$.

In the next definitions, which can be found in [4], γ will indicate the generator of the ideal of a chain ring, not necessarily the maximal ideal.

Definition 2. *The ring R_∞ is defined as a formal power series ring:*

$$R_\infty = \mathbb{F}[[\gamma]] = \{\sum_{l=0}^{\infty} a_l\gamma^l | a_l \in \mathbb{F}\}.$$

Let i be an arbitrary positive integer. The rings R_i are defined as follows:

$$R_i = \{a_0 + a_1\gamma + \cdots + a_{i-1}\gamma^{i-1} | a_i \in \mathbb{F}\},$$

where $\gamma^{i-1} \neq 0$, but $\gamma^i = 0$ in R_i. If i is finite or infinite then the operations over R_i are defined as follows:

$$\sum_{l=0}^{i-1} a_l\gamma^l + \sum_{l=0}^{i-1} b_l\gamma^l = \sum_{l=0}^{i-1}(a_l + b_l)\gamma^l \tag{4}$$

$$\sum_{l=0}^{i-1} a_l\gamma^l \cdot \sum_{l'=0}^{i-1} b_{l'}\gamma^l = \sum_{s=0}^{i-1}(\sum_{l+l'=s} a_l b_{l'})\gamma^s. \tag{5}$$

We note that if $i = 1$ then $R_1 = \mathbb{F}$ and if $i = e$ then $R_e \cong R$.

The following results can be found in [4].

1. The ring R_i is a chain ring with the maximal ideal $\langle\gamma\rangle$ for all $i < \infty$.
2. The multiplicative group $R_\infty^\times = \{\sum_{j=0}^{\infty} a_j\gamma^j | a_0 \neq 0\}$.
3. The ring R_∞ is a principal ideal domain.

We note that the ring R_∞ is an infinite ring whereas each R_i is a finite ring.

The fact that the ring R_∞ is a principal ideal domain makes the situation quite different than it is for codes over finite rings R_i. For example, assume $i > 1$ so that R_i is not a field. Then the ideal in R_i generated by γ is a non-trivial code $\mathcal{C}$ of length 1, where $\mathcal{C}^\perp = \langle\gamma^{i-1}\rangle$. Note here that $(\mathcal{C}^\perp)^\perp = \mathcal{C}$. However, the ideal in R_∞ generated by γ is a non-trivial code $\mathcal{C}$ of length 1, and its orthogonal is $\{0\}$ as the ring is a domain. But, $\{0\}^\perp = R_\infty$. In other words, while there are non-trivial codes of length 1 corresponding to ideals in the rings, their orthogonals act quite differently than they do in the finite ring since there are no zero divisors.

It is well-known that the generator matrix for a code $\mathcal{C}$ over a finite chain ring R_i, where $i < \infty$ is permutation equivalent to a matrix of the following form:

$$G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & & & A_{0,e} \\ & \gamma I_{k_1} & \gamma A_{1,2} & \gamma A_{1,3} & & & \gamma A_{1,e} \\ & & \gamma^2 I_{k_2} & \gamma^2 A_{2,3} & & & \gamma^2 A_{2,e} \\ & & & \ddots & \ddots & & \\ & & & & \ddots & \ddots & \\ & & & & & \gamma^{e-1} I_{k_{e-1}} & \gamma^{e-1} A_{e-1,e} \end{pmatrix}, \tag{6}$$

where e is the nilpotency index of γ. This matrix G is called the standard generator matrix of the code $\mathcal{C}$. In this case, the code $\mathcal{C}$ is said to have type

$$1^{k_0}\gamma^{k_1}(\gamma^2)^{k_2}\ldots(\gamma^{e-1})^{k_{e-1}}. \tag{7}$$

For linear codes over R_∞, the situation is a little different. Let $\mathcal{C}$ be a finitely generated linear code over R_∞. Then the generator matrix of code $\mathcal{C}$ is permutation equivalent to the following standard form generator matrix (see [4] for more details).

Let $\mathcal{C}$ be a finitely generated, nonzero linear code over R_∞ of length n, then any generator matrix of $\mathcal{C}$ is permutation equivalent to a matrix of the following form:

$$G = \begin{pmatrix} \gamma^{m_0}I_{k_0} & \gamma^{m_0}A_{0,1} & \gamma^{m_0}A_{0,2} & \gamma^{m_0}A_{0,3} & & & \gamma^{m_0}A_{0,r} \\ & \gamma^{m_1}I_{k_1} & \gamma^{m_1}A_{1,2} & \gamma^{m_1}A_{1,3} & & & \gamma^{m_1}A_{1,r} \\ & & \gamma^{m_2}I_{k_2} & \gamma^{m_2}A_{2,3} & & & \gamma^{m_2}A_{2,r} \\ & & & \ddots & \ddots & & \\ & & & & \ddots & \ddots & \\ & & & & & \gamma^{m_{r-1}}I_{k_{r-1}} & \gamma^{m_{r-1}}A_{r-1,r} \end{pmatrix}, \tag{8}$$

where $0 \leq m_0 < m_1 < \cdots < m_{r-1}$ for some integer r. The column blocks have sizes $k_0, k_1, \ldots, k_r$ and k_i are nonnegative integers adding to n.

Definition 3. *A code $\mathcal{C}$ with generator matrix of the form given in Equation 8 is said to be of type*

$$(\gamma^{m_0})^{k_0}(\gamma^{m_1})^{k_1}\ldots(\gamma^{m_{r-1}})^{k_{r-1}},$$

where $k = k_0 + k_1 + \cdots + k_{r-1}$ is called its rank and $k_r = n - k$.

A code $\mathcal{C}$ of length n with rank k over R_∞ is called a γ-*adic* $[n, k]$ code. We call k the dimension of $\mathcal{C}$ and denote the dimension by dim $\mathcal{C} = k$.

Let i, j be two integers with $i \leq j$, we define a map

$$\Psi_i^j : R_j \to R_i, \tag{9}$$

$$\sum_{l=0}^{j-1} a_l\gamma^l \mapsto \sum_{l=0}^{i-1} a_l\gamma^l. \tag{10}$$

If we replace R_j with R_∞ then we obtain a map Ψ_i^∞. For convenience, we denote it by Ψ_i. Since both, Ψ_i^j and Ψ_i are projection maps, it is easy to show that Ψ_i^j and Ψ_i are ring homomorphisms. Let a, b be two arbitrary elements in R_j. It is easy to get that

$$\Psi_i^j(a+b) = \Psi_i^j(a) + \Psi_i^j(b),\ \Psi_i^j(ab) = \Psi_i^j(a)\Psi_i^j(b). \tag{11}$$

If $a, b \in R_\infty$, we have that

$$\Psi_i(a+b) = \Psi_i(a) + \Psi_i(b),\ \Psi_i(ab) = \Psi_i(a)\Psi_i(b). \tag{12}$$

Note that the map Ψ_i^j and Ψ_i can be extended naturally from R_j^n to R_i^n and R_∞^n to R_i^n.

The construction method above gives a chain of rings where R_i is a finite ring for all finite i and R_∞ is an infinite principal ideal domain. This gives the following diagram:

$$\begin{tikzcd}
 & & R \arrow[d, equal] & & & \mathbb{F} \arrow[d, equal] \\
R_\infty \arrow[r] & \cdots \arrow[r] & R_e \arrow[r] & R_{e-1} \arrow[r] & \cdots \arrow[r] & R_1
\end{tikzcd}$$

We note that in the above diagram, R is a finite chain ring with maximal ideal $\mathfrak{m} = \langle \tilde{\gamma} \rangle$, where $\tilde{\gamma}$ is a generator of $\mathfrak{m}$ with nilpotency index e.

2.3 G-codes

We begin by defining a circulant matrix, a reverse circulant matrix and a block circulant matrix before we introduce group rings.

