Math. J. Okayama Univ. **53** (2011), 39–53

LIFTED CODES OVER FINITE CHAIN RINGS

Steven T. Dougherty, Hongwei Liu and Young Ho Park

Abstract. In this paper, we study lifted codes over finite chain rings. We use γ-adic codes over a formal power series ring to study codes over finite chain rings.

1. Introduction

Codes over finite rings have been studied for many years. More recently, codes over a wide variety of rings have been studied.

In this paper, we shall first define a series of chain rings and describe the concept of γ-adic codes. Then we will study these γ-adic codes over this class of chain rings.

We begin with some definitions. Throughout we let R be a finite commutative ring with identity $1 \neq 0$. Let $R^n = \{(x_1, \cdots, x_n) \,|\, x_j \in R\}$ be an R-module. An R-submodule C of R^n is called a linear code of length n over R. We assume throughout that all codes are linear.

For $\mathbf{x}, \mathbf{y} \in R^n$, the inner product of $\mathbf{x}, \mathbf{y}$ is defined as follows: $[\mathbf{x}, \mathbf{y}] = x_1y_1 + \cdots + x_ny_n$. If C is a code of length n over R, we define $C^\perp = \{\mathbf{x} \in R^n \,|\, [\mathbf{x}, \mathbf{c}] = 0, \forall\, \mathbf{c} \in C\}$ to be the orthogonal code of C. Notice that $C^\perp$ is linear whether or not C is linear.

It is well known that for any linear code C over a finite Frobenius ring, $|C| \cdot |C^\perp| = R^n$.

A finite 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.

A finite chain ring is a Frobenius ring, so the identity above holds for codes over finite chain rings. If $C \subseteq C^\perp$, then C is called self-orthogonal. Moreover, if $C = C^\perp$, then C is called self-dual.

Let R be a finite chain ring, $\mathfrak{m}$ the unique maximal ideal of R, and let γ be the generator of the unique maximal ideal $\mathfrak{m}$. Then $\mathfrak{m} = \langle \gamma \rangle = R\gamma$,

Mathematics Subject Classification. Primary: 94B05, Secondary: 13A99.
Key words and phrases. Finite chain rings, lifted codes, γ-adic codes.

where $R\gamma = \langle\gamma\rangle = \{\beta\gamma \mid \beta \in R\}$. We have

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

Let e be the minimal number such that $\langle\gamma^e\rangle = \{0\}$. The number e is called the nilpotency index of γ.

Let $|R|$ denote the cardinality of R and $R^\times$ the multiplicative group of all units in R. Let $\mathbb{F} = R/\mathfrak{m} = R/\langle\gamma\rangle$ be the residue field with characteristic p, where p is a prime number. We know that $|\mathbb{F}| = q = p^r$ for some integers q and r and $|\mathbb{F}^\times| = p^r - 1$. The following lemma is well-known (see [10], for example).

Lemma 1.1. *Let R be a finite chain ring with maximal ideal $\mathfrak{m} = \langle\gamma\rangle$, where γ is a generator of $\mathfrak{m}$ with nilpotency index e. For any $0 \neq r \in R$ there is a unique integer i, $0 \leq i < e$ such that $r = \mu\gamma^i$, with μ a unit. The unit μ is unique modulo γ^{e-i}. Let $V \subseteq R$ be a set of representatives for the equivalence classes of R under congruence modulo γ. Then*

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

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

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

By Lemma 1.1, the cardinality of R is:

$$|R| = |\mathbb{F}| \cdot |\langle\gamma\rangle| = |\mathbb{F}| \cdot |\mathbb{F}|^{e-1} = |\mathbb{F}|^e = p^{er}. \tag{2}$$

Let R be a finite ring. We know from [10] that the generator matrix for a code C over R is permutation equivalent to a matrix of the following form:

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

The matrix G above is called the standard generator matrix form of the code C. It is immediate that a code C with this generator matrix has cardinality

$$|C| = |\mathbb{F}|^{\sum_{i=0}^{e-1}(e-i)k_i} = (p^r)^{\sum_{i=0}^{e-1}(e-i)k_i} = (p^{re})^{k_0}(p^{r(e-1)})^{k_1} \cdots (p^r)^{k_{e-1}}. \tag{4}$$

In this case, the code C is said to have type

$$1^{k_0}(\gamma)^{k_1}(\gamma^2)^{k_2}\cdots(\gamma^{e-1})^{k_{e-1}}. \tag{5}$$

2. Lifts of Codes over Finite Chain Rings

Let R be a finite chain ring with the maximal ideal $\langle\gamma\rangle$, where the nilpotency index of γ is e and $R/\langle\gamma\rangle = \mathbb{F}$. We know that for any element a of R, it can be written uniquely as

