J. Algebra Comb. Discrete Appl.
8(2) • 91–105

Received: 20 May 2020
Accepted: 8 December 2020

Journal of Algebra Combinatorics Discrete Structures and Applications

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

Research Article

Adrian Korban

Abstract: In this paper, we extend the work done on G-codes over formal power series rings and finite chain rings $\mathbb{F}_q[t]/(t^i)$, to composite G-codes over the same alphabets. We define composite G-codes over the infinite ring R_∞ 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 γ-adic G-codes over R_∞ 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 σ 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 $v \in RD_{2n}$ 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_∞ to G-codes over the same alphabets. The authors also study γ-adic G-codes over R_∞ and G-codes over principal ideal rings.

Adrian Korban; Department of Mathematical and Physical Sciences, University of Chester, Thornton Science Park, Pool Ln, Chester CH2 4NU, England (email: adrian3@windowslive.com).

https://doi.org/10.13069/jacodesmath.935951

ISSN 2148-838X

Recently in [3], the authors extended the map σ 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 Ω 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 γ-adic G-codes over R_∞ 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 γ-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 $\widehat{R}$ be the character module of the ring R. For a finite ring R the following are equivalent:

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

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

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

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

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

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

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

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

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

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

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

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

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

Let $R^\times$ denote the multiplicative group of all units in the ring R. Let $\mathbb{F} = R/\mathfrak{m} = R/\langle\tilde{\gamma}\rangle$ be the residue field with characteristic p, where p is a prime number, then $|\mathbb{F}| = q = p^r$ for some integers q and r. We know that $|\mathbb{F}^\times| = p^r - 1$. We now state two well-known lemmas for which the proofs can be found in [12].

Lemma 2.2. *For any $0 \neq r \in R$ there is a unique integer i, $0 \leq i < e$ such that $r = \mu\tilde{\gamma}^i$, with ν a unit. The unit μ is unique modulo $\tilde{\gamma}^{e-i}$.*

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

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

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

From Lemma 2.3, 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 $\mathbb{F}$.

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:

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

where e is the nilpotency index of γ. 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

$$1^{k_0}\gamma^{k_1}(\gamma^2)^{k_2}\ldots(\gamma^{e-1})^{k_{e-1}}. \tag{4}$$

2.2.2. Formal power series rings

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

Definition 2.4. *The ring R_∞ is defined as a formal power series ring:*

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

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

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

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

$$\sum_{l=0}^{i-1} a_l\gamma^l + \sum_{l=0}^{i-1} b_l\gamma^l = \sum_{l=0}^{i-1}(a_l + b_l)\gamma^l \tag{5}$$

$$\sum_{l=0}^{i-1} a_l\gamma^l \cdot \sum_{l'=0}^{i-1} b_{l'}\gamma^{l'} = \sum_{s=0}^{i-1}(\sum_{l+l'=s} a_l b_{l'})\gamma^s. \tag{6}$$

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_∞ is a principal ideal domain.

Let $\mathcal{C}$ be a finitely generated linear code over R_∞. Then the generator matrix of code $\mathcal{C}$ is permutation equivalent to the following standard form generator matrix.

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

$$G = \begin{pmatrix} \gamma^{m_0}I_{k_0} & \gamma^{m_0}A_{0,1} & \gamma^{m_0}A_{0,2} & \gamma^{m_0}A_{0,3} & & & \gamma^{m_0}A_{0,r} \\ & \gamma^{m_1}I_{k_1} & \gamma^{m_1}A_{1,2} & \gamma^{m_1}A_{1,3} & & & \gamma^{m_1}A_{1,r} \\ & & \gamma^{m_2}I_{k_2} & \gamma^{m_2}A_{2,3} & & & \gamma^{m_2}A_{2,r} \\ & & & \ddots & \ddots & & \\ & & & & \ddots & \ddots & \\ & & & & & \gamma^{m_{r-1}}I_{k_{r-1}} & \gamma^{m_{r-1}}A_{r-1,r} \end{pmatrix}, \tag{7}$$

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 $\mathcal{C}$ with generator matrix of the form given in Equation 7 is said to be of type*