Definition 4. *1. A circulant matrix over a ring R is a square $n \times n$ matrix, which takes the form*

$$circ(a_1, a_2, \dots, a_n) = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_n & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \dots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & a_4 & \dots & a_1 \end{pmatrix}$$

where $a_i \in R$.

2. A reverse circulant matrix over a ring R is a square $n \times n$ matrix, which takes the form

$$rcirc(a_1, a_2, \dots, a_n) = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_2 & a_3 & a_4 & \dots & a_1 \\ a_3 & a_4 & a_5 & \dots & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n & a_1 & a_2 & \dots & a_{n-1} \end{pmatrix}$$

where $a_i \in R$.

3. A block circulant matrix over a ring R is a square $kn \times kn$ matrix, which takes the form

$$CIRC(A_1, A_2, \dots, A_n) = \begin{pmatrix} A_1 & A_2 & A_3 & \dots & A_n \\ A_n & A_1 & A_2 & \dots & A_{n-1} \\ A_{n-1} & A_n & A_1 & \dots & A_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_2 & A_3 & A_4 & \dots & A_1 \end{pmatrix}$$

where each A_i is a $k \times k$ matrix over R.

We shall now give the necessary definitions for group rings. Let G be a finite group of order n and let R be a ring, then the group ring RG consists of $\sum_{i=1}^{n} \alpha_i g_i$, $\alpha_i \in R$, $g_i \in G$.

Addition in the group ring is done by coordinate addition, namely

$$\sum_{i=1}^{n} \alpha_i g_i + \sum_{i=1}^{n} \beta_i g_i = \sum_{i=1}^{n} (\alpha_i + \beta_i) g_i. \tag{13}$$

The product of two elements in a group ring is given by

$$(\sum_{i=1}^{n} \alpha_i g_i)(\sum_{j=1}^{n} \beta_j g_j) = \sum_{i,j} \alpha_i \beta_j g_i g_j. \tag{14}$$

It follows that the coefficient of g_k in the product is $\sum_{g_i g_j = g_k} \alpha_i \beta_j$.

The following construction, first given by Hurly in [8], produces codes in R^n from elements in the group ring RG. Let R be a ring and let $G = \{g_1, g_2, \dots, g_n\}$ be a group of order n. Let $v = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \cdots + \alpha_{g_n} g_n \in RG$. Define the matrix $\sigma(v) \in M_n(R)$ to be

$$\sigma(v) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \alpha_{g_1^{-1}g_3} & \cdots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \alpha_{g_2^{-1}g_3} & \cdots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \alpha_{g_n^{-1}g_3} & \cdots & \alpha_{g_n^{-1}g_n} \end{pmatrix}. \tag{15}$$

We note that the elements $g_1^{-1}, g_2^{-1}, \dots, g_n^{-1}$ are simply the elements of the group G in a given order. For a given $v \in RG$, the code $C(v)$ is defined as follows:

$$\mathcal{C}(v) = \langle \sigma(v) \rangle. \tag{16}$$

Therefore, the code is formed by taking the row space of $\sigma(v)$ over the ring R. In [3], it is shown that such codes are ideals in the group ring RG, and are held invariant by the action of the elements of G. Such codes are referred to as G-codes. We note that these codes necessarily have the group G as a subgroup of their automorphism group. Namely, there may be other automorphism of the code but the code must be held invariant by the actions of the group G on the coordinates of the code. It is precisely this property that makes these codes interesting. For example, many classical constructions of codes force the code to have a certain automorphism group simply by the form of their generator matrix. Consider how many self-dual codes are generated by matrices of the form $(I \mid M)$ where M is a circulant matrix. This construction means that self-dual codes formed in this manner will have a certain form to its automorphism group, see [3] for a complete description. Then constructing self-dual codes by the group ring construction can give self-dual codes with different automorphism groups thus enabling the discovery of self-dual codes that would not be found using the classical techniques. Hence, part of the motivation for using this technique is to discover codes which the usual techniques fail to produce.

In previous work relating group rings and codes, it has always been assumed that the ring is finite. We shall consider here group rings with the infinite ring R_∞. Of course, the theory of group rings always allowed for the study of infinite rings.

3 G-codes and Ideals in the Group Ring $R_\infty G$

We shall extend the results from [3], where it is shown that the G-codes are ideals in RG and that the dual of a G-code is also a G-code in RG when R was a finite Frobenius ring. Here, we extend the results to $R_\infty G$, where G is an arbitrary finite group. The proofs are very similar to the ones in [3], with the difference that each nonzero element in R_∞ is an infinite sum, rather than a finite sum. For simplicity, we write each non zero element in R_∞ in the form $\gamma^i a$ where $a = a_0 + a_1\gamma + \cdots + \cdots$ with $a_0 \neq 0$ and $i \geq 0$, which means that a is a unit in R_∞. We note that if $v = \gamma^{l_1} a_{g_1} g_1 + \gamma^{l_2} a_{g_2} g_2 + \cdots + \gamma^{l_n} a_{g_n} g_n \in R_\infty G$, then the rows of $\sigma(v)$ consist precisely of the vectors that correspond to the elements hv in $R_\infty G$ where h is any element of the group G. Then we take the row space of the matrix $\sigma(v)$ over R_∞ to get the corresponding G-code, namely $\mathcal{C}(v)$.

Theorem 3.1. *Let R_∞ be the formal power series ring and G a finite group of order n. Let $v \in R_\infty G$ and let $\mathcal{C}(v)$ be the corresponding code in R_∞^n. Let $I(v)$ be the set of elements of $R_\infty G$ such that $\sum \gamma^{l_i} a_i g_i \in I(v)$ if and only if $(\gamma^{l_1} a_1, \gamma^{l_2} a_2, \ldots, \gamma^{l_n} a_n) \in \mathcal{C}(v)$. Then $I(v)$ is a left ideal in $R_\infty G$.*

Proof. The rows of $\sigma(v)$ consist precisely of the vectors that correspond to the elements hv in $R_\infty G$ where h is any element of G. Let $a = \sum \gamma^{l_i} a_i g_i$ and $b = \sum \gamma^{l_j} b_j g_i$ be two elements in $I(v)$, then $a + b = \sum(\gamma^{l_i} a_i + \gamma^{l_j} b_j) g_i$, which corresponds to the sum of the corresponding elements in $\mathcal{C}(v)$. This implies that $I(v)$ is closed under addition.

Let $w_1 = \sum \gamma^{l_i} b_i g_i \in R_\infty G$. Then if w_2 corresponds to a vector in $\mathcal{C}(v)$, it is of the form $\sum(\gamma^{l_j} \alpha_j) h_j v$. Then $w_1 w_2 = \sum \gamma^{l_i} b_i g_i \sum(\gamma^{l_j} \alpha_j) h_j v = \sum \gamma^{l_i} b_i \gamma^{l_j} \alpha_j g_i h_j v$ which corresponds to an element in $\mathcal{C}(v)$ and gives that the element is in $I(v)$. Therefore $I(v)$ is a left ideal of $R_\infty G$. □

It is well known that cyclic codes can be viewed as ideals in the ring $R[X]/\langle X^n - 1\rangle$, and that the reciprocal polynomial of the check polynomial $h(x)$, is used to generate the ideal in $R[X]/\langle X^n - 1\rangle$ corresponding to the dual code. In [3], the authors apply a similar approach to show that the dual of a G-code is also a G-code over a commutative Frobenius ring. They define an element in the group ring RG which is an ideal in that group ring, and also corresponds to the dual code. We now extend this result to G-codes over R_∞.

Let I be an ideal in a group ring $R_\infty G$. Define $\mathcal{R}(\mathcal{C}) = \{w \mid vw = 0, \ \forall v \in I\}$. It is immediate that $\mathcal{R}(I)$ is an ideal of $R_\infty G$.

