ISIT'2013 1569719903

Subsystem Codes over Nice Nearrings

Sangjun Lee
Department of Computer Science and Engineering
Texas A&M University
College Station, TX 77843-3112, USA

Andreas Klappenecker
Department of Computer Science and Engineering
Texas A&M University
College Station, TX 77843-3112, USA

***Abstract*—Subsystem codes are quantum error correcting schemes unifying stabilizer codes, decoherence free subspaces and noiseless subsystems. Subsystem codes were most commonly based on the generalized Pauli basis with dimensions of a power of prime. Recently, a class of nice error bases indexed by a nearring were introduced by the second author. We give a construction of subsystem codes over nice nearrings. Furthermore, we show that free subsystem codes over a finite chain ring cannot perform better than those over a finite field.**

I. Introduction

Subsystem codes are one of the promising quantum error correction schemes for the fault-tolerant quantum computation. The subsystem code formalism unifies the features of stabilizer codes, decoherence free subspaces, and noiseless subsystems [5], [6], [1]. The main idea of the subsystem code is to decompose a subspace C of the Hilbert space H into a tensor product of the subsystem A and the co-subsystem B and encode the quantum information in the subsystem [5], [6], [4] such that

$$H = C \oplus C^{\perp} = (A \otimes B) \oplus C^{\perp}.$$

Since all quantum information is stored in the subsystem A, there is no need to correct any errors affecting only the co-subsystem B.

Quantum error correcting codes that have been studied so far, including the subsystem codes, are mostly based on finite field arithmetic. Recently, nice error bases indexed by a nearring were introduced [3]. The advantage of the nearring formalism is that it allows one to form quantum codes over any finite alphabet size, not just powers of a prime.

As one of efforts to utilize nice error bases indexed by a nearring, the construction of stabilizer codes over distributively generated nice nearrings was studied in [7]. It turns out that distributively generated nice nearrings are finite Frobenius rings [3], so the paper [7] was still confined to rings. In this paper, we give a construction of subsystem codes over nice nearrings. Thus, we generalize the results of [7] by (a) allowing for a more general nice nearring arithmetic, and (b) generalizing from stabilizer codes to subsystem codes.

This paper is structured as follows. In Section II, we recall the definition of a nice nearring and give some mathematical background. In Section III, we show that the construction of subsystem codes over a nice nearring can be done from a Clifford code construction. In the following section, the construction of subsystem codes from classical additive codes over a distributively generated nice nearring is discussed. And finally, we provide some clues whether the subsystem codes over a finite chain ring can outperform those over a finite field in Section V.

II. Preliminaries

In this section, we provide fundamental information about nice nearrings and their properties, see [3]. First of all, the definition of a nearring is introduced as follows.

A set N under an addition operation $+$ and a multiplication operation $\cdot$ is called a (left) nearring if it satisfies

1) $(N, +)$ is a (not necessarily abelian) group,
2) $(N, \cdot)$ is a semigroup,
3) and the left-distributive law $x(y + z) = xy + xz$ holds for all x,y,z $\in N$.

A nearring has fewer constraints than a finite field, so some nearrings offer an arithmetic that is simpler to implement than finite field arithmetic.

Let N be a nearring with q elements, where $2 \leq q < \infty$. We denote by

$$\{|x\rangle | x \in N\}$$

a fixed orthonormal basis of $\mathbb{C}^q$. Let χ be a character of $(N, +)$. For all $a, b \in N$, we define a shift operator $X(a) : \mathbb{C}^q \to \mathbb{C}^q$ and a multiplication operator $Z(b) : \mathbb{C}^q \to \mathbb{C}^q$ by

$$X(a)|x\rangle = |x + a\rangle, \qquad Z(b)|x\rangle = \chi(bx)|x\rangle,$$

for all $x \in N$.

A finite nearring is called nice if and only if there exists a character χ of $(N, +)$ such that $\mathcal{E} = \{X(a)Z(b) | a, b \in N\}$ is a nice error basis (that is, $\mathcal{E}$ contains the identity, is closed under multiplication up to scalars, and is an orthogonal basis with respect to the Hilbert-Schmidt inner product). If N is a nice nearring and $\mathcal{E}$ is a nice error basis indexed by N with respect to the character χ, then we call χ a generating character.

If a finite nearring is nice, then it satisfies the following properties.

Proposition 1 ([3])**.** *If N is a nice nearring, then*

1) *a generating character χ of $(N, +)$ is a linear and irreducible,*
2) *$(N, +)$ is an abelian group,*
3) *and $(N, \cdot)$ has a unique left identity.*

Proof: See [3, Proposition 3 and 6]. ■

So a nice nearring has considerably more structure than a general nearring, but does not need to be right-distributive.