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

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

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

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

$$\Psi_i^j : R_j \to R_i, \tag{8}$$
$$\sum_{l=0}^{j-1} a_l \gamma^l \mapsto \sum_{l=0}^{i-1} a_l \gamma^l. \tag{9}$$

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

$$\Psi_i^j(a+b) = \Psi_i^j(a) + \Psi_i^j(b),\ \Psi_i^j(ab) = \Psi_i^j(a)\Psi_i^j(b). \tag{10}$$

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

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

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

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

This gives the following diagram:

$$\begin{array}{ccccccccc} & & & & R & & & & \mathbb{F} \\ & & & & \| & & & & \| \\ R_\infty & \to & \cdots & \to & R_e & \to & R_{e-1} & \to \cdots \to & R_1 \end{array}$$

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 $A = circ(\alpha_1, \alpha_2, \dots, \alpha_n)$, where α_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

$$\sum_{i=1}^n \alpha_i g_i + \sum_{i=1}^n \beta_i g_i = \sum_{i=1}^n (\alpha_i + \beta_i) g_i. \tag{12}$$

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

$$(\sum_{i=1}^n \alpha_i g_i)(\sum_{j=1}^n \beta_j g_j) = \sum_{i,j} \alpha_i \beta_j g_i g_j. \tag{13}$$

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 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 $\{g_1, g_2, \dots, g_n\}$ be a fixed listing of the elements of G. Let $\{h_1, h_2, \dots, h_r\}$ 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:

$$\begin{aligned}
&\phi : H \mapsto G_r \\
&h_1 \xrightarrow{\phi} \ g_1 \\
&h_2 \xrightarrow{\phi} \ g_2 \\
&\vdots \quad \vdots \quad \vdots \\
&h_r \xrightarrow{\phi} \ g_r.
\end{aligned}$$

Next, let $v = \alpha_{g_1}g_1 + \alpha_{g_2}g_2 + \cdots + \alpha_{g_n}g_n \in RG$. Define the matrix $\Omega(v) \in M_n(R)$ to be

$$\Omega(v) = \begin{pmatrix} A_1 & A_2 & A_3 & \ldots & A_{\frac{n}{r}} \\ A_{\frac{n}{r}+1} & A_{\frac{n}{r}+2} & A_{\frac{n}{r}+3} & \ldots & A_{\frac{2n}{r}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ A_{\frac{(r-1)n}{r}+1} & A_{\frac{(r-1)n}{r}+2} & A_{\frac{(r-1)n}{r}+3} & \ldots & A_{\frac{n^2}{r^2}} \end{pmatrix}, \tag{14}$$

where at least one block has the following form:

$$A'_l = \begin{pmatrix} \alpha_{g_j^{-1}g_k} & \alpha_{g_j^{-1}g_{k+1}} & \cdots & \alpha_{g_j^{-1}g_{k+(r-1)}} \\ \alpha_{\phi_l((h_l)_2^{-1}(h_l)_1)} & \alpha_{\phi_l((h_l)_2^{-1}(h_l)_2)} & \cdots & \alpha_{\phi_l((h_l)_2^{-1}(h_l)_r)} \\ \alpha_{\phi_l((h_l)_3^{-1}(h_l)_1)} & \alpha_{\phi_l((h_l)_3^{-1}(h_l)_2)} & \cdots & \alpha_{\phi_l((h_l)_3^{-1}(h_l)_r)} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{\phi_l((h_l)_r^{-1}(h_l)_1)} & \alpha_{\phi_l((h_l)_r^{-1}(h_l)_2)} & \cdots & \alpha_{\phi_l((h_l)_r^{-1}(h_l)_r)} \end{pmatrix},$$

and the other blocks are of the form:

$$A_l = \begin{pmatrix} \alpha_{g_j^{-1}g_k} & \alpha_{g_j^{-1}g_{k+1}} & \cdots & \alpha_{g_j^{-1}g_{k+(r-1)}} \\ \alpha_{g_{j+1}^{-1}g_k} & \alpha_{g_{j+1}^{-1}g_{k+1}} & \cdots & \alpha_{g_{j+1}^{-1}g_{k+(r-1)}} \\ \alpha_{g_{j+2}^{-1}g_k} & \alpha_{g_{j+2}^{-1}g_{k+1}} & \cdots & \alpha_{g_{j+2}^{-1}g_{k+(r-1)}} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_{j+r-1}^{-1}g_k} & \alpha_{g_{j+r-1}^{-1}g_{k+1}} & \cdots & \alpha_{g_{j+r-1}^{-1}g_{k+(r-1)}} \end{pmatrix},$$