Let $v = \gamma^{l_1} a_{g_1} g_1 + \gamma^{l_2} a_{g_2} g_2 + \cdots + \gamma^{l_n} a_{g_n} g_n \in R_\infty G$ and $\mathcal{C}(v)$ be the corresponding code. Let $\Omega : R_\infty G \to R_\infty^n$ be the canonical map that sends $\gamma^{l_1} a_{g_1} g_1 + \gamma^{l_2} a_{g_2} g_2 + \cdots + \gamma^{l_n} a_{g_n} g_n$ to $(\gamma^{l_1} a_{g_1}, \gamma^{l_2} a_{g_2}, \cdots, \gamma^{l_n} a_{g_n})$. Let I be the ideal $\Omega^{-1}(\mathcal{C})$. Let $\mathbf{w} = (w_1, w_2, \ldots, w_n) \in \mathcal{C}^\perp$. Then any row of the matrix $\sigma(v)$ dot product $\mathbf{w}$ should equal zero:

$$[(\gamma^{l_1} a_{g_j^{-1} g_1}, \gamma^{l_2} a_{g_j^{-1} g_2}, \ldots, \gamma^{l_n} a_{g_j^{-1} g_n}), (w_1, w_2, \ldots, w_n)] = 0, \ \forall j. \tag{17}$$

Which gives

$$\sum_{i=1}^{n} \gamma^{l_i} a_{g_j^{-1} g_i} w_i = 0, \ \forall j. \tag{18}$$

Let $w = \Omega^{-1}(\mathbf{w}) = \sum \gamma^{k_i} w_{g_i} g_i$ and define $\overline{\mathbf{w}} \in R_\infty G$ to be $\overline{\mathbf{w}} = \gamma^{k_1} b_{g_1} g_1 + \gamma^{k_2} b_{g_2} g_2 + \cdots + \gamma^{k_n} b_{g_n} g_n$, where

$$\gamma^{k_i} b_{g_i} = \gamma^{k_i} w_{g_i^{-1}}. \tag{19}$$

Then

$$\sum_{i=1}^{n} \gamma^{l_i} a_{g_j^{-1} g_i} w_i = 0 \implies \sum_{i=1}^{n} \gamma^{l_i} a_{g_j^{-1} g_i} \gamma^{k_i} b_{g_i^{-1}} = 0. \tag{20}$$

Here, $g_j^{-1} g_i g_i^{-1} = g_j^{-1}$, thus this is the coefficient of g_j^{-1} in the product of $\mathbf{w}$ and $g_j^{-1} v$, where $g_j^{-1} v$ is a row of the matrix $\sigma(v)$. This gives that $\overline{\mathbf{w}} \in \mathcal{R}(I)$ if and only if $\mathbf{w} \in \mathcal{C}^\perp$.

Let $\phi : R_\infty^n \to R_\infty G$ by $\phi(\mathbf{w}) = \overline{\mathbf{w}}$, then this map is a bijection between $\mathcal{C}^\perp$ and $\mathcal{R}(\Omega^{-1}(\mathcal{C})) = \mathcal{R}(I)$. Now we have the following result.

Theorem 3.2. *Let $\mathcal{C} = \mathcal{C}(v)$ be a code in $R_\infty G$ formed from the vector $v \in R_\infty G$. Then $\Omega^{-1}(\mathcal{C}^\perp)$ is an ideal of $R_\infty G$.*

Proof. The composite mapping $\Omega(\phi(\mathcal{C}^\perp))$ is permutation equivalent to $\mathcal{C}^\perp$ and $\phi(\mathcal{C}^\perp)$ is an ideal of $R_\infty G$. We know that ϕ is a bijection between $\mathcal{C}^\perp$ and $\mathcal{R}(\Omega^{-1}(\mathcal{C}))$, and we also know that $\Omega^{-1}(\mathcal{C})$ is an ideal of $R_\infty G$ as well. This proves that the dual of a G-code is also a G-code, over the formal power series ring. □

In cyclic codes, the coefficients of the reciprocal polynomial are those of the check polynomial but in reverse order. In $\overline{\mathbf{w}}$ above, the elements $w_{g_i^{-1}}$ correspond to the elements w_{g_i} in $\mathbf{w}$, but in different order, and this order will depend on the choice of the group. Therefore, we have used the permutation equivalence property in the proof.

4 Projections and Lifts of G-codes

We begin by showing that if $v \in R_\infty G$ then $\sigma(v)$ is permutation equivalent to the matrix defined in Equation 8. For simplicity, we write each non-zero element in R_∞ in the form $\gamma^i a$ where $a = a_0 + a_1\gamma + \cdots + \cdots$ with $a_0 \neq 0$ and $i \geq 0$, which means that a is a unit in R_∞.

Theorem 4.1. *Let $v = \gamma^{l_1} a_{g_1} g_1 + \gamma^{l_2} a_{g_2} g_2 + \cdots + \gamma^{l_n} a_{g_n} g_n \in R_\infty G$, where a_{g_i} are units in R_∞. Let $\mathcal{C} = \sigma(v)$ be a finitely generated code over R_∞. Then*

$$\sigma(v) = \begin{pmatrix} \gamma^{l_1} a_{g_1^{-1} g_1} & \gamma^{l_1} a_{g_1^{-1} g_2} & \gamma^{l_1} a_{g_1^{-1} g_3} & \dots & \gamma^{l_1} a_{g_1^{-1} g_n} \\ \gamma^{l_2} a_{g_2^{-1} g_1} & \gamma^{l_2} a_{g_2^{-1} g_2} & \gamma^{l_2} a_{g_2^{-1} g_3} & \dots & \gamma^{l_n} a_{g_2^{-1} g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \gamma^{l_n} a_{g_n^{-1} g_1} & \gamma^{l_n} a_{g_n^{-1} g_2} & \gamma^{l_n} a_{g_n^{-1} g_3} & \dots & \gamma^{l_n} a_{g_n^{-1} g_n} \end{pmatrix},$$

is permutation equivalent to the standard generator given in (8).

Proof. First, we take one non-zero element with form $\gamma^{m_0} a_{g_i}$, where m_0 is the minimal nonnegative integer. By applying column and row permutations and by dividing a row by a unit, the element that corresponds to the first row and column of $\sigma(v)$ can be replaced by γ^{m_0}. The elements in the first column of matrix $\sigma(v)$ have the form $\gamma^{l_j} a_{g_j}$ with $l_j \geq m_0$ and a_{g_j} a unit, thus, these can be replaced by zero when they are added to the first row multiplied by $-\gamma^{l_j - m_0}(a_{g_j})^{-1}$. Continuing the process using elementary operations, we obtain the standard generator matrix of the code $\mathcal{C}$ given in Equation 8. □

Example 1. *Let $v = \gamma^2 + \gamma^2(1+\gamma)yx + \gamma^2(1+\gamma+\gamma^2)yx^2 + \gamma^2 yx^3 \in R_\infty D_8$ where $\langle x, y\rangle \cong D_8$. Then*

$$\sigma(v) = \begin{pmatrix} A & B \\ B & A \end{pmatrix},$$

where $A = circ(\gamma^2, 0, 0, 0), B = rcirc(0, \gamma^2(1+\gamma), \gamma^2(1+\gamma+\gamma^2), \gamma^2)$. Then $\sigma(v)$ is equivalent to

$$G = \begin{pmatrix} \gamma^2 & 0 & 0 & 0 & 0 & \gamma^2(1+\gamma) & \gamma^2(1+\gamma+\gamma^2) & \gamma^2 \\ 0 & \gamma^2 & 0 & 0 & \gamma^2(1+\gamma) & \gamma^2(1+\gamma+\gamma^2) & \gamma^2 & 0 \\ 0 & 0 & \gamma^2 & 0 & \gamma^2(1+\gamma+\gamma^2) & \gamma^2 & 0 & \gamma^2(1+\gamma) \\ 0 & 0 & 0 & \gamma^2 & \gamma^2 & 0 & \gamma^2(1+\gamma) & \gamma^2(1+\gamma+\gamma^2) \end{pmatrix}.$$

Clearly, $G = \mathcal{C}(v) = \langle \sigma(v) \rangle$ is the $[8, 4, 4]$ extended Hamming code. Let $v_1 = \gamma^2 + \gamma^2(1+\gamma)yx + \gamma^2(1+\gamma+\gamma^2)yx^2 + \gamma^2 yx^3 \in R_\infty D_8$, $v_2 = \gamma^2 + \gamma^2(1+\gamma)y + \gamma^2(1+\gamma+\gamma^2)yx + \gamma^2 yx^2 \in R_\infty D_8$, $v_3 = \gamma^2 + \gamma^2(1+\gamma+\gamma^2)y + \gamma^2 yx + \gamma^2(1+\gamma)yx^3 \in R_\infty D_8$ and $v_4 = \gamma^2 + \gamma^2 y + \gamma^2(1+\gamma)yx^2 + \gamma^2(1+\gamma+\gamma^2)yx^3 \in R_\infty D_8$ where v_i are the group ring elements corresponding to the rows of G. Let $I(v) = \{\sum_{i=1}^4 \gamma^{l_1} a_i v_i | \gamma^{l_1} a_i \in R_\infty\}$. Then $I(v)$ is a left ideal of $R_\infty D_8$.