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

where $a_i \in \mathbb{F}$, see [10] for example. For an arbitrary positive integer i, we define R_i as

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

where $\gamma^{i-1} \neq 0$, but $\gamma^i = 0$ in R_i, and define two operations over R_i:

$$\sum_{l=0}^{i-1} a_l\gamma^l + \sum_{l=0}^{i-1} b_l\gamma^l = \sum_{l=0}^{i-1}(a_l + b_l)\gamma^l \tag{6}$$

$$\sum_{l=0}^{i-1} a_l\gamma^l \cdot \sum_{l'=0}^{i-1} b_{l'}\gamma^{l'} = \sum_{s=0}^{i-1}(\sum_{l+l'=s} a_l b'_l)\gamma^s. \tag{7}$$

It is easy to get that all the R_i are finite rings. Moreover, we have the following lemma, the proof of which can be found in [9].

Lemma 2.1. *For any positive integer i, we have*

(i) $R_i^\times = \{\sum_{l=0}^{i-1} a_l\gamma^l \,|\, 0 \neq a_0 \in \mathbb{F}\}$;

(ii) the ring R_i is a chain ring with maximal ideal $\langle\gamma\rangle$.

We define R_∞ as the ring of formal power series as follows:

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

The following lemma is well-known.

Lemma 2.2. *We have that (i)* $R_\infty^\times = \{\sum_{l=0}^{\infty} a_l\gamma^l \,|\, a_0 \neq 0\}$;

(ii) the ring R_∞ is a principal ideal domain.

Lemma 2.3. *Let $\mathcal{C}$ be a nonzero linear code over R_∞ of length n, then any generator matrix of $\mathcal{C}$ is permutation equivalent to a matrix of the following form:*

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

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

Proof. Before proving the lemma, we note that all nonzero elements in R_∞ can be written in the form $\gamma^i a$, where $a = a_0 + a_1\gamma + \cdots + \cdots$ with $a_0 \neq 0$ and $i \geq 0$. This means that a is a unit in R_∞.

Let Ω be an arbitrary set of generators of code $\mathcal{C}$, a generator matrix G can be obtained by eliminating those elements which can be written as a linear combination of other elements in the set Ω. In order to obtain the standard form in this lemma, we do the following operations. First we take one nonzero element with form $\gamma^{m_0} a$, where m_0 is the minimal nonnegative integer such that $m_0 = \min\{i \,|\, \gamma^i a \text{ is a coordinate in an element of } \Omega\}$. By applying column and row permutations and by dividing a row by a unit, the element in position $(1,1)$ of matrix G can be replaced by γ^{m_0}. Since those nonzero elements which are in the first column of matrix G have the form $\gamma^j b$ with $j \geq m_0$ and b a unit, these elements can be replaced by zero when they are added by the first row which multiplied by $-\gamma^{j-m_0} b^{-1}$. Then we continue this process by using elementary operations, and the standard form of G is obtained. □

Definition 1. *A code $\mathcal{C}$ with generator matrix of the form given in Equation (8) is said to be of type*

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

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

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

The following lemma and theorem are direct generalization from [3]. The proofs are simply generalizations to those for the p-adic case.

Lemma 2.4. *If $\mathcal{C}$ is a linear code over R_∞ then $\mathcal{C}^\perp$ has type 1^m for some m.*

We denote the transpose of a matrix M by M^T.

Theorem 2.5. *Let $\mathcal{C}$ be a linear code of length n over R_∞. If $\mathcal{C}$ has a standard generator matrix G as in equation (8), then we have*

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

$$H = \begin{pmatrix} B_{0,r} & B_{0,r-1} & \cdots & B_{0,2} & B_{0,1} & I_{k_r} \end{pmatrix}, \tag{9}$$

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 $1 \le j \le r$;

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

Example 1. *Let $\mathcal{C}$ be a code of length 5 over R_∞ with a standard generator matrix as follows:*

$$G = \begin{pmatrix} \gamma^2 & 0 & \gamma^2(1+\gamma) & \gamma^2(1+\gamma+\gamma^2) & \gamma^2 \\ 0 & \gamma^2 & \gamma^2(1+2\gamma) & \gamma^2(1+\gamma^2) & \gamma^2(1+3\gamma^2) \\ 0 & 0 & \gamma^4 & \gamma^4(1+\gamma^2) & \gamma^4(2+\gamma) \end{pmatrix}. \tag{10}$$