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

$$\begin{aligned}
&\phi_l : H_i \mapsto G_r \\
&(h_i)_1 \xrightarrow{\phi_l} \ g_j^{-1}g_k \\
&(h_i)_2 \xrightarrow{\phi_l} \ g_j^{-1}g_{k+1} \\
&\vdots \quad \vdots \quad \vdots \\
&(h_i)_r \xrightarrow{\phi_l} \ g_j^{-1}g_{k+(r-1)}.
\end{aligned}$$

. 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 $l = \frac{n}{r}$ then $j = 1, k = n - r + 1$. When $l = \frac{n}{r} + 1$ then $j = r + 1, k = 1$, when $l = \frac{n}{r} + 2$ then $j = r + 1, k = r + 1$, when $l = \frac{n}{r} + 3$ then $j = r + 1, k = 2r + 1$, $\ldots$ when $l = \frac{2n}{r}$ 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:

$$\Omega(v) = \begin{pmatrix} \alpha_{g_{1_1}^{-1}g_1} & \alpha_{g_{1_2}^{-1}g_2} & \alpha_{g_{1_3}^{-1}g_3} & \cdots & \alpha_{g_{1_n}^{-1}g_n} \\ \alpha_{g_{2_1}^{-1}g_1} & \alpha_{g_{2_2}^{-1}g_2} & \alpha_{g_{2_3}^{-1}g_3} & \cdots & \alpha_{g_{2_n}^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_{n_1}^{-1}g_1} & \alpha_{g_{n_2}^{-1}g_2} & \alpha_{g_{n_3}^{-1}g_3} & \cdots & \alpha_{g_{n_n}^{-1}g_n} \end{pmatrix},$$

where $g_{j_i}^{-1}$ 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 ϕ_l 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_l of order r, we define the following code over the ring R :

$$\mathcal{C}(v) = \langle \Omega(v) \rangle. \tag{15}$$

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 can not 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_∞ in the form $\gamma^i a$ where $a = a_0 + a_1\gamma + \cdots + \cdots$ with $a_0 \neq 0$ and $i \geq 0$, which means that a is a unit in R_∞.

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

$$v_j^* = \sum_{i=1}^{n} \gamma^{l_{g_{j_i} g_i}} a_{g_{j_i} g_i} g_{j_i} g_i, \tag{16}$$

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

$$\Omega(v) = \begin{pmatrix} \gamma^{l_{g_{1_1} g_1}} a_{g_{1_1} g_1} & \gamma^{l_{g_{1_2} g_2}} a_{g_{1_2} g_2} & \gamma^{l_{g_{1_3} g_3}} a_{g_{1_3} g_3} & \cdots & \gamma^{l_{g_{1_n} g_n}} a_{g_{1_n} g_n} \\ \gamma^{l_{g_{2_1} g_1}} a_{g_{2_1} g_1} & \gamma^{l_{g_{2_2} g_2}} a_{g_{2_2} g_2} & \gamma^{l_{g_{2_3} g_3}} a_{g_{2_3} g_3} & \cdots & \gamma^{l_{g_{2_n} g_n}} a_{g_{2_n} g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \gamma^{l_{g_{n_1} g_1}} a_{g_{n_1} g_1} & \gamma^{l_{g_{n_2} g_2}} a_{g_{n_2} g_2} & \gamma^{l_{g_{n_3} g_3}} a_{g_{n_3} g_3} & \cdots & \gamma^{l_{g_{n_n} g_n}} a_{g_{n_n} g_n} \end{pmatrix}, \tag{17}$$

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 ϕ_l map in individual blocks. Then we take the row space of the matrix $\Omega(v)$ over R_∞ to get the corresponding composite G-code, namely $\mathcal{C}(v)$.