We now examine the projection of codes with a given type.

Proposition 4.2. *Let $\mathcal{C}$ be a G-code over R_∞ of type*

$$\{(\gamma^{m_0})^{k_0}, (\gamma^{m_1})^{k_1}, \dots, (\gamma^{m_{r-1}})^{k_{r-1}}\}$$

with generator matrix $\sigma(v)$. Then the code generated by $\Psi_i(\sigma(v))$ is a code over R_i of type $\{(\gamma^{m_0})^{k_0}, (\gamma^{m_1})^{k_1}, \ldots, (\gamma^{m_{s-1}})^{k_{s-1}}\}$ where s is the largest m_j that is less than i. Moreover, the code generated by $\Psi_i(\sigma(v))$ is equal to

$$\{(\Psi_i(c_1), \Psi_i(c_2), \ldots, \Psi_i(c_n)) \mid (c_1, c_2, \ldots, c_n) \in \mathcal{C}\}. \tag{21}$$

Proof. If $m_j > i-1$ then Ψ_i sends $\gamma^{m_1}M'$, where M' is a matrix, to a zero matrix which gives the first statement.

The code $\mathcal{C}$ is formed by taking the row space of $\sigma(v)$ over the ring R_∞, i.e. $\gamma^{l_1}a_1v_1 + \gamma^{l_2}a_2v_2 + \cdots + \gamma^{l_n}a_nv_n$ where $\gamma^{l_i}a_i \in R_\infty$ and v_j are the rows of $\sigma(v)$. If $w = \gamma^{l_j}a_jv_j$, then $\Psi_i(w) = \Psi_i(\gamma^{l_j}a_j)\Psi_i(v_j)$ by the equation given in (12) where $\Psi_i(v_j)$ applies the map coordinate-wise. This gives the second statement. □

Example 2. *Let $v = \sum_{j=0}^{3} \gamma^{l_{j+1}}a_{j+1}x^j + \gamma^{l_{j+5}}a_{j+5}x^jy \in R_\infty(C_2 \times C_4)$ where $(C_2 \times C_4) = \langle x_1, x_2 \mid x^4 = y^2 = 1, xy = yx\rangle$. Then,*

$$\sigma(v) = \begin{pmatrix} A & B \\ B & A \end{pmatrix},$$

where $A = circ(\gamma^{l_1}a_1, \gamma^{l_2}a_2, \gamma^{l_3}a_3, \gamma^{l_4}a_4), B = circ(\gamma^{l_5}a_5, \gamma^{l_6}a_6, \gamma^{l_7}a_7, \gamma^{l_8}a_8)$ and $\gamma^{l_j}a_j \in R_\infty$. Let $\sigma(v)$ be a generator matrix of a $(C_2 \times C_4)$-code $\mathcal{C}$. We know from Theorem 4.1 that $\mathcal{C}$ is a type $\{(\gamma^{m_0})^{k_0}, (\gamma^{m_1})^{k_1}, \ldots, (\gamma^{m_{r-1}})^{k_{r-1}}\}$ code, since it is permutation equivalent to the standard generator matrix. Each row of $\sigma(v)$ has the elements $\gamma^{l_1}a_1, \gamma^{l_2}a_2, \ldots, \gamma^{l_8}a_8$ in some specific order. Now,

$$\Psi_i(\sigma(v)) = \begin{pmatrix} A & B \\ B & A \end{pmatrix},$$

where $A = circ(\Psi_i(\gamma^{l_1}a_1), \Psi_i(\gamma^{l_2}a_2), \Psi_i(\gamma^{l_3}a_3), \Psi_i(\gamma^{l_4}a_4)), B = circ(\Psi_i(\gamma^{l_5}a_5), \Psi_i(\gamma^{l_6}a_6),$ $\Psi_i(\gamma^{l_7}a_7), \Psi_i(\gamma^{l_8}a_8))$ and $\Psi_i(\gamma^{l_j}a_{g_j}) \in R_i$. It follows that $\Psi_i(\sigma(v))$ is a code over R_i of type $\{(\gamma^{m_0})^{k_0}, (\gamma^{m_1})^{k_1}, \ldots, (\gamma^{m_{s-1}})^{k_{s-1}}\}$ where s is the largest m_j that is less than i.

We note that Ψ_i may send a non-zero coordinate to 0. This means that the Hamming weight of a code may decrease by applying Ψ_i, i.e. the minimum weight of $\Psi(\mathcal{C})$ may be less than the minimum weight of $\mathcal{C}$. The minimum weight cannot increase with the application of this map.

Lemma 4.3. *If $\mathcal{C}$ is a G-code over R_∞, then $\mathcal{C}^\perp$ has type 1^m for some m.*

Proof. First we notice that $\mathcal{C}$ is a linear code. From the matrix $\sigma(v)$, and the fact that it is permutation equivalent to the standard generator matrix in Equation 8, we know that all the codewords in $\mathcal{C}^\perp$ are of the form $\gamma^l\mathbf{v}$ for some nonnegative integer l. This gives that $[\gamma^l\mathbf{v}, \mathbf{w}] = 0 \ \forall \ \mathbf{w} \in \mathcal{C}^\perp$, Hence, $[\gamma^l\mathbf{v}, \mathbf{w}] = \gamma^l \sum_{l=1}^{n} v_lw_l = \gamma^l[\mathbf{v}, \mathbf{w}] = 0$, which gives that $[\mathbf{v}, \mathbf{w}] = 0$, since $0 \neq \gamma^l \in R_\infty$ and R_∞ is a domain. So if $\gamma^l\mathbf{v} \in \mathcal{C}^\perp$ then $\mathbf{v} \in \mathcal{C}^\perp$. Therefore the code $\mathcal{C}^\perp$ has the type 1^m for some m. □

Proposition 4.4. *Let $\mathcal{C}$ be a G-code over R_∞. Then $\mathcal{C} = (\mathcal{C}^\perp)^\perp$ if and only if $\mathcal{C}$ has type 1^k for some k.*

Proof. First we note that $\mathcal{C}$ is linear. Secondly, we note that $(\mathcal{C}^\perp)^\perp \subseteq \mathcal{C}$. Since $\mathcal{C}$ is a linear code then by Lemma 4.3, the code $\mathcal{C}^\perp$ is a linear code with type 1^k for some k. This gives that $(\mathcal{C}^\perp)^\perp$ has type $1^{n-(n-k)} = 1^k$. □

The above two are extensions of the results from [4]. The following result, which can also be found in [4], is very useful when it comes to finding the generator matrix of the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$, given that $\mathcal{C}$ has a standard generator matrix G as in Equation 8. We extend this result to G-codes over R_∞ but omit the proof as it is exactly the same as in [4].

