Composite $G$-codes over formal power series rings and finite chain rings

Adrian Korban

Abstract: In this paper, we extend the work done on $G$-codes over formal power series rings and finite chain rings $F_q[t]/(t^i)$, to composite $G$-codes over the same alphabets. We define composite $G$-codes over the infinite ring $R_\infty$ as ideals in the group ring $R_\infty G$. We show that the dual of a composite $G$-code is again a composite $G$-code in this setting. We extend the known results on projections and lifts of $G$-codes over the finite chain rings and over the formal power series rings to composite $G$-codes. Additionally, we extend some known results on $\gamma$-adic $G$-codes over $R_\infty$ to composite $G$-codes and study these codes over principal ideal rings.

2010 MSC: 94B05, 16S34

Keywords: Composite $G$-codes, Group rings, Finite chain rings, Formal power series rings, $p$-adic integers

1. Introduction

In [11], T. Hurley introduced a map $\sigma$ which sends the group ring element $v \in RG$ to a matrix $\sigma(v)$ over the ring $R$. The author also used this map to construct and study codes over fields. The feature of this map is that for different finite groups in the group ring element $v$, the map $\sigma(v)$ will produce different matrices over the ring $R$. For example in [10], the authors show that if $v \in RD_2$, then the generator matrix of the form $[I_n \mid \sigma(v)]$ produces the well-known four circulant construction used in coding theory.

In [7], the authors apply the above map and study codes generated by $\langle \sigma(v) \rangle$ over the Frobenius rings. They define $G$-codes which are ideals in the group ring $RG$, where $R$ is a finite commutative Frobenius ring and $G$ is a finite group. In [4], the authors study $G$-codes over formal power series rings and finite chain rings. They extend many well known results on codes over $R_i$ and $R_\infty$ to $G$-codes over the same alphabets. The authors also study $\gamma$-adic $G$-codes over $R_\infty$ and $G$-codes over principal ideal rings.
Recently in [3], the authors extended the map $\sigma$ introduced by T. Hurley in [11], so that the group ring element $v$ gets sent to more complex matrices over the ring $R$. The authors denote this map $\Omega$ and call the matrices $\Omega(v)$ the composite matrices—see [3] for details. In [6], the authors introduce and study composite $G$-codes which are defined by taking the row space of the composite matrix $\Omega(v)$, i.e., $\langle \Omega(v) \rangle$. They also extend many results from [4] on $G$-codes to composite $G$-codes.

In this work, we generalize the results on $G$-codes over formal power series rings and finite chain rings $\mathbb{F}_q[t]/(t^i)$ from [4] and some results from [8] to composite $G$-codes over the same alphabets. We study the projections and lifts of composite $G$-codes over the finite chain rings and over the formal power series rings respectively. We also extend the results on $\gamma$-adic $G$-codes over $R_\infty$ to composite $G$-codes and some results on $G$-codes over principal ideal rings to composite $G$-codes. In many parts of this work, the results we present are a simple generalization or a consequence of the results proven in [4] and [8].

The rest of the work is organized as follows. In Section 2, we give preliminary definitions and results on codes, finite chain rings, formal power series and composite $G$-codes. In Section 3, we show that the composite $G$-codes are ideals in the group ring $R_\infty G$. In Section 4, we study the projections and lifts of the composite $G$-codes with a given type. In Sections 5 and 6, we extend the results from [4]; we study self-dual $\gamma$-adic composite $G$-codes and composite $G$-codes over principal ideal rings. We finish with concluding remarks and directions for possible future research.

2. Preliminaries

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. 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.

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

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 $R_\infty$. We refer the reader to [8] and [9] for details and further explanations. In this paper, we assume that all
rings have a multiplicative identity and that all rings are commutative. We also stress that the results we present in this work are given only for finite chain rings \( \mathbb{F}_q[t]/(t^i) \).

### 2.2.1. Finite chain rings

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 \( m \), and let \( \bar{\gamma} \) be the generator of the unique maximal ideal \( m \). This gives that \( m = \langle \bar{\gamma} \rangle = R\bar{\gamma}, \) where \( R\bar{\gamma} = \langle \bar{\gamma} \rangle = \{ \beta \bar{\gamma} \mid \beta \in R \} \). We have the following chain of ideals:

\[
R = \langle \bar{\gamma}^0 \rangle \supseteq \langle \bar{\gamma}^1 \rangle \supseteq \cdots \supseteq \langle \bar{\gamma}^i \rangle \supseteq \cdots. \tag{1}
\]

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

\[
R = \langle \bar{\gamma}^0 \rangle \supseteq \langle \bar{\gamma}^1 \rangle \supseteq \cdots \supseteq \langle \bar{\gamma}^e \rangle. \tag{2}
\]

If the ring \( R \) is infinite then the chain in Equation 1 is also infinite.

Let \( R^\times \) denote the multiplicative group of all units in the ring \( R \). Let \( \mathbb{F} = R/m = R/\langle \bar{\gamma} \rangle \) 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 [12].

**Lemma 2.2.** For any \( 0 \neq r \in R \) there is a unique integer \( i \), \( 0 \leq i < e \) such that \( r = \mu \bar{\gamma}^i \), with \( \nu \) a unit. The unit \( \mu \) is unique modulo \( \bar{\gamma}^{e-1} \).