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

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

Let $w_1 = \sum \gamma^{l_i} b_i g_i \in R_\infty G$. Then if w_2 corresponds to a vector in $\mathcal{C}(v)$, it is of the form $\sum (\gamma^{l_j} \alpha_j) v_j^*$. Then $w_1 w_2 = \sum \gamma^{l_i} b_i g_i \sum (\gamma^{l_j} \alpha_j) v_j^* = \sum \gamma^{l_i} b_i \gamma^{l_j} \alpha_j g_i v_j^*$ 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 $v = \gamma^{l_{g_1}} a_{g_1} g_1 + \gamma^{l_{g_2}} a_{g_2} g_2 + \cdots + \gamma^{l_{g_n}} a_{g_n} g_n \in R_\infty G$ and $\mathcal{C}(v)$ be the corresponding code. Let $\Omega : R_\infty G \to R_\infty^n$ be the canonical map that sends $\gamma^{l_{g_1}} a_{g_1} g_1 + \gamma^{l_{g_2}} a_{g_2} g_2 + \cdots + \gamma^{l_{g_n}} a_{g_n} g_n$ to $(\gamma^{l_{g_1}} a_{g_1}, \gamma^{l_{g_2}} a_{g_2}, \cdots, \gamma^{l_{g_n}} a_{g_n})$. Let I be the ideal $\Omega^{-1}(\mathcal{C})$. Let $\mathbf{w} = (w_1, w_2, \ldots, w_n) \in \mathcal{C}^\perp$. Then the operator of product between any row of $\Omega(v)$ and $\mathbf{w}$ is zero:

$$[(\gamma^{l_{g_{j_1} g_1}} a_{g_{j_1} g_1}, \gamma^{l_{g_{j_2} g_1}} a_{g_{j_2} g_1}, \ldots, \gamma^{l_{g_{j_n} g_1}} a_{g_{j_n} g_1}), (w_1, w_2, \ldots, w_n)] = 0, \ \forall j. \tag{18}$$

Which gives

$$\sum_{i=1}^n \gamma^{l_{g_{j_i} g_i}} a_{g_{j_i} g_i} w_i = 0, \ \forall j. \tag{19}$$

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

$$\gamma^{k_{g_i}} b_{g_i} = \gamma^{k_{g_i^{-1}}} w_{g_i^{-1}}. \tag{20}$$

Then

$$\sum_{i=1}^n \gamma^{l_{g_{j_i} g_i}} a_{g_{j_i} g_i} w_i = 0 \implies \sum_{i=1}^n \gamma^{l_{g_{j_i} g_i}} a_{g_{j_i} g_i} \gamma^{k_{g_i^{-1}}} b_{g_i^{-1}} = 0. \tag{21}$$

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

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

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

Proof. The composite mapping $\Omega(\phi(\mathcal{C}^\perp))$ is permutation equivalent to $\mathcal{C}^\perp$ and $\phi(\mathcal{C}^\perp)$ is an ideal of $R_\infty G$. We know that ϕ is a bijection between $\mathcal{C}^\perp$ and $\mathcal{R}(\Omega^{-1}(\mathcal{C}))$, and we also know that $\Omega^{-1}(\mathcal{C})$ is an ideal of $R_\infty G$ as well. This proves that the dual of a 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_∞ in the form $\gamma^i a$ where $a = a_0 + a_1\gamma + \cdots + \cdots$ with $a_0 \neq 0$ and $i \geq 0$, which means that a is a unit in R_∞.

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

$$\Omega(v) = \begin{pmatrix} \gamma^{l_{g_{1_1} g_1}} a_{g_{1_1} g_1} & \gamma^{l_{g_{1_2} g_2}} a_{g_{1_2} g_2} & \gamma^{l_{g_{1_3} g_3}} a_{g_{1_3} g_3} & \dots & \gamma^{l_{g_{1_n} g_n}} a_{g_{1_n} g_n} \\ \gamma^{l_{g_{2_1} g_1}} a_{g_{2_1} g_1} & \gamma^{l_{g_{2_2} g_2}} a_{g_{2_2} g_2} & \gamma^{l_{g_{2_3} g_3}} a_{g_{2_3} g_3} & \dots & \gamma^{l_{g_{2_n} g_n}} a_{g_{2_n} g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \gamma^{l_{g_{n_1} g_1}} a_{g_{n_1} g_1} & \gamma^{l_{g_{n_2} g_2}} a_{g_{n_2} g_2} & \gamma^{l_{g_{n_3} g_3}} a_{g_{n_3} g_3} & \dots & \gamma^{l_{g_{n_n} g_n}} a_{g_{n_n} g_n} \end{pmatrix},$$