Theorem 4.5. *Let $\mathcal{C}$ be a G-code of length n over R_∞. If $\mathcal{C}$ has a standard generator matrix G as in equation (8), then we have*

(i) the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$ has a generator matrix

$$H = \begin{pmatrix} B_{0,r} & B_{0,r-1} & \dots & B_{0,2} & B_{0,1} & I_{k_r} \end{pmatrix}, \tag{22}$$

where $B_{0,j} = -\sum_{l=1}^{j-1} B_{0,l} A^T_{r-j,r-l} - A^T_{r-j,r}$ for all $1 \leq j \leq r$;

(ii) rank($\mathcal{C}$)+rank($\mathcal{C}^\perp$)=n.

Example 3. *If we take the generator matrix G of a code $\mathcal{C}$ from Example 1, we can see that*

$$G = \left(\gamma^2 \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \gamma^2 \begin{pmatrix} 0 & 1+\gamma & 1+\gamma+\gamma^2 & 1 \\ 1+\gamma & 1+\gamma+\gamma^2 & 1 & 0 \\ 1+\gamma+\gamma^2 & 1 & 0 & 1+\gamma \\ 1 & 0 & 1+\gamma & 1+\gamma+\gamma^2 \end{pmatrix} \right),$$

which is the standard generator matrix- here,

$$A_{0,1} = \begin{pmatrix} 0 & 1+\gamma & 1+\gamma+\gamma^2 & 1 \\ 1+\gamma & 1+\gamma+\gamma^2 & 1 & 0 \\ 1+\gamma+\gamma^2 & 1 & 0 & 1+\gamma \\ 1 & 0 & 1+\gamma & 1+\gamma+\gamma^2 \end{pmatrix}.$$

In this case the generator matrix of the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$ has the form:

$$H = \begin{pmatrix} B_{0,1} & I_{k_1} \end{pmatrix}.$$

Now, from Theorem 4.5

$$B_{0,1} = -A^T_{0,1},$$

thus

$$H = \begin{pmatrix} 0 & -(1+\gamma) & -(1+\gamma+\gamma^2) & -1 & 1 & 0 & 0 & 0 \\ -(1+\gamma) & -(1+\gamma+\gamma^2) & -1 & 0 & 0 & 1 & 0 & 0 \\ -(1+\gamma+\gamma^2) & -1 & 0 & -(1+\gamma) & 0 & 0 & 1 & 0 \\ -1 & 0 & -(1+\gamma) & -(1+\gamma+\gamma^2) & 0 & 0 & 0 & 1 \end{pmatrix}.$$

We also have

$$\mathit{rank}(\mathcal{C}) + \mathit{rank}(\mathcal{C}^{\perp}) = 4 + 4 = 8 = n.$$

Proposition 4.6. *Let $\mathcal{C}$ be a self-orthogonal G-code over R_∞. Then the code $\Psi_i(\mathcal{C})$ is a self-orthogonal G-code over R_i for all $i < \infty$.*

Proof. We first show that $\Psi_i(\mathcal{C})$ is self-orthogonal. Let $v \in R_\infty G$ and $\langle \sigma(v) \rangle = \mathcal{C}(v)$ be the corresponding self-orthogonal G-code. This implies that $[\mathbf{v}, \mathbf{w}] = 0$ for all $\mathbf{v}, \mathbf{w} \in \langle \sigma(v) \rangle = \mathcal{C}(v)$. This gives that

$$\sum_{l=1}^{n} v_l w_l \equiv \sum_{l=1}^{n} \Psi_i(v_l)\Psi_i(w_l) (\text{mod } \gamma^i) \equiv \Psi_i([\mathbf{v}, \mathbf{w}]) (\text{mod } \gamma^i) \equiv 0 \ (\text{mod } \gamma^i).$$

Hence $\Psi_i(\mathcal{C})$ is a self-orthogonal code over R_i. To show that $\Psi_i(\mathcal{C})$ is also a G-code, we notice that when taking $\Psi_i(\mathcal{C}) = \Psi_i(\langle \sigma(v) \rangle)$, it corresponds to $\Psi_i(v) = \Psi_i(\gamma^{l_i} a_{g_i})g_1 + \Psi_i(\gamma^{l_2} a_{g_2})g_2 + \cdots + \Psi_i(\gamma^{l_n} a_{g_n})g_n$, then $\Psi_i(\mathcal{C}) \in R_i G$. Thus $\Psi_i(\mathcal{C})$ is also a G-code. □

Definition 5. *Let i, j be two integers such that $1 \leq i \leq j < \infty$. We say that an $[n, k]$ code $\mathcal{C}_1$ over R_i lifts to an $[n, k]$ code $\mathcal{C}_2$ over R_j, denoted by $\mathcal{C}_1 \succeq \mathcal{C}_2$, if $\mathcal{C}_2$ has a generator matrix G_2 such that $\Psi_i^j(G_2)$ is a generator matrix of $\mathcal{C}_1$. We also denote $\mathcal{C}_1$ by $\Psi_i^j(\mathcal{C}_2)$. If $\mathcal{C}$ is a $[n, k]$ γ-adic code, then for any $i < \infty$, we call $\Psi_i(\mathcal{C})$ a projection of $\mathcal{C}$. We denote $\Psi_i(\mathcal{C})$ by $\mathcal{C}^i$.*

Lemma 4.7. *Let $\mathcal{C}$ be a G-code over R_∞ with type 1^k. If $\sigma(v)$ is a standard form of $\mathcal{C}$, then for any positive integer, i, $\Psi_i(\sigma(v))$ is a standard form of $\Psi_i(\mathcal{C})$.*

Proof. We know from Theorem 4.1 that $\sigma(v)$ is permutation equivalent to a standard form matrix defined in Equation 8. We also have that $\mathcal{C}$ has type 1^k, hence $\Psi_i(\mathcal{C})$ has type 1^k. The rest of the proof is the same as in [4]. □

In the following, to avoid confusion, we let v_∞ and v be elements of the group rings $R_\infty G$ and $R_i G$ respectively. Let $v_\infty = \gamma^{l_1} a_{g_1} g_1 + \gamma^{l_2} a_{g_2} g_2 + \cdots + \gamma^{l_n} a_{g_n} g_n \in R_\infty G$, and $\mathcal{C}(v_\infty) = \langle \sigma(v_\infty) \rangle$ be the corresponding G-code. We now define the following map:

$$\sigma_1 : R_\infty G \to \mathcal{C}(v_\infty),$$

$$(\gamma^{l_1} a_{g_1} g_1 + \gamma^{l_2} a_{g_2} g_2 + \cdots + \gamma^{l_n} a_{g_n} g_n) \mapsto M(R_\infty G, v_\infty).$$

We define a projection of G-codes from $R_\infty G$ to $R_i G$.

Let

$$\Psi_i : R_\infty G \to R_i G \tag{23}$$

$$\gamma^i a \mapsto \Psi(\gamma^i a). \tag{24}$$

The projection is a homomorphism which means that if I is an ideal of $R_\infty G$, then $\Psi_i(I)$ is an ideal of $R_i G$. We have the following commutative diagram:

$$\begin{tikzcd} R_\infty G \arrow[r, "\sigma_1"] \arrow[d, "\Psi_i"'] & \mathcal{C}(v_\infty) \arrow[d, "\Psi_i"] \\ R_i G \arrow[r, "\sigma_1"'] & \mathcal{C}(v) \end{tikzcd} .$$

This gives that $\Psi_i \sigma_1 = \sigma_1 \Psi_i$, which gives the following theorem.

