Abstract: In this work, we define $G$-codes over the infinite ring $R_\infty$ 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 $\gamma$-adic codes over $R_\infty$ to $\gamma$-adic $G$-codes over the same ring. We also study $G$-codes over principal ideal rings.

2010 MSC: 94B05, 16S34

Keywords: $G$-codes, Finite chain rings, Formal power series rings, $\gamma$-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 $\mathbb{Z}_p \epsilon$ by studying cyclic codes over the $p$-adic numbers. This approach implied results for cyclic codes over $\mathbb{Z}_p \epsilon$ for all $\epsilon > 0$ 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], $\gamma$-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 $\hat{R}$ 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, $\hat{R} \cong_R R$.
- As a right module, $\hat{R} \cong_R R$.

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

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

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

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

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

**Definition 2.1.** A linear code $C$ over an infinite ring $R$ is called basic if $C = (C^\perp)^\perp$. 

56
Not all linear codes are basic. For example, consider the code over the $p$-adic integers of length 2 given by $C = \langle \langle p, p \rangle \rangle$. Here $C^\perp = \langle \langle 1, -1 \rangle \rangle$. However, $\langle \langle 1, -1 \rangle \rangle^\perp = \langle \langle 1, 1 \rangle \rangle$ which strictly contains the code $C$. Therefore, this code is not basic.

\section{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 $R_\infty$. We refer the reader to \cite{4} and \cite{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 $R\tilde{\gamma} = \langle \beta \tilde{\gamma} | \beta \in R \rangle$. We have the following chain of ideals:

\[ R = \langle \tilde{\gamma}^0 \rangle \supseteq \langle \tilde{\gamma}^1 \rangle \supseteq \cdots \supseteq \langle \tilde{\gamma}^e \rangle. \]

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:

\[ R = \langle \tilde{\gamma}^0 \rangle \supseteq \langle \tilde{\gamma}^1 \rangle \supseteq \cdots \supseteq \langle \tilde{\gamma}^e \rangle. \]

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:

\[ (1) \supseteq \langle p \rangle \supseteq \langle p^2 \rangle \supseteq \langle p^3 \rangle \cdots. \]

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 $|\mathbb{F}| = q = p^e$ for some integers $q$ and $r$. We know that $|\mathbb{F}^\times| = p^e - 1$. We now state two well-known lemmas for which the proofs can be found in \cite{10}.

\textbf{Lemma 2.2.} 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 $\mu$ a unit. The unit $\mu$ is unique modulo $\tilde{\gamma}^{e-1}$.

\textbf{Lemma 2.3.} 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 $r_0, \ldots, r_{e-1} \in V$ such that $r = \sum_{i=0}^{e-1} r_i \tilde{\gamma}^i$;

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

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

From Lemma 2.3, 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 \cite{4}, $\gamma$ will indicate the generator of the ideal of a chain ring, not necessarily the maximal ideal.

\textbf{Definition 2.4.} The ring $R_\infty$ is defined as a formal power series ring:

\[ R_\infty = \mathbb{F}[\gamma] = \{ \sum_{i=0}^{\infty} a_i \gamma^i | a_i \in \mathbb{F} \}. \]
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:

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

$$\sum_{l=0}^{i-1} a_l \gamma^l \cdot \sum_{l'=0}^{i-1} b_{l'} \gamma^{l'} = \sum_{s=0}^{i-1} (\sum_{l+l'=s} a_l b_{l'}) \gamma^s.$$  \hspace{1cm} (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 $R_\infty$ is a principal ideal domain.

We note that the ring $R_\infty$ is an infinite ring whereas each $R_i$ is a finite ring.

The fact that the ring $R_\infty$ 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 $\gamma$ is a non-trivial code $\mathcal{C}$ of length 1, where $\mathcal{C}^\perp = \langle \gamma^{i-1} \rangle$. Note here that $\langle \mathcal{C}^\perp \rangle^\perp = \mathcal{C}$. However, the ideal in $R_\infty$ generated by $\gamma$ 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:

$$G = \begin{pmatrix}
I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & A_{0,e} \\
\gamma I_{k_1} & \gamma^2 A_{1,2} & \gamma^2 A_{1,3} & \gamma^2 A_{1,4} & \cdots & \gamma^2 A_{1,e} \\
\gamma^2 I_{k_2} & \gamma^2 A_{2,3} & \gamma^2 A_{2,4} & \cdots & \gamma^2 A_{2,e} \\
\gamma^3 I_{k_3} & \gamma^3 A_{3,4} & \cdots & \gamma^3 A_{3,e} \\
\gamma^e I_{k_{e-1}} & \gamma^{e-1} A_{e-1,2} & \gamma^{e-1} A_{e-1,3} & \cdots & \gamma^{e-1} A_{e-1,e} \\
\end{pmatrix},$$  \hspace{1cm} (6)

where $e$ is the nilpotency index of $\gamma$. 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

$$1^{k_0} \gamma^{k_1} (\gamma^2)^{k_2} \cdots (\gamma^{e-1})^{k_{e-1}}.$$  \hspace{1cm} (7)