**Lemma 2.3.** Let \( R \) be a finite chain ring with maximal ideal \( m = \langle \bar{\gamma} \rangle \), where \( \bar{\gamma} \) is a generator of \( m \) with nilpotency index \( e \). Let \( V \subseteq R \) be a set of representatives for the equivalence classes of \( R \) under congruence modulo \( \bar{\gamma} \). Then

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

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

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

From Lemma 2.3, we know that any element \( \bar{a} \) of \( R \) can be written uniquely as

\[
\bar{a} = a_0 + a_1 \bar{\gamma} + \cdots + a_{e-1} \bar{\gamma}^{e-1},
\]

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

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

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

where \( e \) is the nilpotency index of \( \gamma \). This matrix \( G \) is called the standard generator matrix form for the code \( C \). In this case, the code \( C \) is said to have type

\[
1^{k_0} \gamma^{k_1} (\gamma^2)^{k_2} \cdots (\gamma^{e-1})^{k_{e-1}}. \tag{4}
\]
2.2.2. Formal power series rings

In the next definitions, which can be found in [8], \( \gamma \) will indicate the generator of the ideal of a chain ring, not necessarily the maximal ideal.

**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:

\[
\sum_{i=0}^{i-1} a_i \gamma^i + \sum_{i=0}^{i-1} b_i \gamma^i = \sum_{i=0}^{i-1} (a_i + b_i) \gamma^i \quad (5)
\]

\[
\sum_{i=0}^{i-1} a_i \gamma^i \cdot \sum_{i=0}^{i-1} b_i \gamma^i = \sum_{s=0}^{i-1} \left( \sum_{i+j=s} a_i b_j \right) \gamma^s. \quad (6)
\]

The following results can be found in [8].

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.

Let \( C \) be a finitely generated linear code over \( R_\infty \). Then the generator matrix of code \( C \) is permutation equivalent to the following standard form generator matrix.

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:

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

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 7 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 we write by \( \dim C = k \).
Let $i, j$ be two integers with $i \leq j$, we define a map
\[ \Psi_{ji} : R_j \to R_i, \]
\[ \sum_{l=0}^{j-1} a_l \gamma^l \mapsto \sum_{l=0}^{i-1} a_l \gamma^l. \] 

If we replace $R_j$ with $R_\infty$ then we obtain a map $\Psi_{i\infty}$. For convenience, we denote it by $\Psi_i$. It is easy to get that $\Psi_{ji}$ and $\Psi_i$ are ring homomorphisms. Let $a, b$ be two arbitrary elements in $R_j$. It is easy to get that
\[ \Psi_{ji}(a + b) = \Psi_{ji}(a) + \Psi_{ji}(b), \]
\[ \Psi_{ji}(ab) = \Psi_{ji}(a)\Psi_{ji}(b). \] 

If $a, b \in R_\infty$, we have that
\[ \Psi_i(a + b) = \Psi_i(a) + \Psi_i(b), \]
\[ \Psi_i(ab) = \Psi_i(a)\Psi_i(b). \] 

Note that the map $\Psi_{ji}$ and $\Psi_i$ can be extended naturally from $R^n_j$ to $R^n_i$ and $R_\infty^n$ to $R^n_\infty$.

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:
\[
\begin{array}{ccc}
R & \parallel & R_\infty \\
R_\infty & \rightarrow & \cdots & \rightarrow & R_e & \rightarrow & R_{e-1} & \rightarrow & \cdots & \rightarrow & R_1 \\
\end{array}
\]

2.3. Composite $G$-codes

In this section, we define a circulant matrix, give the definitions for group rings and introduce composite $G$-codes.

A circulant matrix is one where each row is shifted one element to the right relative to the preceding row. We label the circulant matrix as $A = \text{circ}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, where $\alpha_i$ are ring elements.

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
\[ \sum_{i=1}^{n} \alpha_i g_i + \sum_{i=1}^{n} \beta_i g_i = \sum_{i=1}^{n} (\alpha_i + \beta_i) g_i. \]

The product of two elements in a group ring is given by
\[ (\sum_{i=1}^{n} \alpha_i g_i)(\sum_{j=1}^{n} \beta_j g_j) = \sum_{i,j} \alpha_i \beta_j g_i g_j. \]

It follows that the coefficient of $g_k$ in the product is $\sum_{i,j} g_{ij} g_k$. 

The following matrix construction was first introduced in [3]. In [6], the authors have shown that the same construction produces codes in $R^n$ from elements in the group ring $RG$.

Let $\{g_1, g_2, \ldots, g_n\}$ be a fixed listing of the elements of $G$. Let $\{h_1, h_2, \ldots, h_r\}$ be a fixed listing of the elements of $H$, where $H$ is a group of order $r$. Here, let $r$ be a factor of $n$ with $n > r$ and $n,r \neq 1$.

Also, let $G_r$ be a subset of $G$ containing $r$ distinct elements of $G$. Define the map:
where at least one block has the following form:

$$A_l' = \begin{pmatrix}
\alpha_{g_j^{-1}g_k} & \alpha_{g_j^{-1}g_{k+1}} & \ldots & \alpha_{g_j^{-1}g_{k+(r-1)}} \\
\alpha_{\phi_1((h_l)_{2z-1}^z h_l)_{2z-1}} & \alpha_{\phi_1((h_l)_{2z-1}^z h_l)_{2z-2}} & \ldots & \alpha_{\phi_1((h_l)_{2z-1}^z h_l)_{2z-1}} \\
\vdots & \vdots & \ddots & \vdots \\
\alpha_{\phi_1((h_l)_{2z-1}^z h_l)_{2z-1}} & \alpha_{\phi_1((h_l)_{2z-1}^z h_l)_{2z-2}} & \ldots & \alpha_{\phi_1((h_l)_{2z-1}^z h_l)_{2z-1}} \\
\end{pmatrix},$$

and the other blocks are of the form:

$$A_l = \begin{pmatrix}
\alpha_{g_j^{-1}g_k} & \alpha_{g_j^{-1}g_{k+1}} & \ldots & \alpha_{g_j^{-1}g_{k+(r-1)}} \\
\alpha_{g_{j+1}^{-1}g_k} & \alpha_{g_{j+1}^{-1}g_{k+1}} & \ldots & \alpha_{g_{j+1}^{-1}g_{k+(r-1)}} \\
\vdots & \vdots & \ddots & \vdots \\
\alpha_{g_{j+r-1}^{-1}g_k} & \alpha_{g_{j+r-1}^{-1}g_{k+1}} & \ldots & \alpha_{g_{j+r-1}^{-1}g_{k+(r-1)}} \\
\end{pmatrix},$$

where \( l = \{1, 2, 3, \ldots, \frac{n^2}{2}\} \) and where:

$$\phi_r : H_r \rightarrow G_r,$$

\((h_i)_1 \xrightarrow{\phi_l} g_j^{-1}g_k,
(h_i)_2 \xrightarrow{\phi_l} g_j^{-1}g_{k+1},
\ldots
(h_i)_r \xrightarrow{\phi_l} g_j^{-1}g_{k+(r-1)}.
$$