Theorem 4.8. *If $\mathcal{C}$ is a G-code over R_∞, then $\Psi_i(\mathcal{C})$ is a G-code over R_i for all $i < \infty$.*

Proof. Let $v_\infty \in R_\infty G$ and $\mathcal{C}(v_\infty)$ be the corresponding G-code over R_∞. Then $\sigma_1(v_\infty) = \mathcal{C}(v_\infty)$ is an ideal of $R_\infty G$. By the homomorphism in Equation 23 and the commutative diagram above, we know that $\Psi_i(\sigma_1(v_\infty)) = \sigma_1(\Psi_i(v_\infty))$ is an ideal of the group ring $R_i G$. This implies that $\Psi_i(\mathcal{C})$ is a G-code over R_i for all $i < \infty$. □

This gives that if we take any element $v \in R_\infty G$, for a finite group G, and form $\sigma(v)$, then we get a family of infinitely many G-code by taking $\Psi_i(\mathcal{C}(v))$ for all i. In the same way, if we take any element $v \in R_1 G$, then we get a family of infinitely many G-code by taking the lifts of the code $\mathcal{C}(v)$. Hence, each G code over a finite chain ring is part of an infinite family of G-codes.

Theorem 4.9. *Let $\mathcal{C}$ be a G-code over R_i, then the lift of $\mathcal{C}$, $\tilde{\mathcal{C}}$ over R_j, where $j > i$, is also a G-code.*

Proof. Let $v_1 = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \cdots + \alpha_{g_n} g_n \in R_i G$ and $\mathcal{C} = \langle \sigma(v_1) \rangle$ be the corresponding G-code. Let $v_2 = \beta_{g_1} g_1 + \beta_{g_2} g_2 + \cdots + \beta_{g_n} g_n \in R_j G$ and $\tilde{\mathcal{C}} = \langle \sigma(v_2) \rangle$ be the corresponding G-code. We can say that v_1 and v_2 act as generators of $\mathcal{C}$ and $\tilde{\mathcal{C}}$ respectively. We can clearly see that $\Psi_i^j(v_2) = \Psi_i^j(\beta_{g_1}) g_1 + \Psi_i^j(\beta_{g_2}) g_2 + \cdots + \Psi_i^j(\beta_{g_n}) g_n = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \cdots + \alpha_{g_n} g_n \in R_i G$, thus $\Psi_i^j(v_2)$ is a generator matrix of $\mathcal{C}$. This implies that the G-code $\mathcal{C}(v_1)$ over R_i lifts to a G-code over R_j, for all $j > i$. □

Example 4. *Here we construct an infinite family of a G-code. If we take $v_\infty = \gamma^2 + \gamma^2(1 + \gamma)yx + \gamma^2(1 + \gamma + \gamma^2)yx^2 + \gamma^2 yx^3 \in R_\infty D_8$ where $\langle x, y \rangle \cong D_8$, then we saw in Example 1 that $\mathcal{C}(v_\infty) = \langle \sigma(v_\infty) \rangle$ is the $[8, 4, 4]$ extended Hamming code. If we take $\Psi_1(\mathcal{C}(v_\infty))$ so that* *the elements $\{\gamma^2, \gamma^2(1+\gamma), \gamma^2(1+\gamma+\gamma^2)\} \in R_\infty$ all get mapped to $1 \in R_1 = \mathbb{F}_2$, we get the $[8,4,4]$ extended binary Hamming code, i.e.,*

$$\begin{tikzcd}
v_\infty = \gamma^2 + \gamma^2(1+\gamma)yx + \gamma^2(1+\gamma+\gamma^2)yx^2 + \gamma^2 yx^3 \in R_\infty D_8 \arrow[r, "\sigma_1"] \arrow[d, "\Psi_1"'] & \mathcal{C}(v_\infty) \arrow[d, "\Psi_1"] \\
v = 1 + yx + yx^2 + yx^3 \in R_1 D_8 = \mathbb{F}_2 D_8 \arrow[r, "\sigma_1"] & \mathcal{C}(v)
\end{tikzcd} .$$

If we now take $v = 1 + yx + yx^2 + yx^3 \in R_1 D_8 = \mathbb{F}_2 D_8$ then $C(v) = \langle \sigma(v) \rangle$ is equivalent to the $[8,4,4]$ extended binary Hamming code. Next we take $v_\infty = \gamma^2 + \gamma^2(1+\gamma)yx + \gamma^2(1+\gamma+\gamma^2)yx^2 + \gamma^2 yx^3 \in R_\infty D_8$ where $\mathcal{C}(v_\infty) = \langle \sigma(v_\infty) \rangle$ is also the $[8,4,4]$ extended Hamming code. We can then have $\Psi_1(v_\infty) = \Psi_1(\gamma^2)1 + \Psi_1(\gamma^2(1+\gamma)yx + \Psi_1(\gamma^2(1+\gamma+\gamma^2)yx^2 + \Psi_1(\gamma^2)yx^3 = 1 + yx + yx^2 + yx^3 \in R_1 D_8 = \mathbb{F}_2 D_8$. Thus, $\Psi_1(v_\infty)$ is a generator matrix of $C(v)$. This implies that the G-code $\mathcal{C}(v)$ over $R_1 = \mathbb{F}_2$ lifts to a G-code over R_∞.

Hence we have constructed an infinite family of G-codes.

The following is an extension of codes over chain rings that are projections of γ-adic codes (see [4] for details), to G-codes.

By Lemma 4.7 and Theorem 4.8, we know that for an $[n,k]$ G-code $\mathcal{C}$ over R_∞ of type 1^k, $\mathcal{C}^i = \Psi_i(\mathcal{C})$ is an $[n,k]$ G-code of type 1^k over R_i. We also have $\mathcal{C}^i \preceq \mathcal{C}^{i+1}$ for all i. Thus if a G-code $\mathcal{C}$ over R_∞ of type 1^k is given, then we obtain a series of lifts of G-codes as follows:

$$\mathcal{C}^i \preceq \mathcal{C}^2 \preceq \cdots \preceq \mathcal{C}^i \preceq \dots$$

Conversely, let $\mathcal{C}$ be an $[n,k]$ G-code over $\mathbb{F} = R_e/\langle\gamma\rangle = R_1$, and let $G = G_1$ be its generator matrix. It is clear that we can define a series of generator matrices, $G_i \in M_{k\times n}(R_i)$ such that $\Psi_i^{i+1}(G_{i+1}) = G_i$, where $M_{k\times n}(R_i)$ denotes all the matrices with k rows and n columns over R_i. This defines a series of lifts $\mathcal{C}_i$ of $\mathcal{C}$ to R_i for all i. Then this series of lifts determines a unique code $\mathcal{C}$ that $\mathcal{C}^i = \mathcal{C}_i$.

Let $\mathcal{C}$ be an $[n,k]$ G-code of type 1^k, and G, H be a generator and parity-check matrices of $\mathcal{C}$. Let $G_i = \Psi_i(G)$ and $H_i = \Psi_i(H)$. Then G_i and H_i are generator and parity check matrices of $\mathcal{C}^i$ respectively. The following results are well known and can be applied to G-codes over R_∞ since these are also γ-adic codes. Proofs can be found in [4].

Lemma 4.10. *Let $i < j < \infty$ be two positive integers, then*

(i) $\gamma^{j-i} G_i \equiv \gamma^{j-i} G_j \pmod{\gamma^j}$;

(ii) $\gamma^{j-i} H_i \equiv \gamma^{j-i} H_j \pmod{\gamma^j}$.

(iii) $\gamma^{j-1}\mathcal{C}^i \subseteq \mathcal{C}^j$;

(iv) $\mathbf{v} = \gamma^i \mathbf{v}_0 \in \mathcal{C}^j$ *if and only if* $\mathbf{v}_0 \in \mathcal{C}^{j-i}$;

(v) $Ker(\Psi_i^j) = \gamma^i \mathcal{C}^{j-i}$.

Lemma 4.10 (v) shows that the Hamming weight enumerator of the kernel $Ker(\Psi_i^j)$ is equal to the Hamming weight enumerator of $\mathcal{C}^{j-i}$.

In [4], the authors study the weights of codewords in lifts of a code. We state the result with an extension to G-codes over R_∞. We omit the proof since it is the same as in [4] as G-codes over R_∞ are just a special type of γ-adic codes.