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

$$H = \begin{pmatrix} \gamma^3 & 2\gamma+2\gamma^3 & -(1+\gamma^2) & 1 & 0 \\ 1+3\gamma+\gamma^2 & 1+5\gamma-\gamma^2 & -(2+\gamma) & 0 & 1 \end{pmatrix}. \tag{11}$$

This gives that

$$\mathrm{rank}(\mathcal{C}) + \mathrm{rank}(\mathcal{C}^\perp) = 3 + 2 = 5.$$

For two positive integers $i < j$, we define a map as follows:

$$\Psi_i^j : R_j \rightarrow R_i, \tag{12}$$

$$\sum_{l=0}^{j-1} a_l\gamma^l \mapsto \sum_{l=0}^{i-1} a_l\gamma^l. \tag{13}$$

If we replace R_j with R_∞ then we denote Ψ_i^∞ by Ψ_i. Let a, b be two arbitrary elements in R_j. It is easy to get that

$$\Psi_i^j(a+b) = \Psi_i^j(a) + \Psi_i^j(b),\ \Psi_i^j(ab) = \Psi_i^j(a)\Psi_i^j(b). \tag{14}$$

If $a, b \in R_\infty$. We have that

$$\Psi_i(a+b) = \Psi_i(a) + \Psi_i(b),\ \Psi_i(ab) = \Psi_i(a)\Psi_i(b). \tag{15}$$

We note that the two maps Ψ_i and Ψ_i^j can be extended naturally from R_∞^n to R_i^n and R_j^n to R_i^n respectively.

Remark 1. *The construction method above gives a series of chain rings (up to the principal ideal domain R_∞) as follows:*

$$R_\infty \ \rightarrow \ \cdots \ \rightarrow \ R_e \ \rightarrow \ R_{e-1} \ \rightarrow \ \cdots \rightarrow \ R_1 = \mathbb{F}$$

Definition 2. *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 $\Psi_i^j(G_2)$ is a generator matrix of C_1. It can be proven that $C_1 = \Psi_i^j(C_2)$. 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 2.6. *Let M be a matrix over R_∞ with type 1^k. If M' is a standard form of M, then for any positive integer $i, \Psi_i(M')$ is a standard form of $\Psi_i(M)$.*

Proof. We note that M has type 1^k, hence $\Psi_i(M)$ has type 1^k. We know M' is a standard form of M, this implies that there exist elementary matrices $P_1, \cdots, P_s$ and $Q_1, \cdots, Q_t$ such that

$$P_1 \cdots P_s M Q_1 \cdots Q_t = M'.$$

Hence for any positive integer i, by Equation (15), we have that

$$\Psi_i(P_1) \cdots \Psi_i(P_s)\Psi_i(M)\Psi_i(Q_1) \cdots \Psi_i(Q_t) = \Psi_i(M').$$

Since the inverse matrices of elementary matrices are the same type of elementary matrices, we have that $\Psi_i(M')$ is a standard form of $\Psi_i(M)$. $\square$

Remark 2. *In the lemma above we must assume that M has type 1^k. For example, if we take*

$$M = \begin{pmatrix} \gamma^5 & \gamma^5 + \gamma^7 \\ 0 & \gamma^{15} \end{pmatrix}, \tag{16}$$

then some of its projections are the zero matrix.

Let $\mathcal{C}$ be a code over R_∞, we know that $\mathcal{C} \subseteq (\mathcal{C}^\perp)^\perp$. But in general $\mathcal{C} \neq (\mathcal{C}^\perp)^\perp$. For example, let $\mathcal{C} = \langle \gamma^i \rangle$ be a code of length 1 over R_∞ for some i. Then $\mathcal{C}^\perp = \{0\}$ and $(\mathcal{C}^\perp)^\perp = R_\infty$ since R_∞ is a domain. This means that $\mathcal{C} \subsetneq (\mathcal{C}^\perp)^\perp$. We have the following proposition.