Here we notice that when when \( l = 1 \) then \( j = 1, k = 1 \), when \( l = 2 \) then \( j = 1, k = r + 1 \), when \( l = 3 \) then \( j = 1, k = 2r + 1, \ldots \) when \( l = \frac{n^2}{2} \) then \( j = 1, k = n - r + 1 \). When \( l = \frac{n^2}{2} + 1 \) then \( j = r + 1, k = 1 \), when \( l = \frac{n^2}{2} + 2 \) then \( j = r + 1, k = r + 1 \), when \( l = \frac{n^2}{2} + 3 \) then \( j = r + 1, k = 2r + 1, \ldots \) when \( l = \frac{2n^2}{r} \) then \( j = r + 1, k = n - r + 1, \ldots \), and so on.

In [6], it is shown that the matrix \( \Omega(v) \) can be written as:

$$\Omega(v) = \begin{pmatrix}
\alpha_{g_{j_1}^{-1}g_1} & \alpha_{g_{j_2}^{-1}g_2} & \alpha_{g_{j_3}^{-1}g_3} & \ldots & \alpha_{g_{j_n}^{-1}g_n} \\
\alpha_{g_{j_1}^{-1}g_2} & \alpha_{g_{j_2}^{-1}g_2} & \alpha_{g_{j_3}^{-1}g_3} & \ldots & \alpha_{g_{j_n}^{-1}g_n} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\alpha_{g_{j_1}^{-1}g_n} & \alpha_{g_{j_2}^{-1}g_n} & \alpha_{g_{j_3}^{-1}g_n} & \ldots & \alpha_{g_{j_n}^{-1}g_n} \\
\end{pmatrix}.$$
where $g_j^{-1}$ are simply the elements of the group $G$. These elements are determined by how the matrix has been partitioned, what groups $H_i$ of order $r$ have been employed and how the maps $\phi_j$ have been defined to form the composite matrix. This representation of the composite matrix $\Omega(v)$ will make it easier to prove the upcoming results.

For a given element $v \in RG$ and some groups $H_i$ of order $r$, we define the following code over the ring $R$:

$$
\mathcal{C}(v) = \langle \Omega(v) \rangle.
$$

The code is formed by taking the row space of $\Omega(v)$ over the ring $R$. The code $\mathcal{C}(v)$ is a linear code over the ring $R$, since it is the row space of a generator matrix. It is not possible to determine the size of the code immediately from the matrix. In [6], 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 composite $G$-codes.

We note that the matrix $\Omega(v)$ is an extension of the matrix $\sigma(v)$ defined in [11]. Also, in [6], the authors show when the matrices $\Omega(v)$ are inequivalent to the matrices obtained from $\sigma(v)$. This is one reason to study codes constructed from $\Omega(v)$- this technique can produce codes which cannot be obtained from codes constructed from $\sigma(v)$ or other classical techniques. For example, please see [5] where many new binary self-dual codes are constructed via the composite matrices.

## 3. Composite $G$-codes and ideals in the group ring $R_\infty G$

In this section, we show that the composite $G$-codes are ideals in the group ring $R_\infty G$ and that the dual of the composite $G$-code is also a composite $G$-code in this setting. These two results are a simple generalization of Theorem 3.1 and Theorem 3.2 from [4]. We use the same arguments as in [4] to prove our results.

For simplicity, we write each non-zero element in $R_\infty$ in the form $\gamma^i a$ where $a = a_0 + a_1 \gamma + \cdots + \cdots$ with $a_0 \neq 0$ and $i \geq 0$, which means that $a$ is a unit in $R_\infty$.

We note that if $v = \gamma^{s_1} a_{g_{j_1}} g_1 + \gamma^{s_2} a_{g_{j_2}} g_2 + \cdots + \gamma^{s_n} a_{g_{j_n}} g_n \in R_\infty G$, then each row of $\Omega(v)$ corresponds to an element in $R_\infty G$ of the following form:

$$
v_j^* = \sum_{i=1}^{n} \gamma^{s_{i,j_i}} a_{g_{j_i}} g_{j_i},
$$

where $\gamma^{s_{i,j_i}} a_{g_{j_i}} \in R_\infty$, $g_{j_i}, g_{j_i} \in G$ and $j$ is the $j$th row of the matrix $\Omega(v)$. In other words, we can define the composite matrix $\Omega(v)$ as:

$$
\Omega(v) = \\
\begin{pmatrix}
\gamma^{s_{1,j_1}} a_{g_{j_1}} g_1 & \gamma^{s_{2,j_1}} a_{g_{j_1}} g_1 & \gamma^{s_{3,j_1}} a_{g_{j_1}} g_1 & \cdots & \gamma^{s_{n,j_1}} a_{g_{j_1}} g_n \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\gamma^{s_{1,j_n}} a_{g_{j_n}} g_1 & \gamma^{s_{2,j_n}} a_{g_{j_n}} g_1 & \gamma^{s_{3,j_n}} a_{g_{j_n}} g_1 & \cdots & \gamma^{s_{n,j_n}} a_{g_{j_n}} g_n \\
\end{pmatrix}
$$

where the elements $g_{j_i}$ are simply the group elements $G$. Which elements of $G$ these are, depends how the composite matrix is defined, i.e., what groups we employ and how we define the $\phi_i$ map in individual blocks. Then we take the row space of the matrix $\Omega(v)$ over $R_\infty$ to get the corresponding composite $G$-code, namely $\mathcal{C}(v)$. 