A nice error basis $\mathcal{E}$ can be extended to n components by tensoring,

$$\mathcal{E}^{\otimes n} = \{M_1 \otimes \cdots \otimes M_n \,|\, M_k \in \mathcal{E}, 1 \leq k \leq n\}.$$

This yields a nice error basis of $\mathbb{C}^{q^n}$. The elements in $\mathcal{E}$ generalize the Pauli matrices, and the nice error basis $\mathcal{E}^{\otimes n}$ is the generalization of the Pauli basis on n qubits.

A nice error basis is not a group, since it is not closed under multiplication. The group generated by a nice error basis is called an error group. In our case, the error group of $\mathcal{E}^{\otimes n}$ is given by

$$E_n = \{\chi(c)X(a)Z(b)|a, b \in N^n, c \in N\}. \tag{1}$$

This is a finite group with center $Z(E_n) = \{\chi(c)1|c \in N\}$, where 1 is the identity.

Suppose an error e in E_n is given by $\chi(c)X(a)Z(b)$ for $a, b \in N^n$ and $c \in N$. Then the weight $\mathrm{wt}(e)$ of the error e is defined as the number of its tensor components which are not scalar multiples of the identity. Similarly, given $(a|b) \in N^{2n}$, we can introduce its symplectic weight by

$$\mathrm{swt}(a|b) = |\{i|a_i \neq 0 \text{ or } b_i \neq 0, 1 \leq i \leq n\}|.$$

Thus, we have the relation $\mathrm{wt}(\chi(c)X(a)Z(b)) = \mathrm{swt}(a|b)$ between these two types of weights.

Notation: Let G be a group, and H a subgroup of G. The centralizer $\{g \in G \,|\, gh = hg \text{ for all } h \in H\}$ of H in G is denoted by $C_G(H)$. The center $C_G(G)$ of G is denoted by $Z(G)$. For $x, y \in G$, the commutator $[x, y]$ is defined as $x^{-1}y^{-1}xy$. Given subgroups X and Y of G, we define $[X, Y] = \langle [x, y]|x \in X, y \in Y\rangle$. As usual, we denote the commutator subgroup $[X, X]$ by X'.

III. Construction of Subsystem Codes over a Nice Nearring

In this section, we give the construction of subsystem codes over nice nearrings. For this purpose, we use the more general theory of Clifford subsystem codes, see [4].

Let M be a normal subgroup of an error group E_n and χ an irreducible character of M. The inertia group of χ is given by

$$I_{E_n}(\chi) = \{g \in E_n \,|\, \chi(gng^{-1}) = \chi(n) \text{ for all } n \in M\}.$$

The inertia group of a character determines the parameters of the subsystem code in the following theorem from [4]:

Theorem 2 ([4])**.** *Let E_n be an error group such that $E_n' \subseteq Z(E_n)$, M a normal subgroup of E_n, and χ an irreducible character of M chosen such that the orthogonal projector*

$$P = \frac{\chi(1)}{|N|} \sum_{n \in N} \chi(n^{-1})n$$

is nonzero.[1] *Then $C = image(P)$ is the corresponding Clifford code. The inertia group of χ is given by $I_{E_n}(\chi) = C_{E_n}(Z(M))$. If $C_{E_n}(Z(M)) = LM$ for some subgroup L of E_n such that $[L, M] = 1$, then C is a subsystem code $C = A \otimes B$ such that*

1) $\dim A = |Z(E_n) \cap M||E_n : Z(E_n)|^{1/2}|M : Z(M)|^{1/2}/|M|$,
2) $\dim B = |M : Z(M)|^{1/2}$.

An error e in E_n is detectable by subsystem A if and only if e is contained in the set $E_n \setminus (C_{E_n}(Z(M)) \setminus Z(L)M)$.

Proof: See [4, Theorem 2]. ∎

We will show that Theorem 2 can be used to construct subsystem codes over nice nearrings. For this purpose, we will prove that (a) the error group given in (1) satisfies $E_n' \subseteq Z(E_n)$ and (b) give a convenient condition on M which ensures that the inertia group factorizes into a central product of the form required by Theorem 2. The next two lemmas will establish the required facts.