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

\[
G = \begin{pmatrix}
\gamma^{m_0}I_{k_0} & \gamma^{m_0}A_{0,1} & \gamma^{m_0}A_{0,2} & \cdots & \gamma^{m_0}A_{0,r} \\
\gamma^{m_1}I_{k_1} & \gamma^{m_1}A_{1,1} & \gamma^{m_1}A_{1,2} & \cdots & \gamma^{m_1}A_{1,r} \\
\gamma^{m_2}I_{k_2} & \gamma^{m_2}A_{2,1} & \gamma^{m_2}A_{2,2} & \cdots & \gamma^{m_2}A_{2,r} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\gamma^{m_{r-1}}I_{k_{r-1}} & \gamma^{m_{r-1}}A_{r-1,1} & \gamma^{m_{r-1}}A_{r-1,2} & \cdots & \gamma^{m_{r-1}}A_{r-1,r}
\end{pmatrix},
\]

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 2.5.** A code \( C \) with generator matrix of the form given in Equation 8 is said to be of type \((\gamma^{m_0})^{k_0}(\gamma^{m_1})^{k_1}\cdots(\gamma^{m_{r-1}})^{k_{r-1}},\)

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

A code \( C \) of length \( n \) with rank \( k \) over \( R_\infty \) is called a \( \gamma \)-adic \( [n,k] \) code. We call \( k \) the dimension of \( C \) and denote the dimension by \( \dim C = k \).

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

\[
\Psi_j^i : R_j \to R_i,
\]

\[
\sum_{l=0}^{j-1} a_l \gamma^l \mapsto \sum_{l=0}^{i-1} a_l \gamma^l.
\]

If we replace \( R_j \) with \( R_\infty \) then we obtain a map \( \Psi_\infty^i \). For convenience, we denote it by \( \Psi_i \). Since both, \( \Psi_j^i \) and \( \Psi_i \) are projection maps, it is easy to show that \( \Psi_j^i \) and \( \Psi_i \) are ring homomorphisms. Let \( a, b \) be two arbitrary elements in \( R_j \). It is easy to get that

\[
\Psi_j^i(a + b) = \Psi_j^i(a) + \Psi_j^i(b), \quad \Psi_j^i(ab) = \Psi_j^i(a)\Psi_j^i(b).
\]

If \( a, b \in R_\infty \), we have that

\[
\Psi_i(a + b) = \Psi_i(a) + \Psi_i(b), \quad \Psi_i(ab) = \Psi_i(a)\Psi_i(b).
\]

Note that the map \( \Psi_j^i \) and \( \Psi_i \) can be extended naturally from \( R_j \) to \( R_i \) and \( R_\infty \) to \( R_i \).

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

\[
\begin{array}{c}
R_\infty \\
\Psi \\
R \\
\end{array} \xrightarrow{\Psi} \begin{array}{c}
R_{i+1} \\
\vdots \\
R_1
\end{array}
\]
We note that in the above diagram, \( R \) is a finite chain ring with maximal ideal \( m = (\tilde{\gamma}) \), where \( \tilde{\gamma} \) is a generator of \( m \) 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 2.6.**

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

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

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

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

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

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

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

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

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 Hurley in [8], produces codes in $R^n$ from elements in the group ring $RG$. Let $R$ be a ring and let $G = \{g_1, g_2, \ldots, g_n\}$ 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

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

We note that the elements $g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}$ 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:

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

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 $R_{\infty}$. 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 $R_{\infty}$ is an infinite sum, rather than a finite sum. For simplicity, we write each non zero element in $R_{\infty}$ in the form $\gamma^i a$ where $a = a_0 + a_1 \gamma + \cdots + \gamma^n$ with $a_0 \neq 0$ and $i \geq 0$, which means that $a$ is a unit in $R_{\infty}$. We note that if $v = \gamma^i a_{g_1}g_1 + \gamma^j a_{g_2}g_2 + \cdots + \gamma^n a_{g_n}g_n \in R_{\infty}G$, 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 $R_{\infty}$ to get the corresponding $G$-code, namely $C(v)$.