Theorem 3.1. Let \( R_\infty \) be the formal power series ring and \( G \) a finite group of order \( n \). Let \( H_i \) be finite groups of order \( r \) such that \( r \) is a factor of \( n \) with \( n > r \) and \( n, r \neq 1 \). Also, let \( v \in R_\infty G \) and let \( \mathcal{C}(v) = (\Omega(v)) \) be the corresponding code in \( R_\infty^\infty \). Let \( I(v) \) be the set of elements of \( R_\infty G \) such that \( \sum \gamma^i a_i g_i \in I(v) \) if and only if \( (\gamma^i a_1, \gamma^i a_2, \ldots, \gamma^i a_n) \in \mathcal{C}(v) \). Then \( I(v) \) is a left ideal in \( R_\infty G \).

Proof. We saw above that the rows of \( \Omega(v) \) consist precisely of the vectors that correspond to the elements of the form \( v^*_i = \sum_{i=1}^n \gamma^i a_i g_i, g_i, g_i, g_i \in R_\infty G \), where \( \gamma^i a_i, a_{g_i, g_i} \in R_\infty, g_i, g_i, g_i \in G \) and \( j \) is the \( j \)-th row of the matrix \( \Omega(v) \). Let \( a = \sum \gamma^i a_i g_i \) and \( b = \sum \gamma^i b_i g_i \) be two elements in \( I(v) \), then \( a + b = \sum (\gamma^i a_i + \gamma^i b_i) g_i \), which corresponds to the sum of the corresponding elements in \( \mathcal{C}(v) \). This implies that \( I(v) \) is closed under addition.

Let \( w_1 = \sum \gamma^i b_i g_i \in R_\infty G \). Then if \( w_2 \) corresponds to a vector in \( \mathcal{C}(v) \), it is of the form \( \sum (\gamma^j a_j) v^*_j \). Then \( w_1 w_2 = \sum \gamma^i b_i g_i \sum (\gamma^j a_j) v^*_j = \sum \gamma^i b_i \gamma^j a_j g_i v^*_j \) 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 \( R_\infty G \).

Next we show that the dual of a composite \( G \)-code is also a composite \( G \)-code.

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 follows that \( \mathcal{R}(I) \) is an ideal of \( R_\infty G \).

Let \( v = \gamma^i a_i g_i, g_i + \gamma^i a_i g_i + \cdots + \gamma^i a_i g_i \in R_\infty G \) and \( \mathcal{C}(v) \) be the corresponding code. Let \( \Omega : R_\infty G \to R_\infty^\infty \) be the canonical map that sends \( \gamma^i a_i g_i, g_i + \gamma^i a_i g_i + \cdots + \gamma^i a_i g_i \) to \( (\gamma^i, a_i, g_i, g_i, \ldots, \gamma^i, a_i, g_i) \). Let \( I \) be the ideal \( \Omega^{-1}(\mathcal{C}) \). Let \( w = (w_1, w_2, \ldots, w_n) \in \mathcal{C}^1 \). Then the operator of product between any row of \( \Omega(v) \) and \( w \) is zero:

\[
[(\gamma^i a_i g_i, \gamma^i a_i g_i, \ldots, \gamma^i a_i g_i), (w_1, w_2, \ldots, w_n)] = 0, \forall j.
\] (18)

Which gives

\[
\sum_{i=1}^n \gamma^i a_i g_i w_i = 0, \forall j.
\] (19)

Let \( w = \Omega^{-1}(w) = \sum \gamma^i a_i g_i \) and define \( w \in R_\infty G \) to be \( w = \gamma^i a_i g_i + \gamma^i a_i g_i + \cdots + \gamma^i a_i g_i \), where

\[
\gamma^i a_i g_i = \gamma^i a_i g_i w_i^{-1}.
\] (20)

Then

\[
\sum_{i=1}^n \gamma^i a_i g_i w_i = 0 \Rightarrow \sum_{i=1}^n \gamma^i a_i g_i \gamma^i a_i g_i w_i^{-1} = 0.
\] (21)

Here, \( j, g_i, g_i^{-1} = g_i \), thus this is the coefficient of \( g_i \) in the product of \( w \) and \( v^*_j \), where \( v^*_j \) is any row of the matrix \( \Omega(v) \). This gives that \( w \in \mathcal{R}(I) \) if and only if \( w \in \mathcal{C}^1 \).

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

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 \( \Omega^{-1}(\mathcal{C}) \) is an ideal of \( R_\infty G \).

Proof. The composite mapping \( \Omega(\phi(\mathcal{C})) \) is permutation equivalent to \( \mathcal{C}^1 \) and \( \phi(\mathcal{C}^1) \) is an ideal of \( R_\infty G \). We know that \( \phi \) is a bijection between \( \mathcal{C}^1 \) 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 composite \( G \)-code is also a composite \( G \)-code over the formal power series ring. \]
4. Projections and lifts of composite $G$-codes

In this section, we extend more results from [4]. In fact, many of the results presented in this section are a consequence of the results proven in [8] and a simple generalization of the results proven in [4].

We first show that if $v \in R_{\infty}G$ then $\Omega(v)$ is permutation equivalent to the matrix defined in Equation 7. For simplicity, we write each non-zero element in $R_{\infty}$ in the form $\gamma^a$ where $a = a_0 + a_1 \gamma + \cdots$ with $a_0 \neq 0$ and $i \geq 0$, which means that $a$ is a unit in $R_{\infty}$.