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 γ^{m_0}. The elements in the first column of matrix $\Omega(v)$ have the form $\gamma^{l_{g_j}} a_{g_j}$ with $l_{g_j} \geq m_0$ and a_{g_j} a unit, thus, these can be replaced by zero when they are added to the first row multiplied by $-\gamma^{l_{g_j} - m_0}(a_{g_j})^{-1}$. Continuing the process using elementary operations, we obtain the standard generator matrix of the code $\mathcal{C}$ given in Equation 7. $\square$

Example 4.2. *Let $G = \langle x, y \mid x^4 = 1, y^2 = x^2, yxy^{-1} = x^{-1} \rangle \cong Q_8$. Let $v = \sum_{i=0}^{3} \left(\alpha_{i+1} x^i + \alpha_{i+5} x^i y \right) \in R_\infty Q_8$, where $\alpha_i = \alpha_{g_i} \in R_\infty$. 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:*

$$\Omega(v) = \begin{pmatrix} A_1' & A_2 \\ A_3 & A_4' \end{pmatrix} =$$

$$\left(\begin{array}{cccc|cccc} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \alpha_{g_1^{-1}g_3} & \alpha_{g_1^{-1}g_4} & \alpha_{g_1^{-1}g_5} & \alpha_{g_1^{-1}g_6} & \alpha_{g_1^{-1}g_7} & \alpha_{g_1^{-1}g_8} \\ \alpha_{\phi_1((h_1)_2^{-1}(h_1)_1)} & \alpha_{\phi_1((h_1)_2^{-1}(h_1)_2)} & \alpha_{\phi_1((h_1)_2^{-1}(h_1)_3)} & \alpha_{\phi_1((h_1)_2^{-1}(h_1)_4)} & \alpha_{g_2^{-1}g_5} & \alpha_{g_2^{-1}g_6} & \alpha_{g_2^{-1}g_7} & \alpha_{g_2^{-1}g_8} \\ \alpha_{\phi_1((h_1)_3^{-1}(h_1)_1)} & \alpha_{\phi_1((h_1)_3^{-1}(h_1)_2)} & \alpha_{\phi_1((h_1)_3^{-1}(h_1)_3)} & \alpha_{\phi_1((h_1)_3^{-1}(h_1)_4)} & \alpha_{g_3^{-1}g_5} & \alpha_{g_3^{-1}g_6} & \alpha_{g_3^{-1}g_7} & \alpha_{g_3^{-1}g_8} \\ \alpha_{\phi_1((h_1)_4^{-1}(h_1)_1)} & \alpha_{\phi_1((h_1)_4^{-1}(h_1)_2)} & \alpha_{\phi_1((h_1)_4^{-1}(h_1)_3)} & \alpha_{\phi_1((h_1)_4^{-1}(h_1)_4)} & \alpha_{g_4^{-1}g_5} & \alpha_{g_4^{-1}g_6} & \alpha_{g_4^{-1}g_7} & \alpha_{g_4^{-1}g_8} \\ \hline \alpha_{g_5^{-1}g_1} & \alpha_{g_5^{-1}g_2} & \alpha_{g_5^{-1}g_3} & \alpha_{g_5^{-1}g_4} & \alpha_{g_5^{-1}g_5} & \alpha_{g_5^{-1}g_6} & \alpha_{g_5^{-1}g_7} & \alpha_{g_5^{-1}g_8} \\ \alpha_{g_6^{-1}g_1} & \alpha_{g_6^{-1}g_2} & \alpha_{g_6^{-1}g_3} & \alpha_{g_6^{-1}g_4} & \alpha_{\phi_4((h_1)_2^{-1}(h_1)_1)} & \alpha_{\phi_4((h_1)_2^{-1}(h_1)_2)} & \alpha_{\phi_4((h_1)_2^{-1}(h_1)_3)} & \alpha_{\phi_4((h_1)_2^{-1}(h_1)_4)} \\ \alpha_{g_7^{-1}g_1} & \alpha_{g_7^{-1}g_2} & \alpha_{g_7^{-1}g_3} & \alpha_{g_7^{-1}g_4} & \alpha_{\phi_4((h_1)_3^{-1}(h_1)_1)} & \alpha_{\phi_4((h_1)_3^{-1}(h_1)_2)} & \alpha_{\phi_4((h_1)_3^{-1}(h_1)_3)} & \alpha_{\phi_4((h_1)_3^{-1}(h_1)_4)} \\ \alpha_{g_8^{-1}g_1} & \alpha_{g_8^{-1}g_2} & \alpha_{g_8^{-1}g_3} & \alpha_{g_8^{-1}g_4} & \alpha_{\phi_4((h_1)_4^{-1}(h_1)_1)} & \alpha_{\phi_4((h_1)_4^{-1}(h_1)_2)} & \alpha_{\phi_4((h_1)_4^{-1}(h_1)_3)} & \alpha_{\phi_4((h_1)_4^{-1}(h_1)_4)} \end{array} \right),$$