**Theorem 3.1.** Let $R_{\infty}$ be the formal power series ring and $G$ a finite group of order $n$. Let $v \in R_{\infty}G$ and let $C(v)$ be the corresponding code in $R_{\infty}^n$. Let $I(v)$ be the set of elements of $R_{\infty}G$ such that $\sum \gamma^i a_{g_i}g_i \in I(v)$ if and only if $(\gamma^i a_{g_1}, \gamma^j a_{g_2}, \ldots, \gamma^n a_{g_n}) \in C(v)$. 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 $a = \sum \gamma^i a_{g_i}g_i$ and $b = \sum \gamma^j b_{g_i}g_i$ be two elements in $I(v)$, then $a + b = \sum(\gamma^i a_i + \gamma^j b_i)g_i$, which corresponds to the sum of the corresponding elements in $C(v)$. This implies that $I(v)$ is closed under addition.
Let \( w_1 = \sum \gamma^i b_i g_i \in R_\infty G \). Then if \( w_2 \) corresponds to a vector in \( \mathcal{C}(v) \), it is of the form \( \sum (\gamma^i \alpha_j) h_j v \). Then \( w_1 w_2 = \sum \gamma^i b_i g_i \sum (\gamma^i \alpha_j) h_j v = \sum \gamma^i b_i \gamma^j \alpha_j g_i h_j v \) 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 \( R[X]/(X^n - 1) \), and that the reciprocal polynomial of the check polynomial \( h(x) \), is used to generate the ideal in \( R[X]/(X^n - 1) \) 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 \( R_\infty \).

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

Let \( v = \gamma^1 a_{g_1} g_1 + \gamma^2 a_{g_2} g_2 + \cdots + \gamma^n a_{g_n} g_n \in R_\infty G \) and \( \mathcal{C}(v) \) be the corresponding code. Let \( \Omega : R_\infty G \to R_\infty \) be the canonical map that sends \( \gamma^1 a_{g_1} g_1 + \gamma^2 a_{g_2} g_2 + \cdots + \gamma^n a_{g_n} g_n \) to \( (\gamma^1 a_{g_1}, \gamma^2 a_{g_2}, \cdots, \gamma^n a_{g_n}) \). Let \( I \) be the ideal \( \Omega^{-1}(C) \). Let \( w = (w_1, w_2, \ldots, w_n) \in C^\perp \). Then any row of the matrix \( \sigma(v) \) dot product \( w \) should equal zero:

\[
[\gamma^1 a_{g_1}, \gamma^2 a_{g_2}, \cdots, \gamma^n a_{g_n}], (w_1, w_2, \ldots, w_n) = 0, \forall j. \tag{17}
\]

Which gives

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

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

\[
\gamma^{k_i} b_{g_i} = \gamma^{k_i} w_i^{-1}. \tag{19}
\]

Then

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

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

Let \( \phi : R_\infty \to R_\infty G \) by \( \phi(w) = \tilde{w} \), then this map is a bijection between \( C^\perp \) and \( \mathcal{R}(\Omega^{-1}(C)) = \mathcal{R}(I) \).

Now we have the following result.

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

**Proof.** The composite mapping \( \Omega(\phi(C^\perp)) \) is permutation equivalent to \( C^\perp \) and \( \phi(C^\perp) \) is an ideal of \( R_\infty G \). We know that \( \phi \) is a bijection between \( C^\perp \) and \( \mathcal{R}(\Omega^{-1}(C)) \), and we also know that \( \Omega^{-1}(C) \) 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 \( \tilde{w} \) above, the elements \( w_{g_i}^{-1} \) correspond to the elements \( w_{g_i} \) in \( w \), 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 of $R_\infty$ in the form $\gamma^a$ 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 $R_\infty$.

**Theorem 4.1.** Let $v = \gamma^i a_1 g_1 + \gamma^j a_2 g_2 + \cdots + \gamma^k a_k g_k \in R_\infty G$, where $a_k$ are units in $R_\infty$. Let $\mathcal{C} = C(v)$ be a finitely generated code over $R_\infty$. Then

$$
\sigma(v) = \begin{pmatrix}
\gamma^{i_1} a_{g_1}^{-1} \gamma^{i_2} a_{g_2}^{-1} \cdots \
\gamma^{i_2} a_{g_2}^{-1} \gamma^{i_3} a_{g_3}^{-1} \
\vdots \
\gamma^{i_n} a_{g_n}^{-1}
\end{pmatrix}
$$

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

**Proof.** First, we take one non-zero element with form $\gamma^m a$, where $m$ is a unit, 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 $\gamma^m$. The elements in the first column of matrix $\sigma(v)$ have the form $\gamma^i a_k$ with $l_i \geq m_0$ and $a_k$ a unit, thus, these can be replaced by zero when they are added to the first row multiplied by $-\gamma^{-m_0}(a_k)$. Continuing the process using elementary operations, we obtain the standard generator matrix of the code $C$ given in Equation 8. □

**Example 4.2.** Let $v = \gamma^2 + \gamma^2(1 + \gamma)yx + \gamma^2(1 + \gamma + \gamma^2)yx^2 + \gamma^2yx^3 \in R_\infty D_8$ where $(x, y) \cong D_8$. Then

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

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

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

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

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

**Proposition 4.3.** Let $C$ be a $G$-code over $R_\infty$ of type

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

with generator matrix $\sigma(v)$. Then the code generated by $\Psi_1(\sigma(v))$ is a code over $R_4$ of type $\{(\gamma^{m_0})^{k_0}, (\gamma^{m_1})^{k_1}, \ldots, (\gamma^{m_r-1})^{k_{r-1}}\}$ where $s$ is the largest $m_j$ that is less than $i$. Moreover, the code generated by $\Psi_1(\sigma(v))$ is equal to

$$
\{(\Psi_1(c_1), \Psi_1(c_2), \ldots, \Psi_1(c_n)) \mid (c_1, c_2, \ldots, c_n) \in C\}.
$$

(21)
**Theorem 4.7.** Let \( \gamma \) be a matrix, to a zero matrix which gives the first statement.