Proposition 2.7. *Let $\mathcal{C}$ be a linear code over R_∞. Then $\mathcal{C} = (\mathcal{C}^\perp)^\perp$ if and only if $\mathcal{C}$ has type 1^k for some k.*

Proof. First we note that $(\mathcal{C}^\perp)^\perp \subseteq \mathcal{C}$. If $\mathcal{C}$ is a linear code then by Lemma 2.4, the code $\mathcal{C}^\perp$ is a linear code with type 1^{n-k} for some k. This implies that $(\mathcal{C}^\perp)^\perp$ has type $1^{n-(n-k)} = 1^k$. □

Proposition 2.8. *Let $\mathcal{C}$ be a self-orthogonal code over R_∞. Then the code $\Psi_i(\mathcal{C})$ is a self-orthogonal code over R_i for all $i < \infty$.*

Proof. We have that $[\mathbf{v}, \mathbf{w}] = 0$ for all $\mathbf{v}, \mathbf{w} \in \mathcal{C}$ since $\mathcal{C}$ is a self-orthogonal code over R_∞. This gives that

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

Hence $\Psi_i(\mathcal{C})$ is a self-orthogonal code over R_i. □

By Lemma 2.6, we know that for a γ-adic $[n, k]$ code $\mathcal{C}$ of type 1^k, $\mathcal{C}^i = \Psi_i(\mathcal{C})$ is an $[n, k]$ code of type 1^k over R_i. In the following, we consider codes over chain rings that are projections of γ-adic codes.

Note that $\mathcal{C}^i \preceq \mathcal{C}^{i+1}$ for all i. Thus if a code $\mathcal{C}$ over R_∞ of type 1^k is given, then we obtain a series of lifts of codes as follows:

$$\mathcal{C}^1 \preceq \mathcal{C}^2 \preceq \cdots \preceq \mathcal{C}^i \preceq \cdots$$

Conversely, let C be an $[n, k]$ code over $\mathbb{F} = R_e/\langle\gamma\rangle = R_1$, and let $G = G_1$ be its generator matrix. It is clear that we can define a series of generator matrices $G_i \in M_{k\times n}(R_i)$ such that $\Psi_i^{i+1}(G_{i+1}) = G_i$, where $M_{k\times n}(R_i)$ denotes all the matrices with k rows and n columns over R_i. This defines a series of lifts C_i of C to R_i for all i. Then this series of lifts determines a code $\mathcal{C}$ such that $\mathcal{C}^i = C_i$, the code is not necessarily unique.

Let $\mathcal{C}$ be a γ-adic $[n, k]$ 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.

Lemma 2.9. *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) $\gamma^{j-i}H_i \equiv \gamma^{j-i}H_j \pmod{\gamma^j}$*.*

Proof. Let $\mathbf{x}_l$ be the row vectors of G_i and $\mathbf{y}_l$ be the row vectors of G_j. Since we have that $G_i = \Psi_i^j(G_j)$, this implies that $\mathbf{x}_l \equiv \mathbf{y}_l \pmod{\gamma^i}$. Thus $\gamma^{j-i}\mathbf{x}_l \equiv \gamma^{j-i}\mathbf{y}_l \pmod{\gamma^j}$.

The proof of (ii) is similar. □

Lemma 2.10. *Let $i < j < \infty$ be two positive integers. Then*
(i) $\gamma^{j-i}\mathcal{C}^i \subseteq \mathcal{C}^j$*;*
(ii) $\mathbf{v} = \gamma^i\mathbf{v}_0 \in \mathcal{C}^j$ *if and only if* $\mathbf{v}_0 \in \mathcal{C}^{j-i}$*;*
(iii) $\mathrm{Ker}(\Psi_i^j) = \gamma^i\mathcal{C}^{j-i}$*.*

Proof. (i) Let $\mathbf{v}$ be an arbitrary codeword of $\mathcal{C}^i$. By Lemma 2.9 (ii), we have that

$$H_j(\gamma^{j-i}\mathbf{v})^T = \gamma^{j-i}H_j\mathbf{v}^T \equiv \gamma^{j-i}H_i\mathbf{v}^T \equiv \mathbf{0} \pmod{\gamma^j}.$$

This implies that $\gamma^{j-i}\mathcal{C}^i \subseteq \mathcal{C}^j$.