where:

$$\phi_1 : \begin{array}{c} (h_1)_i \xrightarrow{\phi_1} g_1^{-1} g_i \\ \text{for } i = \{1,2,3,4\} \end{array} \quad \phi_4 : \begin{array}{c} (h_1)_i \xrightarrow{\phi_4} g_5^{-1} g_j \\ \text{for when } \{i = 1, \dots, 4 \text{ and } j = i+4\}, \end{array}$$

in A_1' and A_4' respectively. This results in a composite matrix over R_∞ of the following form:

$$\Omega(v) = \left(\begin{array}{cc|c} X_1 & Y_1 & \multirow{2}{*}{X_2} \\ Y_1 & X_1 & \\ \hline \multicolumn{2}{c|}{\multirow{2}{*}{X_3}} & \begin{matrix} X_4 & Y_4 \\ Y_4 & X_4 \end{matrix} \end{array}\right) = \left(\begin{array}{cccc|cccc} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 \\ \alpha_2 & \alpha_1 & \alpha_4 & \alpha_3 & \alpha_8 & \alpha_5 & \alpha_6 & \alpha_7 \\ \alpha_3 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_7 & \alpha_8 & \alpha_5 & \alpha_6 \\ \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_5 \\ \hline \alpha_7 & \alpha_6 & \alpha_5 & \alpha_8 & \alpha_1 & \alpha_4 & \alpha_3 & \alpha_2 \\ \alpha_8 & \alpha_7 & \alpha_6 & \alpha_5 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_5 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_4 \\ \alpha_6 & \alpha_5 & \alpha_8 & \alpha_7 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_1 \end{array}\right).$$

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

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

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

and $\mathcal{C}(v)$ *is equivalent to*

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

Clearly $\mathcal{C}(v) = \langle \Omega(v) \rangle$ *is the* $[8, 4, 4]$ *extended Hamming code.*

We now generalize the results from [4] on the projection of codes with a given type.

Proposition 4.3. *Let* $\mathcal{C}$ *be a composite* G*-code over* R_∞ *of type*

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

with generator matrix $\Omega(v)$. *The code generated by* $\Psi_i(\Omega(v))$ *is a code over* R_i *of type* $\{(\gamma^{m_0})^{k_0}, (\gamma^{m_1})^{k_1}, \dots, (\gamma^{m_{s-1}})^{k_{s-1}}\}$ *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*

$$\{(\Psi_i(c_1), \Psi_i(c_2), \dots, \Psi_i(c_n)) \mid (c_1, c_2, \dots, c_n) \in \mathcal{C}\}. \tag{22}$$

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

The code $\mathcal{C}$ is formed by taking the row space of $\Omega(v)$ over the ring R_∞, i.e. $\gamma^{l_1}a_1v_1 + \gamma^{l_2}a_2v_2 + \cdots + \gamma^{l_n}a_nv_n$ where $\gamma^{l_i}a_i \in R_\infty$ and v_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. $\square$