The code \( C \) is formed by taking the row space of \( \sigma(v) \) over the ring \( R_{\infty} \), i.e. \( \gamma_1 v_1 + \gamma_2 v_2 + \cdots + \gamma_n v_n \) where \( \gamma_i \in R_{\infty} \) and \( v_i \) are the rows of \( \sigma(v) \). If \( w = \gamma_1 v_1 \), then \( \Psi_i(w) = \Psi_i(\gamma_1 v_1) \) by the equation given in (12) where \( \Psi_i(v_j) \) applies the map coordinate-wise. This gives the second statement.

**Example 4.4.** Let \( v = \sum_{i=0}^{3} \gamma_{i+1} a_i + x^j + \gamma_{i+5} a_j + 5x^j y \in R_{\infty}(C_2 \times C_4) \) where \( (C_2 \times C_4) = (x_1, x_2 \mid x^4 = y^2 = 1, xy = yx) \). Then,

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

where \( A = circ(\gamma_{i1} a_1, \gamma_{i2} a_2, \gamma_{i3} a_3, \gamma_{i4} a_4), B = circ(\gamma_{i5} a_5, \gamma_{i6} a_6, \gamma_{i7} a_7, \gamma_{i8} a_8) \) and \( \gamma_i a_j \in R_{\infty} \). Let \( \sigma(v) \) be a generator matrix of a \( (C_2 \times C_4) \)-code \( C \). We know from Theorem 4.1 that \( C \) is a type \( \{ (\gamma_{m0})^{k_0}, (\gamma_{m1})^{k_1}, \ldots, (\gamma_{m-1})^{k_{m-1}} \} \) code, since it is permutation equivalent to the standard generator matrix. Each row of \( \sigma(v) \) has the elements \( \gamma_{i1} a_1, \gamma_{i2} a_2, \gamma_{i3} a_3, \gamma_{i4} a_4 \) in some specific order. Now,

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

where \( A = circ(\Psi_i(\gamma_{i1} a_1), \Psi_i(\gamma_{i2} a_2), \Psi_i(\gamma_{i3} a_3), \Psi_i(\gamma_{i4} a_4)), B = circ(\Psi_i(\gamma_{i5} a_5), \Psi_i(\gamma_{i6} a_6), \Psi_i(\gamma_{i7} a_7), \Psi_i(\gamma_{i8} a_8)) \) and \( \Psi_i(\gamma_{i1} a_j) \in R_i \). It follows that \( \Psi_i(\sigma(v)) \) is a code over \( R_i \) of type \( \{ (\gamma_{m0})^{k_0}, (\gamma_{m1})^{k_1}, \ldots, (\gamma_{m-1})^{k_{m-1}} \} \) where \( s \) is the largest \( m_j \) that is less than \( i \).

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

**Lemma 4.5.** If \( C \) is a \( G \)-code over \( R_{\infty} \), then \( C \) has type \( 1^m \) for some \( m \).

**Proof.** First we notice that \( C \) 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 \( C \) are of the form \( \gamma v \) for some nonnegative integer \( l \). This gives that \( [\gamma v, w] = 0 \forall w \in C \). Hence, \( [\gamma v, w] = \gamma \sum_{i=0}^{n} v_i w_i = \gamma [v, w] = 0 \), which gives that \( [v, w] = 0 \), since \( 0 \neq \gamma \in R_{\infty} \) and \( R_{\infty} \) is a domain. So if \( \gamma v \in C \), then \( v \in C \). Therefore the code \( C \) has the type \( 1^m \) for some \( m \).

**Proposition 4.6.** Let \( C \) be a \( G \)-code over \( R_{\infty} \). Then \( \dot{C} = (C \perp)^\perp \) if and only if \( C \) has type \( 1^k \) for some \( k \).

**Proof.** First we note that \( C \) is linear. Secondly, we note that \( (C \perp)^\perp \subseteq C \). Since \( C \) is a linear code then by Lemma 4.5, the code \( C \) is a linear code with type \( 1^k \) for some \( k \). This gives that \( (C \perp)^\perp \) 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 \( C \) of \( C \) given that \( C \) has a standard generator matrix \( G \) as in Equation 8. We extend this result to \( G \)-codes over \( R_{\infty} \) but omit the proof as it is exactly the same as in [4].