(ii) We know that $\gamma^i\mathbf{v}_0 \in \mathcal{C}^j$ if and only if $\gamma^i H_j\mathbf{v}_0^T \equiv \mathbf{0} \pmod{\gamma^j}$. By Lemma 2.9(ii), we have that

$$\gamma^i H_j = \gamma^{j-(j-i)}H_j \equiv \gamma^{j-(j-i)}H_{j-i} \equiv \gamma^i H_{j-i} \pmod{\gamma^j}.$$

This implies that $\gamma^i\mathbf{v}_0 \in \mathcal{C}^j \Leftrightarrow \gamma^i H_{j-i}\mathbf{v}_0^T \equiv \mathbf{0} \pmod{\gamma^j}$. Hence we have that

$$\gamma^i\mathbf{v}_0 \in \mathcal{C}^j \Leftrightarrow H_{j-i}\mathbf{v}_0^T \equiv \mathbf{0} \pmod{\gamma^{j-i}} \Leftrightarrow \mathbf{v}_0 \in \mathcal{C}^{j-i}.$$

(iii) By the definition of Kernel and (ii), we know that the vector $\mathbf{v} \in \mathrm{Ker}(\Psi_i^j)$ if and only if $\mathbf{v} \in \mathcal{C}^j$ and $\mathbf{v} = \gamma^i\mathbf{v}_0$, where $\mathbf{v}_0 \in \mathcal{C}^{j-i}$. Thus the result follows. □

Remark 3. *Lemma 2.10(iii) shows that the Hamming weight enumerator of* $\mathrm{Ker}(\Psi_i^j)$ *is equal to the Hamming weight enumerator of* $\mathcal{C}^{j-i}$*.*

We now study the weights of codewords in the lifts of a code. Suppose $i < j$. By Lemma 2.10(i), we know that any weight of a codeword in $\mathcal{C}^i$ is a weight of a codeword in $\mathcal{C}^j$. This implies that if $\mathbf{v} \in \mathcal{C}^i$ then there exists a $\mathbf{w} \in \mathcal{C}^j$ such that $w_H(\mathbf{w}) = w_H(\mathbf{v})$, where $w_H(\cdot)$ denotes the Hamming weight of a vector. But in general the converse is not always true. We have the following theorem.

Theorem 2.11. *Let $\mathcal{C}$ be a γ-adic code. 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 $d = d_H(\mathcal{C}^1)$.

Proof. (i) Let $\mathbf{v}_0$ be a vector of $\mathcal{C}^1$ with minimal Hamming weight d of $\mathcal{C}^1$. By Lemma 2.10(iii), we know that $\gamma^{i-1}\mathbf{v}_0$ is a codeword of $\mathcal{C}^i$ with Hamming weight d. Hence $d_H(\mathcal{C}^i) \leq d$ for all i. Now we use induction on the index number i and assume that $d_H(\mathcal{C}^j) = d$ for all $j \leq i$. Suppose that $d_H(\mathcal{C}^{i+1}) < d$ and there is a non-zero vector $\mathbf{v} \in \mathcal{C}^{i+1}$ such that $w_H(\mathbf{v}) < d$. Then $w_H(\Psi_i^{i+1}(\mathbf{v})) \leq w_H(\mathbf{v}) < d$. Since we have that $d_H(\mathcal{C}^i) = d$ we must have that $\Psi_i^{i+1}(\mathbf{v}) = \mathbf{0}$ in $\mathcal{C}^i$. This implies that $\mathbf{v} \in \mathrm{Ker}(\Psi_i^{i+1})$. By Lemma 2.10(iii), we get that $\mathbf{v} = \gamma^i\mathbf{v}_0$, where $\mathbf{0} \neq \mathbf{v}_0 \in \mathcal{C}^1$. This means that $0 < w_H(\mathbf{v}_0) = w_H(\mathbf{v}) < d$, which is a contradiction.

(ii) If there exists a non-zero codeword $\mathbf{v} \in \mathcal{C}$ such that $w_H(\mathbf{v}) < d$, then let N be a sufficiently large integer such that $\Psi_N(\mathbf{v}) \neq \mathbf{0}$. We would have that $w_H(\Psi_N(\mathbf{v})) \leq w_H(\mathbf{v}) < d$, which is a contradiction. □

In the remainder of this section, we focus on MDS and MDR codes. It is well known (see [7]) that for codes C of length n over any alphabet of size m

$$d_H(C) \leq n - \log_m(|C|) + 1. \tag{17}$$

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

For a code C of length n over an finite Quasi-Frobenius ring R, Horimoto and Shiromoto (see [6]) define the following:

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

If C is linear, then we have (see [6])

$$d_H(C) \leq n - r_C + 1. \tag{18}$$

Codes meeting this bound are called MDR (*Maximal Distance with respect to Rank*) codes. For codes over R_∞ we say that an MDR code is MDS if it is of type 1^k for some k. See [4] and [5] for a discussion of this bound for several rings.