Since a composite G- code over R_∞ 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* $\mathcal{C}$ *be a composite* G*-code of length* n *over* R_∞, *then,* *(1) $\mathcal{C}^\perp$ has type 1^m for some m,*

(2) $\mathcal{C} = (\mathcal{C}^\perp)^\perp$ if and only if $\mathcal{C}$ has type 1^k for some k,

(3) If $\mathcal{C}$ has a standard generator matrix G as in equation (7), then we have

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

$$H = \begin{pmatrix} B_{0,r} & B_{0,r-1} & \dots & B_{0,2} & B_{0,1} & I_{k_r} \end{pmatrix}, \tag{23}$$

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

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

Example 4.5. *If we take the generator matrix G of a code $\mathcal{C}$ from Example 1, we can see that*

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

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 $\mathcal{C}^\perp$ of $\mathcal{C}$ has the form:

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

Now,

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

thus

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

We also have

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

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

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

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

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

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 $C_1 \succeq C_2$, 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 $\mathcal{C}$ is a $[n,k]$ γ-adic code, then for any $i < \infty$, we call $\Psi_i(\mathcal{C})$ a projection of $\mathcal{C}$. We denote $\Psi_i(\mathcal{C})$ by $\mathcal{C}^i$.*

Lemma 4.8. *Let $\mathcal{C}$ be a composite G-code over R_∞ with type 1^k. If $\Omega(v)$ is a standard form of $\mathcal{C}$, then for any positive integer, i, $\Psi_i(\Omega(v))$ is a standard form of $\Psi_i(\mathcal{C})$.*

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 $\mathcal{C}$ has type 1^k, hence $\Psi_i(\mathcal{C})$ has type 1^k. The rest of the proof is the same as in [8]. □

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

$$\Omega_1 : R_\infty G \to \mathcal{C}(v_\infty),$$

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

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

Let

$$\Psi_i : R_\infty G \to R_i G \tag{24}$$

$$\gamma^i a \mapsto \Psi(\gamma^i a). \tag{25}$$

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:

$$\begin{array}{ccc} R_\infty^n G & \overset{\Omega_1}{\to} & \mathcal{C}(v_\infty) \\ \Psi_i \downarrow & & \downarrow \Psi_i \\ R_i^n G & \underset{\Omega_1}{\to} & \mathcal{C}(v) \end{array}.$$

This gives that $\Psi_i \Omega_1 = \Omega_1 \Psi_i$, which gives the following theorem.

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

Proof. Let $v_\infty \in R_\infty G$ and $\mathcal{C}(v_\infty)$ be the corresponding composite G-code over R_∞. Then $\Omega_1(v_\infty) = \mathcal{C}(v_\infty)$ is an ideal of $R_\infty G$. By the homomorphism in Equation 24 and the commutative diagram above, we know that $\Psi_i(\Omega_1(v_\infty)) = \Omega_1(\Psi_i(v_\infty))$ is an ideal of the group ring $R_i G$. This implies that $\Psi_i(\mathcal{C})$ 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 $\mathcal{C}$, $\tilde{\mathcal{C}}$ 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 $\mathcal{C} = \langle \Omega(v_1) \rangle$ 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 $\tilde{\mathcal{C}} = \langle \Omega(v_2) \rangle$ be the corresponding composite G-code. We can say that v_1 and v_2 act as generators of $\mathcal{C}$ and $\tilde{\mathcal{C}}$ respectively. We can clearly see that we can have $\Psi_i^j(v_2) = \Psi_i^j(\beta_{g_1}) g_1 + \Psi_i^j(\beta_{g_2}) g_2 + \cdots + \Psi_i^j(\beta_{g_n}) g_n = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \cdots + \alpha_{g_n} g_n \in R_i G$, thus $\Psi_i^j(v_2)$ is a generator matrix of $\mathcal{C}$. This implies that the composite G-code $\mathcal{C}(v_1)$ 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 γ-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 $\mathcal{C}$ be a $[n,k]$ composite G-code of type 1^k, and G, H be a generator and parity-check matrices of $\mathcal{C}$. Let $G_i = \Psi_i(G)$ and $H_i = \Psi_i(H)$. Then G_i and H_i are generator and parity check matrices of $\mathcal{C}^i$ respectively. Let $i < j < \infty$ be two positive integers, then*

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

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

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

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

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

Theorem 4.12. *Let $\mathcal{C}$ be a composite G-code over R_∞. Then the following two results hold.*

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

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

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_∞. We omit the proofs since a composite G- code over R_∞ is a linear code and for that fact, the proofs are the same as in [8].