**Theorem 4.7.** Let \( C \) be a \( G \)-code of length \( n \) over \( R_{\infty} \). If \( C \) has a standard generator matrix \( G \) as in equation (8), then we have

(i) the dual code \( C \) of \( C \) has a generator matrix

\[
H = \begin{pmatrix} B_{0r} & B_{0r-1} & \cdots & B_{02} & B_{01} & I_k \end{pmatrix},
\]

where \( B_{0j} = -\sum_{i=1}^{j-1} B_{0i} A_{r-j,r-1}^T + A_{r-j,r}^T \) for all \( 1 \leq j \leq r \).
(ii) $\text{rank}(C) + \text{rank}(C^\perp) = n$.

**Example 4.8.** If we take the generator matrix $G$ of a code $C$ from Example 4.2, we can see that
\[
G = \left( \begin{array}{cccccc}
\gamma^2 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 \\
\end{array} \right) \left( \begin{array}{cccccc}
0 & 1 + \gamma & 1 + \gamma + \gamma^2 & 1 \\
1 + \gamma & 1 + \gamma + \gamma^2 & 1 & 0 \\
1 & 0 & 1 + \gamma & 1 + \gamma + \gamma^2 \\
\end{array} \right),
\]
which is the standard generator matrix here,
\[
A_{0,1} = \left( \begin{array}{cccccc}
0 & 1 + \gamma & 1 + \gamma + \gamma^2 & 1 \\
1 + \gamma + \gamma^2 & 1 + \gamma & 1 & 0 \\
1 & 0 & 1 + \gamma & 1 + \gamma + \gamma^2 \\
\end{array} \right).
\]
In this case the generator matrix of the dual code $C^\perp$ of $C$ has the form:
\[
H = (B_{0,1} \ I_{k_1}).
\]
Now, from Theorem 4.7
\[
B_{0,1} = -A_{0,1}^T,
\]
thus
\[
H = \left( \begin{array}{cccccc}
0 & -(1 + \gamma) & -(1 + \gamma + \gamma^2) & -1 & 0 & 0 & 0 \\
-(1 + \gamma) & -(1 + \gamma + \gamma^2) & 0 & 0 & 1 & 0 & 0 \\
-(1 + \gamma + \gamma^2) & 0 & -(1 + \gamma) & 0 & 0 & 1 & 0 \\
-1 & 0 & -(1 + \gamma) & 0 & 0 & 0 & 1 \\
\end{array} \right).
\]
We also have
\[
\text{rank}(C) + \text{rank}(C^\perp) = 4 + 4 = 8 = n.
\]

**Proposition 4.9.** Let $C$ be a self-orthogonal G-code over $R_\infty$. Then the code $\Psi_i(C)$ is a self-orthogonal $G$-code over $R_i$ for all $i < \infty$.

**Proof.** We first show that $\Psi_i(C)$ is self-orthogonal. Let $v \in R_\infty G$ and $\langle \sigma(v) \rangle = C(v)$ be the corresponding self-orthogonal $G$-code. This implies that $\langle v, w \rangle = 0$ for all $v, w \in \langle \sigma(v) \rangle = C(v)$. This gives that
\[
\sum_{i=1}^{n} v_i w_i \equiv \sum_{i=1}^{n} \Psi_i(v_i) \Psi_i(w_i) \equiv \Psi_i([v, w]) \equiv 0 \pmod{\gamma^i}.
\]
Hence $\Psi_i(C)$ is a self-orthogonal code over $R_i$. To show that $\Psi_i(C)$ is also a $G$-code, we notice that when taking $\Psi_i(C) = \Psi_i(\langle \sigma(v) \rangle)$, it corresponds to $\Psi_i(v) = \Psi_i(\gamma^i a_{g_1}) g_1 + \Psi_i(\gamma^i a_{g_2}) g_2 + \cdots + \Psi_i(\gamma^i a_{g_n}) g_n$, then $\Psi_i(C) \in R G$. Thus $\Psi_i(C)$ is also a $G$-code.

**Definition 4.10.** Let $i, j$ be two integers such that $1 \leq i \leq j < \infty$. We say that an $[n, k]$ code $C_1$ over $R_i$ lifts to an $[n, k]$ code $C_2$ over $R_j$, denoted by $C_1 \succeq C_2$, if $C_2$ has a generator matrix $G_2$ such that $\Psi_i^j(G_2)$ is a generator matrix of $C_1$. We also denote $C_1$ by $\Psi_i^j(C_2)$. If $C$ is a $[n, k]$ $\gamma$-adic code, then for any $i < \infty$, we call $\Psi_i(C)$ a projection of $C$. We denote $\Psi_i(C)$ by $C^i$.

**Lemma 4.11.** Let $C$ be a $G$-code over $R_\infty$ with type $1^k$. If $\sigma(v)$ is a standard form of $C$, then for any positive integer $i$, $\Psi_i(\sigma(v))$ is a standard form of $\Psi_i(C)$. 
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 $C$ has type $1^k$, hence $\Psi_i(C)$ has type $1^k$. The rest of the proof is the same as in [4].