**Theorem 4.1.** Let $v = \gamma^{i_1}a_{g_1}g_1 + \gamma^{i_2}a_{g_2}g_2 + \cdots + \gamma^{i_n}a_{g_n}g_n \in R_{\infty}G$, where $a_{g_i}$ are units in $R_{\infty}$. Let $C$ be a finitely generated code over $R_{\infty}$. Then

$$\Omega(v) = \begin{pmatrix}
\gamma^{i_1}a_{g_1}g_1 & \gamma^{i_2}a_{g_2}g_2 & \cdots & \gamma^{i_n}a_{g_n}g_n \\
\vdots & \vdots & \ddots & \vdots \\
\gamma^{i_{n-1}}a_{g_{n-1}}g_{n-1} & \gamma^{i_n}a_{g_n}g_n
\end{pmatrix},$$

is permutation equivalent to the standard generator matrix given in Equation 7.

**Proof.** Take one non-zero element of the form $\gamma^{m_0}a_{g_i}$, where $m_0$ is the minimal non-negative 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 $\Omega(v)$ can be replaced by $\gamma^{m_0}a$. The elements in the first column of matrix $\Omega(v)$ have the form $\gamma^{i_j}a_{g_i}$ with $i_j \geq m_0$ and $a_{g_i}$ a unit, thus, these can be replaced by zero when they are added to the first row multiplied by $-\gamma^{i_j-m_0}(a_{g_i})^{-1}$. Continuing the process using elementary operations, we obtain the standard generator matrix of the code $C$ given in Equation 7. \qed

**Example 4.2.** Let $G = \langle x, y \mid x^2 = 1, y^2 = x^2, xy^{-1} = x^{-1} \rangle \cong Q_8$. Let $v = \sum_{i=0}^{3} (\alpha_i + 1)x^i + \alpha_i + 5x^i y \in R_{\infty}Q_8$, where $\alpha_i = a_{g_i} \in R_{\infty}$. Let $H_1 = \langle a, b \mid a^2 = b^2 = 1, ab = ba \rangle \cong C_2 \times C_2$. We now define the composite matrix as:

$$\Omega(v) = \begin{pmatrix}
A_1 & A_2 \\
A_3 & A_4
\end{pmatrix} =
\begin{pmatrix}
\begin{pmatrix}
\alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\
\alpha_{g_1} & \alpha_{g_2} & \alpha_{g_3} & \alpha_{g_4}
\end{pmatrix} &
\begin{pmatrix}
\alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\
\alpha_{g_1} & \alpha_{g_2} & \alpha_{g_3} & \alpha_{g_4}
\end{pmatrix} \\
\begin{pmatrix}
\alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\
\alpha_{g_1} & \alpha_{g_2} & \alpha_{g_3} & \alpha_{g_4}
\end{pmatrix} &
\begin{pmatrix}
\alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\
\alpha_{g_1} & \alpha_{g_2} & \alpha_{g_3} & \alpha_{g_4}
\end{pmatrix}
\end{pmatrix},
$$

where:

$$\phi_1: (h_1) \rightarrow g_{i^1}^{-1}g_i, \quad \phi_4: (h_1) \rightarrow g_{i^4}^{-1}g_j,$$

for $i = \{1, 2, 3, 4\}$ and for when $i = 1, \ldots, 4$ and $j = i + 4$.

in $A'_1$ and $A'_4$ respectively. This results in a composite matrix over $R_{\infty}$ of the following form:
Proposition 4.3. Let $C$ be a composite $G$-code over $R_\infty$ of type

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

with generator matrix $\Omega(v)$. The code generated by $\Psi_i(\Omega(v))$ is a code over $R_i$ of type $\{ (\gamma^{m_0})^k, (\gamma^{m_1})^{k_1}, \ldots, (\gamma^{m_{r-1}})^{k_{r-1}} \}$ where $m_s$ is the largest $m_i$ that is less than $e$. Also, the code generated by $\Psi_i(\Omega(v))$ is equal to

$$\{ (\Psi_i(c_1), \Psi_i(c_2), \ldots, \Psi_i(c_n)) \mid (c_1, c_2, \ldots, c_n) \in C \}. \quad (22)$$

Proof. If $m_i > e - 1$ then $\Psi_i$ sends $\gamma^{m_i}M'$, where $M'$ is a matrix, to a zero matrix which gives the first part.

The code $C$ is formed by taking the row space of $\Omega(v)$ over the ring $R_\infty$, 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 $v_i$ are the rows of $\Omega(v)$. If $w = \gamma^{l_j}a_jv_j$, then $\Psi_i(w) = \Psi_i(\gamma^{l_i}a_i)\Psi_i(v_i)$ by the equation given in (11) where $\Psi_i(v_i)$ applies the map coordinate-wise. This gives the second part.

Since a composite $G$-code over $R_\infty$ is a linear code, the following results are a direct consequence of some results proven in [8]. We omit the proofs.