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

Theorem 2.12. *Let $\mathcal{C}$ be a linear code over R_∞. If $\mathcal{C}$ is an MDR or MDS code then $\mathcal{C}^\perp$ is an MDS code.*

Proof. Assume $\mathcal{C}$ is a code of length n and rank k with $d_H(\mathcal{C}) = n-k+1$. Then we know that $\mathcal{C}^\perp$ is type 1^{n-k}. Since R_∞ is a domain, we get that any $n-k$ columns of the generator matrix of $\mathcal{C}^\perp$ are linearly independent. This gives that the minimum Hamming weight of $\mathcal{C}^\perp$ is $n-(n-k)+1 = k+1$. □

Theorem 2.13. *Let C be a linear code over R_i, and $\tilde{C}$ be a lift code of C over R_j, where $j > i$. If C is an MDS code over R_i then the code $\tilde{C}$ is an MDS code over R_j.*

Proof. Assume C is a $[n, k]$ code with minimum Hamming distance d_H. We have that $d_H = n-k+1$ since C is an MDS code. Let $\mathbf{v}$ be a codeword of C such that $w_H(\mathbf{v}) = d_H$. Then for any nonzero codeword $\mathbf{v}' \in C$, we have that $w_H(\mathbf{v}') \geq w_H(\mathbf{v})$. We know that $\tilde{C}$ is a $[n, k]$ code, and that $\mathbf{v}$ can be viewed as a codeword of $\tilde{C}$ since we can write $\mathbf{v} = (v_1, \cdots, v_n)$ where

$$v_l = a_0^l + a_1^l\gamma + \cdots + a_{i-1}^l\gamma^{i-1} + 0\gamma^i + \cdots + 0\gamma^{j-1}.$$

Let $\mathbf{w}$ be any lifted codeword of $\mathbf{v}$. Then we have that $w_H(\mathbf{w}) \geq w_H(\mathbf{v})$. On the other hand, for any lift codeword $\mathbf{w}'$ of $\mathbf{v}'$, where $\mathbf{v}' \in C$, we also have that $w_H(\mathbf{w}') \geq w_H(\mathbf{v}') \geq w_H(\mathbf{v})$. This means that the minimum Hamming weight of $\tilde{C}$ is d_H and this implies that $\tilde{C}$ is an MDS code for all $j > i$. □

3. Self-Dual γ-adic Codes

In this section, we describe self-dual codes over R_∞. We 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. The following theorem can be found from [7].

Theorem 3.1. *(i) If $p = 2$ or $p \equiv 1 \pmod 4$, then a self-dual code of length n exists over $\mathbb{F}_q$ if and only if $n \equiv 0 \pmod 2$;*

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

Theorem 3.2. *If i is even, then self-dual codes of length n exist over R_i for all n.*

Proof. Let C be the code with generator matrix $G = \gamma^{\frac{i}{2}} I_n$. It is clear that C is self-orthogonal over R_i since $\gamma^{\frac{i}{2}}\gamma^{\frac{i}{2}} = \gamma^i = 0$ in R_i. We have that $|C| = (q^{\frac{i}{2}})^n = (q^i)^{\frac{n}{2}} = |R_i|^{\frac{n}{2}}$. Therefore C is self-dual. □

Theorem 3.3. *Let i be odd and C be a code over R_i with type $1^{k_0}(\gamma)^{k_1}(\gamma^2)^{k_2}\cdots(\gamma^{i-1})^{k_{i-1}}$. Then C is a self-dual code if and only if C is self-orthogonal and $k_j = k_{i-j}$ for all j.*

Proof. We know that $C^\perp$ has type $1^{k_i}(\gamma)^{k_{i-1}}(\gamma^2)^{k_{i-2}}\cdots(\gamma^{i-1})^{k_1}$. Hence the only if part follows. Now assume that C is a self-orthogonal code of length n and $k_j = k_{i-j}$ for all j. Let $l = \lfloor \frac{i}{2} \rfloor$, where $\lfloor\ \rfloor$ denotes the greatest integer function. Since i is odd, we have

$$n = \sum_{j=0}^{i} k_j = 2\sum_{j=0}^{\frac{i-1}{2}} k_j = 2\sum_{j=0}^{l} k_j. \tag{19}$$

Since C is self-orthogonal, C is self-dual if and only if $|C| = (q^i)^{\frac{n}{2}}$. We have that

$$\log_q |C| = \sum_{j=0}^{i-1}(i-j)k_j = i\sum_{j=0}^{i-1}k_j - \sum_{j=0}^{i-1} jk_j = in - \sum_{j=0}^{i} jk_j = in - S,$$

where $S = \sum\limits_{j=0}^{i} jk_j$. By Equation (19), we have that

$$\begin{aligned} S &= \sum_{j=0}^{i-1} jk_j + i(n - \sum_{j=0}^{i-1} k_j) = in - \sum_{j=0}^{i}(i-j)k_j \\ &= in - \sum_{j=0}^{i}(i-j)k_{i-j} = in - \sum_{j=0}^{i} jk_j = in - S. \end{aligned}$$