Theorem 4.11. *Let $\mathcal{C}$ be a G-code over R_∞. Then the following two results hold.*

(i) the minimum Hamming distance $d_H(\mathcal{C}^i)$ of $\mathcal{C}^i$ is equal to $d = d_H(\mathcal{C}^1)$ for all $i < \infty$;

(ii) the minimum Hamming distance $d_\infty = d_H(\mathcal{C})$ of $\mathcal{C}$ is at least $d = d_H(\mathcal{C}^1)$.

In the remainder of this section, we extend the two results from [4] on MDS and MDR codes over R_∞ to the same type of codes which are also G-codes over the same ring.

It is known (see [9]) that for codes $\mathcal{C}$ of length n over any alphabet of size m

$$d_H(\mathcal{C}) \leq n - \log_m(|\mathcal{C}|) + 1 \tag{25}$$

Codes meeting this bound are called MDS (*Maximal Distance Separable*) codes.

For a code $\mathcal{C}$ of length n over an finite Quasi-Frobenius ring R, we have (see [7])

$$r_{\mathcal{C}} = \min\{l \mid \text{there exists a monomorphism } \mathcal{C} \to R^l \text{ as } R-\text{modules}\}.$$

If $\mathcal{C}$ is linear, then we have (see [7])

$$d_H(\mathcal{C}) \leq n - r_{\mathcal{C}} + 1. \tag{26}$$

Codes meeting this bound are called MDR (*Maximal Distance with respect to Rank*) codes.

A linear code $\mathcal{C}$ over R is called free if $\mathcal{C}$ is isomorphic as a module to R^t for some t. This implies that if $\mathcal{C}$ is free then $r_{\mathcal{C}} = \text{rank}(\mathcal{C})$.

Theorem 4.12. *Let $\mathcal{C}$ be a G-code over R_∞. If $\mathcal{C}$ is an MDR or MDS code then $\mathcal{C}^\perp$ is an MDS code.*

Proof. We know that $\mathcal{C}$ is linear. Assume that $\mathcal{C}$ is of length n, rank k, with $d_H(\mathcal{C}) = n - k + 1$. We know from Lemma 4.3 that if $\mathcal{C}$ is of rank k then $\mathcal{C}^\perp$ is of type 1^{n-k}. Since R_∞ is a domain, any $n-k$ columns of the generator matrix (equivalently a parity check matrix) of $\mathcal{C}^\perp$ are linearly independent giving that the minimum Hamming weight of $\mathcal{C}^\perp$ is $n - (n-k) + 1 = k + 1$. □

Theorem 4.13. *Let $\mathcal{C}$ be a G-code over R_i, and $\tilde{\mathcal{C}}$ be a lift G-code of $\mathcal{C}$ over R_j, where $j > i$. If $\mathcal{C}$ is an MDS code over R_i then the code $\tilde{\mathcal{C}}$ is an MDS code over R_j.*

Proof. Since $\mathcal{C}$ is a linear code, the proof is the same as in [4]. □

5 Self-Dual γ-adic G-codes

One of the most significant uses of G-codes so far has been their use in constructing good self-dual codes. In this section, we extend some results for self-dual γ-adic codes to G-codes over R_∞. We therefore fix the ring R_∞ with

$$R_\infty \to \cdots \to R_i \to \cdots \to R_2 \to R_1$$

and $R_1 = \mathbb{F}_q$ where $q = p^r$ for some prime p and nonnegative integer r. The field $\mathbb{F}_q$ is said to be the underlying field of the rings. We now state two very well known results for self-dual codes over $\mathbb{F}_q$ and self-dual codes over R_∞. These can be found in [11] and [4] respectively.

Theorem 5.1. *(i) If $p = 2$ or $p \equiv 1 \pmod 4$, then a self-dual code of length n exists over $\mathbb{F}_q$ if and only if $n \equiv 0 \pmod 2$;*

(ii) If $p \equiv 3 \pmod 4$, then a self-dual code of length n exists over $\mathbb{F}_q$ if and only if $n \equiv 0 \pmod 4$.

Corollary 5.2. *Let $\mathcal{C}$ be a self-dual code of length n over R_∞. Recall that p is the characteristic of the underlying field $\mathbb{F}$. We have*

(i) If $p = 2$ or $p \equiv 1 \pmod 4$, then $n \equiv 0 \pmod 2$;

(ii) If $p \equiv 3 \pmod 4$, then $n \equiv 0 \pmod 4$.

In [4], the authors also prove that if i is even, then self-dual codes of length n exist over R_i for all n. This can be easily extended to self-dual G-codes as these are a special type of self-dual codes over R_i. We now look at two theorems from [4] where one considers self-dual codes over R_i with a specific type and one considers projections of self-dual codes over R_∞. We extend these to self-dual G-codes over R_i and R_∞ respectively.

Theorem 5.3. *Let i be odd and $\mathcal{C}$ be a G-code over R_i with type $1^{k_0}(\gamma)^{k_1}(\gamma^2)^{k_2}\ldots(\gamma^{i-1})^{k_{i-1}}$. Then $\mathcal{C}$ is a self-dual code if and only if $\mathcal{C}$ is self-orthogonal and $k_j = k_{i-j}$ for all j.*

Proof. It is enough to show that $\sigma(v)$ where $v \in R_iG$ and G is a finite group, is permutation equivalent to the matrix (6). The rest of the proof is the same as in [4]. □

Theorem 5.4. *If $\mathcal{C}$ is a self-dual G-code of length n over R_∞ then $\Psi_i(\mathcal{C})$ is a self-dual G-code of length n and type 1^k over R_i for all $i < \infty$.*

Proof. We first show that $\Psi_i(\mathcal{C})$ is self-dual. Since $\mathcal{C}$ is self-dual, $\mathcal{C} = \mathcal{C}^\perp$ which gives that $\mathcal{C} = \mathcal{C}^\perp = (\mathcal{C}^\perp)^\perp$. We also know from Proposition 4.4 that the code $\mathcal{C}$ has type 1^k for some k. Hence, $k = n - k$, which implies that $k = \frac{n}{2}$. Then $\Psi_i(\mathcal{C})$ also has type 1^k, with $k = \frac{n}{2}$ giving the desired size condition. We also know from Proposition 4.6 that $\Psi_i(\mathcal{C})$ is self-orthogonal.

Therefore $\Psi_i(\mathcal{C})$ is a self-dual code. To show that $\Psi_i(\mathcal{C})$ is also a G-code, we notice that when taking $\Psi_i(\mathcal{C}) = \Psi_i(\langle\sigma(v)\rangle)$, it corresponds to $\Psi_i(v) = \Psi_i(\gamma^{l_i} a_{g_i})g_1 + \Psi_i(\gamma^{l_2} a_{g_2})g_2 + \cdots + \Psi_i(\gamma^{l_n} a_{g_n})g_n$, then $\Psi_i(\mathcal{C}) \in R_iG$. Thus $\Psi_i(\mathcal{C})$ is also a G-code. □

In the remainder of this section, we extend two more results from [4]. The first one describes a method to construct a self-dual code over $\mathbb{F}$ from a self-dual code over R_i. We extend this to self-dual G-codes.