Lemma 4.4. Let $C$ be a composite $G$-code of length $n$ over $R_\infty$, then,

$$\Omega(v) = \begin{pmatrix} X_1 & Y_1 & X_2 \\ Y_1 & X_1 & Y_2 \\ X_3 & Y_4 & X_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 \\ a_2 & a_1 & a_4 & a_3 & a_8 & a_5 & a_6 & a_7 \\ a_3 & a_4 & a_1 & a_2 & a_7 & a_8 & a_5 & a_6 \\ a_4 & a_3 & a_2 & a_1 & a_6 & a_7 & a_8 & a_5 \\ a_5 & a_4 & a_3 & a_2 & a_6 & a_7 & a_8 & a_5 \\ a_6 & a_5 & a_4 & a_3 & a_2 & a_6 & a_7 & a_8 \\ a_6 & a_5 & a_3 & a_2 & a_6 & a_7 & a_8 & a_5 \end{pmatrix}. $$

If we let $v = \gamma^2x^3 + \gamma^2(1 + \gamma)xy + \gamma^2(1 + \gamma + \gamma^2)x^2y + \gamma^2x^3y \in R_\infty Q_8$, where $(x, y) \equiv Q_8$, then

$$C(v) = \langle \Omega(v) \rangle = \begin{pmatrix} 0 & 0 & 0 & \gamma^2 & 0 & \gamma^2(1 + \gamma) & \gamma^2(1 + \gamma + \gamma^2) & \gamma^2 \\ 0 & \gamma^2 & 0 & \gamma^2 & 0 & \gamma^2(1 + \gamma) & \gamma^2 & 0 \\ \gamma^2(1 + \gamma + \gamma^2) & \gamma^2(1 + \gamma) & 0 & \gamma^2 & 0 & 0 & \gamma^2 & 0 \\ \gamma^2 & \gamma^2(1 + \gamma + \gamma^2) & \gamma^2(1 + \gamma) & 0 & \gamma^2 & 0 & 0 & \gamma^2 \\ \gamma^2 & \gamma^2(1 + \gamma) & 0 & \gamma^2 & 0 & 0 & \gamma^2 & 0 \\ \gamma^2 & \gamma^2 & 0 & \gamma^2 & 0 & 0 & \gamma^2 & 0 \end{pmatrix}. $$

and $C(v)$ is equivalent to

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

Clearly $C(v) = \langle \Omega(v) \rangle$ is the $[8, 4, 4]$ extended Hamming code.
Example 4.5. If we take the generator matrix which is the standard generator matrix—here, in this case the generator matrix of the dual code thus

Let Proposition 4.6. We also have

orthogonal composite

This gives that

Ψ

Hence

Ψ

taking

Ψ
then

(3) If C has a standard generator matrix G as in equation (7), then we have

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

\[ H = \begin{pmatrix} B_{0,r} & B_{0,r-1} & \cdots & B_{0,2} & B_{0,1} & I_{k_r} \end{pmatrix}, \]

where \( B_{0,j} = -\sum_{i=1}^{j-1} B_{0,i} A_{i,j-r-i}^T - A_{r-j,r}^T \) for all \( 1 \leq j \leq r; \)

(ii) \( \text{rank}(C) + \text{rank}(C⊥) = n. \)

Example 4.5. If we take the generator matrix G of a code C from Example 1, we can see that

\[
G = \gamma^2 \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \gamma^2 \begin{pmatrix} 0 & 1 + \gamma & 1 + \gamma + \gamma^2 & 1 \\ 1 & 0 & 1 + \gamma & 1 + \gamma + \gamma^2 \\ 1 + \gamma + \gamma^2 & 1 & 0 & 1 + \gamma \\ 1 + \gamma & 1 + \gamma + \gamma^2 & 1 & 0 \end{pmatrix},
\]

which is the standard generator matrix—here,

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

In this case the generator matrix of the dual code C⊥ of C has the form:

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

Now,

\[ B_{0,1} = -A_{0,1}^T, \]

thus

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

We also have

\[ \text{rank}(C) + \text{rank}(C⊥) = 4 + 4 = 8 = n. \]

Proposition 4.6. Let C be a self-orthogonal composite G-code over \( R_\infty \). Then the code \( \Psi_i(C) \) is a self-orthogonal composite G-code over \( R_\infty \) for all \( i < \infty \).

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

\[
\sum_{i=1}^{n} v_i w_i = \sum_{i=1}^{n} \Psi_i(v_i) \Psi_i(w_i) (\text{mod } \gamma^i) = \Psi_i([v, w]) (\text{mod } \gamma^i) \equiv 0 \text{ (mod } \gamma^i). \]

Hence \( \Psi_i(C) \) is a self-orthogonal code over \( R_\infty \). To show that \( \Psi_i(C) \) is also a G-code, we notice that when taking \( \Psi_i(C) = \Psi_i(\langle \Omega(v) \rangle) \), it corresponds to \( \Psi_i(v) = \Psi_i(\gamma^{a_1} a_{g_1}) g_1 + \Psi_i(\gamma^{a_2} a_{g_2}) g_2 + \cdots + \Psi_i(\gamma^{a_n} a_{g_n}) g_n \), then \( \Psi_i(C) \in R_\infty G \). Thus \( \Psi_i(C) \) is also a composite G-code. \(\square\)
Definition 4.7. 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 \( C_1 \preceq C_2 \), if \( C_2 \) has a generator matrix \( G_2 \) such that \( \Psi_1(G_2) \) is a generator matrix of \( C_1 \). We also denote \( C_1 \) by \( \Psi_1(C_2) \). 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 4.8. Let \( C \) be a composite \( G \)-code over \( R_\infty \) with type \( 1^k \). If \( \Omega(v) \) is a standard form of \( C \), then for any positive integer \( i \), \( \Psi_i(\Omega(v)) \) is a standard form of \( \Psi_i(C) \).

Proof. We know from Theorem 4.1 that \( \Omega(v) \) is permutation equivalent to a standard form matrix defined in Equation 7. 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 [8].

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 \( v_\infty = \gamma^i a_g \gamma^i g_1 + \gamma^i a_g \gamma^i g_2 + \cdots + \gamma^i a_g \gamma^i g_n \in R_\infty G \), and \( C(v_\infty) = \langle \Omega(v_\infty) \rangle \) be the corresponding composite \( G \)-code. Define the following map:

\[
\Omega_1 : R_\infty G \rightarrow C(v_\infty),
\]

\[
(\gamma^i a_g \gamma^i g_1 + \gamma^i a_g \gamma^i g_2 + \cdots + \gamma^i a_g \gamma^i g_n) \mapsto M(R_\infty G, v_\infty).
\]

We define a projection of composite \( G \)-codes over \( R_\infty G \) to \( R_i G \).