This implies that $S = \frac{in}{2}$ and $\log_q |C| = in - \frac{in}{2} = \frac{in}{2}$. Therefore C is self-dual. □

Theorem 3.4. *If $\mathcal{C}$ is a self-dual code of length n over R_∞ then $\Psi_i(\mathcal{C})$ is a self-dual code of length n over R_i for all $i < \infty$.*

Proof. Since $\mathcal{C}$ is a self-dual, we have that $\mathcal{C} = \mathcal{C}^{\perp}$. This gives that $\mathcal{C} = \mathcal{C}^{\perp} = (\mathcal{C}^{\perp})^{\perp}$. By Proposition 2.7, the code $\mathcal{C}$ has type 1^k for some k. Hence we have that $k = n - k$, this gives that $k = \frac{n}{2}$. It is easy to get that $\mathrm{rank}(\Psi_i(\mathcal{C})) = \frac{n}{2}$ and so $\Psi_i(\mathcal{C})$ has $(p^{ri})^{\frac{n}{2}}$ elements. By Proposition 2.8, $\Psi_i(\mathcal{C})$ is self-orthogonal. Therefore $\Psi_i(\mathcal{C})$ is a self-dual code. □

Corollary 3.5. *Let $\mathcal{C}$ be a self-dual code of length n over R_∞. Recall that p is the characteristic of the underlying field $\mathbb{F}$. We have*

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

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

Proof. This result follows by Theorem 3.4 and Theorem 3.1. □

The following theorem gives a method to construct a self-dual code over $\mathbb{F}$ from a self-dual code over R_i.

Theorem 3.6. *Let i be odd. A self-dual code of length n over R_i induces a self-dual code of length n over $\mathbb{F}_q$.*

Proof. Let C be a code over R_i of type $1^{k_0}(\gamma)^{k_1}(\gamma^2)^{k_2}\cdots(\gamma^{i-1})^{k_{i-1}}$ with standard generator matrix G as follows:

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

Let

$$\tilde{G} = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & & & A_{0,i} \\ & I_{k_1} & A_{1,2} & A_{1,3} & & & A_{1,i} \\ & & I_{k_2} & A_{2,3} & & & A_{2,i} \\ & & & \ddots & \ddots & & \\ & & & \ddots & \ddots & \ddots & \\ & & & & & I_{k_l} & A_{l,i} \end{pmatrix},$$

where $l = \lfloor \frac{i}{2} \rfloor$. By Equation (19), $\tilde{G}$ is a $(\frac{n}{2}) \times n$ matrix over R_i. Let $\tilde{\tilde{G}} = \Psi_1^i(\tilde{G})$ be the matrix over $\mathbb{F}_q$ and let $\tilde{\tilde{C}}$ be the code over $\mathbb{F}_q$ with generator matrix $\tilde{\tilde{G}}$. It is clear that $\mathrm{rank}(\tilde{\tilde{C}}) = \frac{n}{2}$, and thus it remains to show that $\tilde{\tilde{C}}$ is self-orthogonal. Let $\mathbf{v}'', \mathbf{w}''$ be any two row vectors of $\tilde{\tilde{G}}$, suppose $\mathbf{v}'' = \Psi_1^i(\mathbf{v}')$ and $\mathbf{w}'' = \Psi_1^i(\mathbf{w}')$, where $\mathbf{v} = \gamma^s \mathbf{v}'$ and $\mathbf{w} = \gamma^t \mathbf{w}'$ are row vectors of G with $s, t \leq l$. We have that

$$0 = [\mathbf{v}, \mathbf{w}] = [\gamma^s \mathbf{v}', \gamma^t \mathbf{w}'] = \gamma^{s+t}[\mathbf{v}', \mathbf{w}'].$$

This implies that $[\mathbf{v}', \mathbf{w}'] = 0$ since $s+t < i$. In particular, the constant term in their inner product is zero. This means that $[\mathbf{v}'', \mathbf{w}''] = [\mathbf{v}', \mathbf{w}'] = 0$. □