In the following, to avoid confusion, we let $v_\infty$ and $v$ be elements of the group rings $R_\infty G$ and $R_i G$ respectively. Let $v_\infty = \gamma_1^i a_{g_1} g_1 + \gamma_2^i a_{g_2} g_2 + \cdots + \gamma_n^i a_{g_n} g_n \in R_\infty G$, and $C(v_\infty) = \langle \sigma(v_\infty) \rangle$ be the corresponding $G$-code. We now define the following map:

$$\sigma_1 : R_\infty G \rightarrow C(v_\infty),$$

$$(\gamma_1^i a_{g_1} g_1 + \gamma_2^i a_{g_2} g_2 + \cdots + \gamma_n^i a_{g_n} g_n) \mapsto M(R_\infty G, v_\infty).$$

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

Let

$$\psi_i : R_\infty G \rightarrow R_i G$$

$$\gamma^i a \mapsto \psi(\gamma^i a).$$

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:

$$R_\infty G \xrightarrow{\sigma_1} C(v_\infty)$$
$$\downarrow \psi_i \downarrow \psi_i$$
$$R_i G \xrightarrow{\sigma_i} C(v)$$

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

Theorem 4.12. If $C$ is a $G$-code over $R_\infty$, then $\psi_i(C)$ is a $G$-code over $R_i$ for all $i < \infty$.

Proof. Let $v_\infty \in R_\infty G$ and $C(v_\infty)$ be the corresponding $G$-code over $R_\infty$. Then $\sigma_1(v_\infty) = C(v_\infty)$ 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 $\psi_i(C)$ 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 $\psi_i(C(v))$ for all $i$. In the same way, if we take any element $v \in R_i G$, then we get a family of infinitely many $G$-code by taking the lifts of the code $C(v)$. Hence, each $G$ code over a finite chain ring is part of an infinite family of $G$-codes.

Theorem 4.13. Let $C$ be a $G$-code over $R_i$, then the lift of $C$, $\tilde{C}$ 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 $C = \langle \sigma(v_1) \rangle$ 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 $\tilde{C} = \langle \sigma(v_2) \rangle$ be the corresponding $G$-code. We can say that $v_1$ and $v_2$ act as generators of $C$ and $\tilde{C}$ respectively. We can clearly see that $\psi_i^1(v_2) = \psi_i^1(\beta_{g_1}) g_1 + \psi_i^1(\beta_{g_2}) g_2 + \cdots + \psi_i^1(\beta_{g_n}) g_n = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \cdots + \alpha_{g_n} g_n \in R_i G$, thus $\psi_i^1(v_2)$ is a generator matrix of $\tilde{C}$. This implies that the $G$-code $C(v_1)$ over $R_i$ lifts to a $G$-code over $R_j$, for all $j > i$.

Example 4.14. Here we construct an infinite family of a $G$-code. If we take $v_\infty = \gamma^2 + \gamma^2(1+\gamma)yx + \gamma^2(1+\gamma+\gamma^2)yx^2 + \gamma^2yx^3 \in R_\infty D_8$ where $(x, y) \cong D_8$, then we saw in Example 4.2 that $C(v_\infty) = \langle \sigma(v_\infty) \rangle$ is the
extended Hamming code. If we take \( \Psi_1(C(\infty)) \) 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.,

\[
v_\infty = \gamma^2 + \gamma^2(1+\gamma)yx + \gamma^2(1+\gamma+\gamma^2)yx^2 + \gamma^2 yx^3 \in R_\infty D_8 \quad \sigma_1 C(\infty)
\]

Thus, \( \Psi \) over \( C \) for details), to \( C \) for \( \infty \)-codes. Proofs can be found in \([4]\).

Conversely, let \( C \) be an \([n,k]\) \( G \)-code \( \infty \)-code over \( R_\infty \) of type \( 1^k \). \( C^i = \Psi_i(C) \) is an \([n,k]\) \( G \)-code of type \( 1^k \). We also have \( C_i \leq C_{i+1} \) for all \( i \). Thus if a \( G \)-code \( C \) over \( R_\infty \) of type \( 1^k \) is given, then we obtain a series of lifts of \( G \)-codes as follows:

\[
C^i \leq C^2 \leq \ldots \leq C^i \leq \ldots
\]

Conversely, let \( C \) be an \([n,k]\) \( G \)-code over \( \mathbb{F} = R_\infty / (\gamma) = R_1 \), 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 \( C_i \) of \( C \) to \( R_1 \) for all \( i \). Then this series of lifts determines a unique code \( C \) that \( C^i = C_i \).

Let \( C \) be an \([n,k]\) \( G \)-code of type \( 1^k \), and \( G, H \) be a generator and parity-check matrices of \( C \). 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 \( C_i \) respectively. The following results are well known and can be applied to \( G \)-codes over \( R_\infty \) since these are also \( \gamma \)-adic codes. Proofs can be found in \([4]\).

**Lemma 4.15.** 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) \( \gamma^{j-i}C^i \subseteq C^j \);

(iv) \( v = \gamma^i v_0 \in C^i \) if and only if \( v_0 \in C^{j-i} \);

(v) \( \text{Ker}(\Psi_i^j) = \gamma^iC^{j-i} \).