Let

\[
\Psi_i : R_\infty G \rightarrow R_i G \tag{24}
\]

\[
\gamma^i a \mapsto \Psi_i(\gamma^i a). \tag{25}
\]

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:

\[
\begin{array}{ccc}
R_\infty G & \xrightarrow{\Omega_1} & C(v_\infty) \\
\Psi_i \downarrow & & \downarrow \Psi_i \\
R_i G & \xrightarrow{\Omega_i} & C(v)
\end{array}
\]

This gives that \( \Omega_i \Omega_1 = \Omega_1 \Psi_i \), which gives the following theorem.

Theorem 4.9. If \( C \) is a composite \( G \)-code over \( R_\infty \), then \( \Psi_i(C) \) is a composite \( G \)-code over \( R_i \) for all \( i < \infty \).

Proof. Let \( v_\infty \in R_\infty G \) and \( C(v_\infty) \) be the corresponding composite \( G \)-code over \( R_\infty \). Then \( \Omega_1(v_\infty) = C(v_\infty) \) is an ideal of \( R_\infty G \). By the homomorphism in Equation 24 and the commutative diagram above, we know that \( \Omega_1(C(v_\infty)) = \Omega_1(\Psi_i(v_\infty)) \) is an ideal of the group ring \( R_i G \). This implies that \( \Psi_i(C) \) is a composite \( G \)-code over \( R_i \) for all \( i < \infty \).

Theorem 4.10. Let \( C \) be a composite \( G \)-code over \( R_i \), then the lift of \( C \), \( \tilde{C} \) over \( R_j \), where \( j > i \), is also a composite \( G \)-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 \( C = \langle \Omega(v_1) \rangle \) be the corresponding composite \( G \)-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 \( \tilde{C} = \langle \Omega(v_2) \rangle \) be the corresponding composite \( G \)-code. We can say that \( v_1 \) and \( v_2 \) act as generators of \( C \) and \( \tilde{C} \) respectively. We can clearly see that we can have \( \Psi_i(v_2) = \Psi_i(\beta_{g_1}) g_1 + \Psi_i(\beta_{g_2}) g_2 + \cdots + \Psi_i(\beta_{g_n}) g_n = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \cdots + \alpha_{g_n} g_n \in R_i G \), thus \( \Psi_i(v_2) \) is a generator matrix of \( \tilde{C} \). This implies that the composite \( G \)-code \( C(v_1) \) over \( R_i \) lifts to a composite \( G \)-code over \( R_j \), for all \( j > i \).
The following results consider composite \( G \)-codes over chain rings that are projections of \( \gamma \)-adic codes. The results are just a simple consequence of the results proven in [8]. For details on notation and proofs, please refer to [8] and [4].

**Lemma 4.11.** Let \( C \) be a \([n, k] \) composite \( G \)-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. 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) \( \mathbf{v} = \gamma^i \mathbf{v}_0 \in C^j \) if and only if \( \mathbf{v}_0 \in C^{j-i} \);

(v) \( \ker(\Psi^i \gamma^i) = \gamma^i C^{j-i} \).

**Theorem 4.12.** Let \( C \) be a composite \( G \)-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 \( d = d_H(C^1) \).

The final two results we present in this section are a simple extension of the two results from [8] on MDS and MDR codes over \( R_\infty \). We omit the proofs since a composite \( G \)-code over \( R_\infty \) is a linear code and for that fact, the proofs are the same as in [8].

**Theorem 4.13.** Let \( C \) be a composite \( G \)-code over \( R_\infty \). If \( C \) is an MDR or MDS code then \( C^\perp \) is an MDS code.

**Theorem 4.14.** Let \( C \) be a composite \( G \)-code over \( R_i \), and \( \tilde{C} \) be a lift 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 \( R_j \).

5. **Self-dual \( \gamma \)-adic composite \( G \)-codes**

In this section, we extend some results for self-dual \( \gamma \)-adic codes to composite \( G \)-codes over \( R_\infty \). As in previous sections, the results presented here are just a simple generalization of the results proven in [8] and [4].

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 generalize four theorems from [8]. The first two consider self-dual codes over \( R_i \) with a specific type and projections of self-dual codes over \( R_\infty \) respectively. The third one considers a method for constructing self-dual codes over \( \mathbb{F} \) from a self-dual code over \( R_i \). We extend these to self-dual composite \( G \)-codes over \( R_i \) and \( R_\infty \) respectively.

**Theorem 5.1.** Let \( i \) be odd and \( C \) be a composite \( G \)-code over \( R_i \) with type \( 1^{k_0}(\gamma^{k_1})^{k_2}(\gamma^{2})^{k_2} \cdots (\gamma^{j-1})^{k_{j-1}} \). 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 \( \Omega(v) \) where \( v \in R_i G \) and \( G \) is a finite group, is permutation equivalent to the matrix (3). The rest of the proof is the same as in [8].
Theorem 5.2. If $C$ is a self-dual composite $G$-code of length $n$ over $R_\infty$ then $\Psi_i(C)$ is a self-dual composite $G$-code of length $n$ over $R_i$ for all $i < \infty$.

Proof. This is a direct consequence of Theorem 3.4 in [8] and Proposition 4.4 of this work.

Theorem 5.3. Let $i$ be odd. A self-dual composite $G$-code of length $n$ over $R_i$ induces a self-dual composite $G$-code of length $n$ over $\mathbb{F}_q$.

Proof. The first part of the proof is identical to the one of Theorem 5.5 from [4]. Secondly, when the map $\Psi_i(\tilde{G})$ is used in [8], we notice that in our case the map will correspond to $\Psi_i(v) = \Psi_i(\gamma a_g)g_1 + \cdots + \Psi_i(\gamma a_g)g_n$, assuming that $\tilde{G}$ is the generator matrix of a composite $G$-code.