Theorem 3.7. *Let $R = R_e$ be a finite chain ring, $\mathbb{F} = R/\langle\gamma\rangle$, where $|\mathbb{F}| = q = p^r, 2 \neq p$ a prime. Then any self-dual code C over $\mathbb{F}$ can be lifted to a self-dual code over R_∞.*

Proof. Let $G_1 = (I \mid A_1)$ be a generator matrix of C over $R_1 (= \mathbb{F})$. Since C is self-orthogonal, we have that

$$I + A_1 A_1^T \equiv 0 \pmod{\gamma}.$$

We show in the following by induction that there exist matrices $G_i = (I \mid A_i)$ such that $\Psi_i^{i+1}(G_{i+1}) = G_i$ and $I + A_i A_i^T \equiv 0 \pmod{\gamma^i}$ for all i. Suppose we have that $I + A_i A_i^T = \gamma^i S_i$. Let $A_{i+1} = A_i + \gamma^i M$, we want to find a matrix M such that

$$I + A_{i+1} A_{i+1}^T \equiv 0 \pmod{\gamma^{i+1}}. \tag{20}$$

We know

$$\begin{aligned} I + A_{i+1} A_{i+1}^T &= I + A_i A_i^T + \gamma^i (A_i M^T + M A_i^T) \\ &= \gamma^i (S_i + A_i M^T + M A_i^T). \end{aligned}$$

This gives that the matrix M should satisfy

$$S_i + A_i M^T + M A_i^T \equiv 0 \pmod{\gamma}. \tag{21}$$

In order to find all solutions to this equation, we consider the map $\eta : M_n(\mathbb{F}) \to M_n(\mathbb{F})$ defined by $\eta(M) = A_i M^T + M A_i^T$. It is easy to get that η is linear and the kernel of η is

$$\mathrm{Ker}(\eta) = \{K A_i \mid \text{where } K \text{ is skew-symmetric}\}.$$

It follows since $A_i M^T + M A_i^T = 0$ if and only if $(M A_i^T)^T + M A_i^T = 0$ if and only if $M A_i^T = K$ is skew-symmetric if and only if $M = K(A_i^T)^{-1} = -K A_i$.

Note that $A_iA_i^T = -I$ over $\mathbb{F}$ and $\gcd(2,p) = 1$. This implies that 2 is a unit in $\mathbb{F}$. Hence

$$\eta(2^{-1}S_iA_i) = 2^{-1}(A_iA_i^tS_i^T + S_iA_iA_i^T) = 2^{-1}(-2)S_i = -S_i.$$

Therefore the solutions to (20) exist and they are given by

$$A_{i+1} = A_i + \gamma^i M,$$

where $M \equiv 2^{-1}(S_i + K)A_1 \pmod{\gamma}$ with any skew-symmetric K. □

References

[1] Dougherty S. T., Kim S. Y., Park Y. H., *Lifted codes and their weight enumerators*, Discrete Math., **305**, 2005, 123–135.

[2] Dougherty S. T., Liu H., *Independence of Vectors in Codes over Rings*, to appear in Des. Codes and Cryptogr.

[3] Dougherty S.T., Park Y.H., *Codes over the p-adic integers*, Des. Codes and Cryptogr., **39**, 2006, 65–80.

[4] Dougherty S.T., Shiromoto K., *MDR Codes over Z_k*, IEEE Trans. Inform. Theory, **46**, 2000, 265–269.

[5] Dougherty S.T., Shiromoto K., Maximum Distance Codes over Rings of Order 4, IEEE-IT, **47**, No 1, January 2001.

[6] Horimoto, H. and Shiromoto, K., *A Singleton bound for linear codes over quasi-Frobenius rings*, Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, Hawaii (USA), 1999, 51–52.

[7] W.C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes (with W. C. Huffman), Cambridge University Press, 2003.

[8] Hungerford T.W., Algebra, Springer-Verlag, New York, 1974.

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

[10] Norton G. H., Sălăgean A., *On the Hamming distance of linear codes over a finite chain ring*, IEEE Trans. Inform. Theory, **46**, 2000, 1060–1067.

Steven T. Dougherty
Department of Mathematics
University of Scranton
Scranton, PA 18510, USA

e-mail address: doughertys1@scranton.edu

Hongwei Liu
Department of Mathematics
Huazhong Normal University
Wuhan, Hubei 430079, P. R. China

e-mail address: h_w_liu@yahoo.com.cn

Young Ho Park
Department of Mathematics
Kangwon National University
Chuncheon 200-701, Korea
e-mail address: yhpark@kangwon.ac.kr

(*Received December 10, 2008*)
(*Revised November 10, 2009*)