Theorem 5.5. *Let i be odd. A self-dual G-code of length n over R_i induces a self-dual G-code of length n over $\mathbb{F}_q$.*

Proof. The proof is similar to the one in [4] but with two extra things added. First, we notice that $\sigma(v)$ where $v \in R_iG$ which generates the self-dual code $\mathcal{C}(v)$, is permutation equivalent to a standard generator matrix G of the form:

$$G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & & & A_{0,i} \\ & \gamma I_{k_1} & \gamma A_{1,2} & \gamma A_{1,3} & & & \gamma A_{1,i} \\ & & \gamma^2 I_{k_2} & \gamma^2 A_{2,3} & & & \gamma^2 A_{2,i} \\ & & & \ddots & \ddots & & \\ & & & & \ddots & \ddots & \\ & & & & & \gamma^{i-1} I_{k_{i-1}} & \gamma^{i-1} A_{i-1,i} \end{pmatrix}.$$

Then the code $\mathcal{C}$ over R_i is of type $1^{k_0}(\gamma)^{k_1}(\gamma^2)^{k_2}\dots(\gamma^{i-1})^{k_{i-1}}$. Secondly, when the map $\Psi_1^i(\tilde{G})$ is used in [4], we notice that in our case the map will correspond to $\Psi_1^i(\tilde{G}) = \Psi_1^i(v) = \Psi_1^i(\gamma^{l_i} a_{g_i})g_1 + \Psi_1^i(\gamma^{l_2} a_{g_2})g_2 + \cdots + \Psi_1^i(\gamma^{l_n} a_{g_n})g_n$, assuming that $\tilde{G}$ is the generator matrix of a G-code and $v \in R_iG$. Then $\Psi_1^i(\tilde{G})$ is the generator matrix of a G-code over $\mathbb{F}_q$. □

The last result from [4] which we extend to G-codes is the one which considers lifts of self-dual codes over $\mathbb{F}$ to self-dual codes over R_∞. The authors prove the result by starting with a generator matrix of the code $\mathcal{C}$ over $R_1(= \mathbb{F})$ which has the form $G_1 = (I \mid A_1)$, and then using the induction to show that there exist matrices $G_i = (I \mid A_i)$ such that $\Psi_i^{i+1}(G_{i+1}) = G_i$. To extend this to self-dual G-codes, we can define the matrix G_1 by taking the row space of $\sigma(v)$ over $\mathbb{F}$ and perform row or column permutations to get a self-dual code of the form $(I \mid A_1)$ where A_1 is a matrix over $\mathbb{F} = R_1$. A similar approach can be found in [3], where examples of the $[16, 5, 8]$ Reed-Muller code, the $[8, 4, 4]$ extended Hamming code or $[24, 12, 8]$ Golay code over $\mathbb{F}_2$ are constructed from group rings and $\sigma(v)$.

Theorem 5.6. *Let $R = R_e$ be a finite chain ring, $\mathbb{F} = R/\langle\gamma\rangle$, where $|\mathbb{F}| = q = p^r, 2 \neq p$ is a prime. Then any self-dual G-code $\mathcal{C}$ over $\mathbb{F}$ can be lifted to a self-dual G-code over R_∞.*

Proof. We know by Theorem 4.9 that a G-code over R_i can be lifted to a G-code over R_j, where $j > i$. To show that a self-dual G-code over $\mathbb{F}$ lifts to a self-dual G-code over R_∞, it is enough to follow the proof in [4], but with the generator matrix G_1 being defined as above. □

6 G-codes over Principal Ideal Rings

Let $R^1_{e_1}, R^2_{e_2}, \ldots, R^s_{e_s}$ be chain rings, where $R^j_{e_j}$ has unique maximal ideal $\langle \gamma_j \rangle$ and the nilpotency index of γ_j is e_j. Let $\mathbb{F}^j = R^j_{e_j}/\langle \gamma_j \rangle$. Let

$$A = \mathrm{CRT}(R^1_{e_1}, \ldots, R^j_{e_j}, \ldots, R^s_{e_s}).$$

We know that A is a principal ideal ring. For any $1 \leq i < \infty$, let

$$A^j_i = \mathrm{CRT}(R^1_{e_1}, \ldots, R^j_i, \ldots, R^s_{e_s}).$$

This gives that all the rings A^j_i are principal ideal rings. In particular, $A^j_{e_j} = A$. We denote $\mathrm{CRT}(R^1_{e_1} \ldots, R^j_\infty, \ldots, R^s_{e_s})$ by A^j_∞.

For $1 \leq i < \infty$, let $\mathcal{C}^j_i$ be a code over R^j_i. Let

$$\mathcal{C}^j_i = \mathrm{CRT}(\mathcal{C}^1_{e_1}, \ldots, \mathcal{C}^j_i, \ldots, \mathcal{C}^s_{e_s})$$

be the associated code over A^j_i. Let

$$\mathcal{C}^j_\infty = \mathrm{CRT}(\mathcal{C}^1_{e_1}, \ldots, \mathcal{C}^j_\infty, \ldots, \mathcal{C}^s_{e_s})$$

be associated code over A^j_∞. We can now prove the following.

Theorem 6.1. *Let $\mathcal{C}^j_{e_j}$ be a G-code over the chain ring $R^j_{e_j}$. Then $\mathcal{C}^j_\infty = CRT(\mathcal{C}^1_{e_1}, \ldots, \mathcal{C}^j_\infty, \ldots, \mathcal{C}^s_{e_s})$ is a G-code over A^j_∞.*

Proof. Let $g \in G$ and $\mathbf{v}_i \in \mathcal{C}^j_{e_j}$. Each row of $\mathcal{C}^j_{e_j}$ is of the form $g\mathbf{v}_i$, for all i. Now, if $\mathbf{v} = CRT(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s)$, then $g\mathbf{v} = CRT(g\mathbf{v}_1, g\mathbf{v}_2, \ldots, g\mathbf{v}_s)$ and so $g\mathbf{v} \in \mathcal{C}^j_\infty$, giving that $\mathcal{C}^j_\infty$ is an ideal in $A^j_\infty G$. □

7 Conclusion

In this work, we studied G-codes over the formal power series rings and finite chain rings. We generalized many known results of codes over these rings to G-codes. We showed that the dual of a G-code is also a G-code and we studied projections and lifts of G-codes with a given type in this setting. We also extended known methods of constructing a self-dual code over $\mathbb{F}$ from a self-dual code over R_i and a self-dual code over $\mathbb{F}$ to a self-dual code over R_∞, to self-dual G-codes. We lastly considered G-codes over principal ideal rings. Throughout the paper, we constructed examples in which the codes have generator matrices that consist of blocks which are either circulant or reverse circulant matrices. We do not know if this is a general feature for any finite group ring, we therefore suggest that this is studied in the future work.

References

[1] A.R. Calderbank, N.J.A. Sloane, “Modular and p-adic Cyclic Codes”, Des. Codes and Cryptog., vol. 6, pp. 21–35, 1995.

[2] Dougherty, S.T., “Algebraic Coding Theory Over Finite Commutative Rings”, Springer Briefs in Mathematics, Springer, 2017.

[3] S.T. Dougherty, J. Gildea, R. Taylor, A. Tylshchak, “Group Rings, G-Codes and Constructions of Self-Dual and Formally Self-Dual Codes”, Des. Codes and Cryptog., vol. 86, no. 9, pp. 2115–2138, 2018.

[4] S.T. Dougherty, H. Liu, Y.H. Park, “Lifted Codes over Finite Chain Rings”, Mathematical Journal of Okayama University, vol. 53, pp. 39–53, 2010.

[5] S.T. Dougherty, H. Liu, “Cyclic Codes over Formal Power Series Rings”, Acta Mathematica Scientia, vol. 31, no. 1, pp. 331–343, 2011.

[6] S.T. Dougherty, Y.H. Park, “Codes over the p-adic integers”, Des. Codes and Cryptog., vol. 39, no. 1, pp. 65–80, 2006.

[7] Horimoto, H. and Shiromoto, K., “A Singleton bound for linear codes over quasi-Frobenius rings”, Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, pp. 51–52, 1999.

[8] T. Hurley, “Group Rings and Rings of Matrices”, Int. Jour. Pure and Appl. Math, vol. 31 , no. 3, 319-335, 2006.

[9] MacWilliams F. J., Sloane N. J. A., “The Theory of Error-Correcting Codes”. North-Holland, Amsterdam, 1977.

[10] B. R. McDonald, “Finite Rings with Identity”, New York: Marcel Dekker, Inc, 1974.

[11] Rains E., Sloane N.J.A., “Self-dual codes, in the Handbook of Coding Theory”, Pless V.S. and Huffman W.C., eds., Elsevier, Amsterdam, pp. 177–294, 1998.