**Lemma 4.15** (v) shows that the Hamming weight enumerator of the kernel \( \text{Ker}(\Psi_i^j) \) is equal to the Hamming weight enumerator of \( C^{j-i} \).

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 \( R_\infty \). We omit the proof since it is the same as in \([4]\) as \( G \)-codes over \( R_\infty \) are just a special type of \( \gamma \)-adic codes.

**Theorem 4.16.** Let \( C \) be a \( G \)-code over \( R_\infty \). Then the following two results hold.

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

(ii) the minimum Hamming distance \( d_\infty = d_H(C) \) of \( C \) is at least \( d = d_H(C^1) \).
In the remainder of this section, we extend the two results from [4] on MDS and MDR codes over $R_\infty$ to the same type of codes which are also $G$-codes over the same ring.

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

$$d_H(C) \leq n - \log_m(|C|) + 1$$  (25)

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

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

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

If $C$ is linear, then we have (see [7])

$$d_H(C) \leq n - r_C + 1.$$  (26)

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

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

**Theorem 4.17.** Let $C$ be a $G$-code over $R_\infty$. If $C$ is an MDR or MDS code then $C^\perp$ is an MDS code.

**Proof.** We know that $C$ is linear. Assume that $C$ is of length $n$, rank $k$, with $d_H(C) = n - k + 1$. We know from Lemma 4.5 that if $C$ is of rank $k$ then $C^\perp$ is of type $1^{n-k}$. Since $R_\infty$ is a domain, any $n - k$ columns of the generator matrix (equivalently a parity check matrix) of $C^\perp$ are linearly independent giving that the minimum Hamming weight of $C^\perp$ is $n - (n - k) + 1 = k + 1$.

**Theorem 4.18.** Let $C$ be a $G$-code over $R_i$, and $\tilde{C}$ be a lift $G$-code of $C$ over $R_j$, where $j > i$. If $C$ is an MDS code over $R_i$ then the code $\tilde{C}$ is an MDS code over $R_j$.

**Proof.** Since $C$ is a linear code, the proof is the same as in [4].

**5. Self-dual $\gamma$-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 $\gamma$-adic codes to $G$-codes over $R_\infty$. We therefore fix the ring $R_\infty$ with

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

and $R_i = \mathbb{F}_q$ 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 $R_\infty$. 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 $C$ be a self-dual code of length $n$ over $R_\infty$. Recall that $p$ is the characteristic of the underlying field $F$. 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 $R_\infty$. We extend these to self-dual $G$-codes over $R_i$ and $R_\infty$ respectively.

**Theorem 5.3.** Let $i$ be odd and $C$ 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 $C$ is a self-dual code if and only if $C$ is self-orthogonal and $k_j = k_{i-j}$ for all $j$.

**Proof.** It is enough to show that $\sigma(v)$ where $v \in R_i G$ 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 $C$ is a self-dual $G$-code of length $n$ over $R_\infty$ then $\Psi_i(C)$ 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 $\Psi_i(C)$ is self-dual. Since $C$ is self-dual, $C = C^\perp$ which gives that $C = C^\perp = (C^\perp)^\perp$. We also know from Proposition 4.6 that the code $C$ has type $1^k$ for some $k$. Hence, $k = n - k$, which implies that $k = \frac{n}{2}$. Then $\Psi_i(C)$ also has type $1^k$, with $k = \frac{n}{2}$ giving the desired size condition. We also know from Proposition 4.9 that $\Psi_i(C)$ is self-orthogonal. Therefore $\Psi_i(C)$ is a self-dual code. To show that $\Psi_i(C)$ is also a $G$-code, we notice that when taking $\Psi_i(C) = \Psi_i((\sigma(v)))$, it corresponds to $\Psi_i(v) = \Psi_i(\gamma^l a_{g_1})g_1 + \Psi_i(\gamma^l a_{g_2})g_2 + \ldots + \Psi_i(\gamma^l a_{g_n})g_n$, then $\Psi_i(C) \in R_i G$. Thus $\Psi_i(C)$ 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 $v \in R_i G$ which generates the self-dual code $C(v)$, is permutation equivalent to a standard generator matrix $G$ of the form:

$$ G = \begin{pmatrix}
I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & A_{0,4} & \ldots & A_{0,i} \\
\gamma I_{k_1} & \gamma A_{1,1} & \gamma A_{1,2} & \gamma A_{1,3} & \gamma A_{1,4} & \ldots & \gamma A_{1,i} \\
\gamma^2 I_{k_2} & \gamma^2 A_{2,2} & \gamma^2 A_{2,3} & \gamma^2 A_{2,4} & \ldots & \gamma^2 A_{2,i} \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\gamma^{i-1} I_{k_{i-1}} & \gamma^{i-1} A_{i-1,1} & \gamma^{i-1} A_{i-1,2} & \gamma^{i-1} A_{i-1,3} & \gamma^{i-1} A_{i-1,4} & \ldots & \gamma^{i-1} A_{i-1,i}
\end{pmatrix}. $$