Theorem 4.13. *Let $\mathcal{C}$ be a composite G-code over R_∞. If $\mathcal{C}$ is an MDR or MDS code then $\mathcal{C}^\perp$ is an MDS code.*

Theorem 4.14. *Let $\mathcal{C}$ be a composite G-code over R_i, and $\tilde{\mathcal{C}}$ be a lift of C over R_j, where $j > i$. If $\mathcal{C}$ is an MDS code over R_i then the code $\tilde{\mathcal{C}}$ is an MDS code over R_j.*

5. Self-dual γ-adic composite G-codes

In this section, we extend some results for self-dual γ-adic codes to composite G-codes over R_∞. 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_∞ with

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

and $R_1 = \mathbb{F}_q$ where $q = p^r$ for some prime p and nonnegative integer r. The field $\mathbb{F}_q$ is said to be the underlying field of the rings.

We now 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_∞ 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_∞ respectively.

Theorem 5.1. *Let i be odd and $\mathcal{C}$ be a composite G-code over R_i with type $1^{k_0}(\gamma)^{k_1}(\gamma^2)^{k_2}\ldots(\gamma^{i-1})^{k_{i-1}}$. Then $\mathcal{C}$ is a self-dual code if and only if $\mathcal{C}$ is self-orthogonal and $k_j = k_{i-j}$ for all j.*

Proof. It is enough to show that $\Omega(v)$ where $v \in R_iG$ 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 $\mathcal{C}$ is a self-dual composite G-code of length n over R_∞ then $\Psi_i(\mathcal{C})$ 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 $\Psi_1^i(\tilde{G})$ is used in [8], we notice that in our case the map will correspond to $\Psi_1^i(\tilde{G}) = \Psi_1^i(v) = \Psi_1^i(\gamma^{l_{g_1}} a_{g_1})g_1 + \Psi_1^i(\gamma^{l_{g_2}} a_{g_2})g_2 + \cdots + \Psi_1^i(\gamma^{l_{g_n}} a_{g_n})g_n$, assuming that $\tilde{G}$ is the generator matrix of a composite G-code and $v \in R_iG$. Then $\Psi_1^i(\tilde{G})$ is the generator matrix of a composite G-code over $\mathbb{F}_q$. □

Theorem 5.4. *Let $R = R_e$ be a finite chain ring, $\mathbb{F} = R/\langle\gamma\rangle$, where $|\mathbb{F}| = q = p^r, 2 \neq p$ is a prime. Then any self-dual composite G-code $\mathcal{C}$ over $\mathbb{F}$ can be lifted to a self-dual composite G-code over R_∞.*

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

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

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

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

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

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

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

be the associated code over A^j_i. Let

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

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

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

Proof. Let $\mathbf{v}_j \in \mathcal{C}^j_{e_j}$. We know that $\mathbf{v}^*_j$ also belongs to $\mathcal{C}^j_{e_j}$ where $\mathbf{v}^*_j$ has the form defined in (16). Let $\mathbf{v} \in \mathcal{C}^j_\infty$. Now if $\mathbf{v} = CRT(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s)$, then $\mathbf{v}^* = CRT(\mathbf{v}^*_1, \mathbf{v}^*_2, \ldots, \mathbf{v}^*_s)$ and so $\mathbf{v}^* \in \mathcal{C}^j_\infty$ giving that $\mathcal{C}^j_\infty$ is an ideal in $A^j_\infty G$, and thus giving that $\mathcal{C}^j_\infty$ is a composite G-code over A^j_∞. □

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 γ-adic G-codes and G-codes over principal ideal rings to composite γ-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. Tylshchak, 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).