Theorem 5.4. Let $R = R_\infty$ 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 composite $G$-code $\mathbb{C}$ over $\mathbb{F}$ can be lifted to a self-dual composite $G$-code over $R_\infty$.

Proof. From Theorem 4.10 we know that a composite $G$-code over $R_i$ can be lifted to a composite $G$-code over $R_j$, where $j > i$. To show that a self-dual composite $G$-code over $\mathbb{F}$ lifts to a self-dual composite $G$-code over $R_\infty$, it is enough to follow the proof in [8].

6. Composite $G$-codes over principal ideal rings

In this section, we study composite $G$-codes over principal ideal rings. We study codes over this class of rings by the generalized Chinese Remainder Theorem. Please see [2] for more details on the notation and definitions of the principal ideal rings.

Let $R_{e_1}^1, R_{e_2}^1, \ldots, R_{e_s}^n$ be chain rings, where $R_{e_j}^1$ has unique maximal ideal $\langle \gamma_j \rangle$ and the nilpotency index of $\gamma_j$ is $e_j$. Let $A = \text{CRT}(R_{e_1}^1, \ldots, R_{e_s}^n)$.

We know that $A$ is a principal ideal ring. For any $1 \leq i < \infty$, let $A_i = \text{CRT}(R_{e_1}^1, \ldots, R_i^1, \ldots, R_{e_s}^n)$. This gives that all the rings $A_i$ are principal ideal rings. In particular, $A_\infty = A$. We denote $\text{CRT}(R_{e_1}^1, \ldots, R_{e_s}^n)$ by $A_{e_s}^n$.

For $1 \leq i < \infty$, let $C_i^1$ be a code over $R_i^1$. Let

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

be the associated code over $A_i$. Let

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

be associated code over $A_{e_s}^n$. We can now prove the following.

Theorem 6.1. Let $C_i^1$ be a composite $G$-code over the chain ring $R_i^1$ that is $C_i^1$ is an ideal in $R_{e_j}G$. Then $C_{e_s}^n = \text{CRT}(C_{e_1}^1, \ldots, C_{e_s}^n)$ is a composite $G$-code over $A_{e_s}^n$.

Proof. Let $v_j \in C_j^1$, we know that $v_j$ also belongs to $C_j^1$ where $v_j$ has the form defined in (16). Let $v \in C_{e_s}^n$. Now if $v = \text{CRT}(v_1, v_2, \ldots, v_s)$, then $v^* = \text{CRT}(v_1^*, v_2^*, \ldots, v_s^*)$ and so $v^* \in C_{e_s}^n$ giving that $C_{e_s}^n$ is an ideal in $A_{e_s}^nG$, and thus giving that $C_{e_s}^n$ is a composite $G$-code over $A_{e_s}^n$.
7. Conclusion

In this work, we generalized the known results on $G$-codes over the formal power series rings and finite chain rings $\mathbb{F}_q[[t]]/(t^i)$ to composite $G$-codes over the same alphabets. We showed that the dual of a composite $G$-code is also a composite $G$-code and we studied the projections and lifts of the composite $G$-codes with a given type in this setting. We extended many theoretical results on $\gamma$-adic $G$-codes and $G$-codes over principal ideal rings to composite $\gamma$-adic $G$-codes and composite $G$-codes over principal ideal rings. Since the results presented in this paper and in [4] only consider the finite chain rings $\mathbb{F}_q[[t]]/(t^i)$, it is suggested that for future research, these families of codes; $G$-Codes and composite $G$-Codes, are studied over a more general finite chain rings as it was done using a unified treatment in [1].

References

[1] R. L. Bouzara, K. Guenda, E. Martinez-Moro, Lifted codes and lattices from codes over finite chain rings, arXiv:2007.05871.
[2] S. T. Dougherty, Algebraic coding theory over finite commutative rings, SpringerBriefs in Mathematics Springer (2017).
[3] S. T. Dougherty, J. Gildea, A. Korban, Extending an established isomorphism between group rings and a subring of the $n \times n$ matrices, International Journal of Algebra and Computation, Published: 25 February 2021.
[4] S. T. Dougherty, J. Gildea, A. Korban, $G$-codes over formal power series rings and finite chain rings, J. Algebra Comb. Discrete Appl. 7 (2020) 55–71.
[5] S. T. Dougherty, J. Gildea, A. Korban, A. Kaya, Composite constructions of self-dual codes from group rings and new extremal self-dual binary codes of length 68, Advances in Mathematics of Communications 14(4) (2020) 677–702.
[6] S. T. Dougherty, J. Gildea, A. Korban, A. Kaya, Composite matrices from group rings, composite $G$-codes and constructions of self-dual codes, arXiv:2002.11614.
[7] S. T. Dougherty, J. Gildea, R. Taylor, A. Tylyshchak, Group rings, $G$-codes and constructions of self-dual and formally self-dual codes, Des. Codes, Cryptogr. 86(9) (2017) 2115–2138.
[8] S. T. Dougherty, H. Liu, Y. H. Park, Lifted codes over finite chain rings, Mathematical Journal of Okayama University 53 (2011) 39–53.
[9] S. T. Dougherty, H. Liu, Cyclic codes over formal power series rings, Acta Mathematica Scientia 31(1) (2011) 331–343.
[10] J. Gildea, A. Kaya, R. Taylor, B. Yildiz, Constructions for self-dual codes induced from group rings, Finite Fields Appl. 51 (2018) 71–92.
[11] T. Hurley, Group rings and rings of matrices, Int. Jour. Pure and Appl. Math 31(3) (2006) 319–335.
[12] B. R. McDonald, Finite rings with identity, New York: Marcel Dekker (1974).