Then the code $C$ over $R_i$ is of type $1^{k_0}(\gamma)^{k_1}(\gamma^2)^{k_2}\ldots(\gamma^{i-1})^{k_{i-1}}$. Secondly, when the map $\Psi_i(\tilde{G})$ is used in [4], we notice that in our case the map will correspond to $\Psi_i(\tilde{G}) = \Psi_i(v) = \Psi_i(\gamma^l a_{g_1})g_1 + \Psi_i(\gamma^l a_{g_2})g_2 + \ldots + \Psi_i(\gamma^l a_{g_n})g_n$, assuming that $\tilde{G}$ is the generator matrix of a $G$-code and $v \in R_i G$. Then $\Psi_i(\tilde{G})$ 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 $R_\infty$. The authors prove the result by starting with a generator matrix of the code $C$ over $R_i(=\mathbb{F})$ 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 $(I \mid A_i)$ where $A_1$ is a matrix over $\mathbb{F} = R_i$. 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 $\sigma(v)$. 

---

69
Theorem 5.6. Let $R = R_s$ 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 over $\mathbb{F}$ can be lifted to a self-dual $G$-code over $R_\infty$.

Proof. We know by Theorem 4.13 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 $R_\infty$, 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 $R_{e_1}^1, R_{e_2}^2, \ldots, R_{e_s}^s$ be chain rings, where $R_{e_j}^j$ has unique maximal ideal $\langle \gamma_j \rangle$ and the nilpotency index of $\gamma_j$ is $e_j$. Let $\mathbb{F}^j = R_{e_j}^j/\langle \gamma_j \rangle$. Let

$$A = \text{CRT}(R_{e_1}^1, \ldots, R_{e_s}^s).$$

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

$$A_i^j = \text{CRT}(R_{e_1}^1, \ldots, R_{e_s}^s).$$

This gives that all the rings $A_i^j$ are principal ideal rings. In particular, $A_{e_j}^j = A$. We denote $\text{CRT}(R_{e_1}^1, \ldots, R_{\infty}^s)$ by $A_{\infty}^s$. For $1 \leq i < \infty$, let $C_i^j$ be a code over $R_{e_j}^i$. Let

$$C_i^j = \text{CRT}(C_{e_1}^1, \ldots, C_{e_s}^s)$$

be the associated code over $A_i^j$. Let

$$C_{\infty}^s = \text{CRT}(C_{e_1}^1, \ldots, C_{\infty}^s)$$

be associated code over $A_{\infty}^s$. We can now prove the following.

Theorem 6.1. Let $C_{e_j}^j$ be a $G$-code over the chain ring $R_{e_j}^j$. Then $C_{\infty}^j = \text{CRT}(C_{e_1}^1, \ldots, C_{\infty}^s)$ is a $G$-code over $A_{\infty}^s$.

Proof. Let $g \in G$ and $v_i \in C_{e_j}^j$. Each row of $C_{e_j}^j$ is of the form $g v_i$, for all $i$. Now, if $v = \text{CRT}(v_1, v_2, \ldots, v_s)$, then $gv = \text{CRT}(gv_1, gv_2, \ldots, gv_s)$ and so $gv \in C_{\infty}^j$, giving that $C_{\infty}^j$ is an ideal in $A_{\infty}^j G$.

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 $R_\infty$, 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 Cryptogr. 6(1) (1995) 21–35.
[2] S. T. Dougherty, Algebraic Coding Theory over Finite Commutative Rings, Springer Briefs in Mathematics, Springer, 2017.
[3] S. T. Dougherty, J. Gildea, R. Taylor, A. Tyshchak, Group rings, G–codes and constructions of self–dual and formally self–dual codes, Des. Codes Cryptogr. 86(9) (2018) 2115–2138.
[4] S. T. Dougherty, L. Hongwei, Y. H. Park, Lifted codes over finite chain rings, Math. J. Okayama Univ. 53 (2011) 39–53.
[5] S. T. Dougherty, L. Hongwei, Cyclic codes over formal power series rings, Acta Mathematica Scientia 31(1) (2011) 331–343.
[6] S. T. Dougherty, Y. H. Park, Codes over the $p$–adic integers, Des. Codes and Cryptogr. 39(1) (2006) 65–80.
[7] H. Horimoto, K. Shiromoto, 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 (1999) 51–52.
[8] T. Hurley, Group rings and rings of matrices, Int. Jour. Pure and Appl. Math 31(3) (2006) 319–335.
[9] F. J. MacWilliams, N. J. A. Sloane, 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] E. Rains, N. J. A. Sloane, Self–dual codes, in the Handbook of Coding Theory , Pless V.S. and Huffman W.C., eds., Elsevier, Amsterdam, 177–294, 1998.