Lemma 3. *Let N be a finite nice nearring. The error group $E_n = \{\chi(c)X(a)Z(b)|a, b \in N^n, c \in N\}$ satisfies $E_n' \subseteq Z(E_n)$.*

Proof: From the definitions of the shift operator and the multiplication operator, we know that $X(a)X(b) = X(a + b)$ and $Z(a)Z(b) = Z(a+b)$ for $a, b \in N$. Furthermore, we have $\chi(ba)X(a)Z(b) = Z(b)X(a)$. Since $Z(E_n) = \{\chi(c)1|c \in N\}$, the quotient group $E_n/Z(E_n)$ is isomorphic to N^{2n}. By Proposition 1, a nice nearring is an abelian group under addition. In other words, $E_n/Z(E_n)$ is abelian, and it follows that $E_n' \subseteq Z(E_n)$, as claimed. ∎

Our next concern is to find a convenient sufficient condition which ensures that $C_{E_n}(Z(M))$ factors into a central product of the form LM for some subgroup L of E_n.

A subgroup H of a group is called c-closed if and only if $H = C_G(C_G(H))$ holds. This terminology is motivated by the fact that the centralizer map $x \mapsto C_G(x)$ yields a Galois connection on the lattice of subsets of the group G.

Lemma 4. *Let E_n be an error group. Let M be a c-closed normal subgroup of the error group E_n such that $MC_{E_n}(M)$ is c-closed. Then*

$$C_{E_n}(Z(M)) = MC_{E_n}(M).$$

Proof: Since $MC_{E_n}(M)$ and M are c-closed, we have

$$\begin{aligned} MC_{E_n}(M) &= C_{E_n}(C_{E_n}(MC_{E_n}(M))) \\ &= C_{E_n}(C_{E_n}(M) \cap C_{E_n}(C_{E_n}(M))) \\ &= C_{E_n}(C_{E_n}(M) \cap M) \\ &= C_{E_n}(C_M(M)) = C_{E_n}(Z(M)), \end{aligned}$$

which proves the claim. ∎

The existence of normal subgroups satisfying the hypothesis of the previous lemma follows from a well-known group-theoretic result by Chermak and Delgado, see [2]. We can now

[1] We can always find such a character. Notice that the parameters of the resulting code do not depend on the particular choice of χ.

combine the previous results and formulate the construction of subsystem codes over nice nearrings in the following form:

Corollary 5. *Let E_n be the error group given in (1) over a nice nearring N. Let M be a c-closed normal subgroup of E_n such that $MC_{E_n}(M)$ is c-closed. Then there exists a subsystem code $C = A \otimes B$ such that*

1) $\dim A = |Z(E_n) \cap M||E_n : Z(E_n)|^{1/2}|M : Z(M)|^{1/2}/|M|$,
2) $\dim B = |M : Z(M)|^{1/2}$.

An error e in E_n is detectable by subsystem A if and only if e is contained in the set $E_n \setminus (MC_{E_n}(M) \setminus M)$.

Proof: By Lemma 3, the error group satisfies $E_n' \subseteq Z(E_n)$. By Theorem 2, the inertia group is of the form $C_{E_n}(Z(M)$. This inertia group factorizes into the central product

$$C_{E_n}(Z(M)) = MC_{E_n}(M),$$

with $[M, C_{E_n}(M)] = 1$, by Lemma 4. Furthermore, we have

$$\begin{aligned} Z(C_{E_n}(M)) &= C_{E_n}(C_{E_n}(M)) \cap C_{E_n}(M) \\ &= M \cap C_{E_n}(M) = Z(M) \leq M. \end{aligned}$$

Thus, the claim is obtained from Theorem 2 using $L = C_{E_n}(M)$ and the fact that $Z(L)$ is a subset of M. ∎

In the next section, we will remove the assumption on the normal subgroup M in the case of rings.

IV. Construction of Subsystem Codes over a Nice Ring

In this section, we will assume that N is a distributively generated nice nearring. A distributively generated nearring is nice if and only if it is a finite Frobenius ring [3]. Finite Frobenius rings play a prominent role in classical coding theory. We will relate the construction of subsystem codes over nice rings to classical codes over rings.

Let N be a nice ring. For $u = (a|b)$ and $v = (a'|b')$ in N^{2n}, we define

$$\langle u|v\rangle = \chi(b \cdot a' - b' \cdot a).$$

We write $u \perp v$ if and only if $\langle u|v\rangle = 1$ holds. Thus, $X(a)Z(b)$ and $X(a')Z(b')$ commute if and only if $u \perp v$. For a subset $S \subseteq N^{2n}$, we define

$$\begin{aligned} S^{\perp} &= \{u \in N^{2n} \mid \langle s|u\rangle = 1 \text{ for all } s \in S\} \\ {}^{\perp}S &= \{u \in N^{2n} \mid \langle u|s\rangle = 1 \text{ for all } s \in S\} \end{aligned}$$

One can show that for a subgroup C of N^{2n}, we have

$$|C||C^{\perp}| = |{}^{\perp}C||C| = |N^{2n}|,$$

see [7, Lemma 6].

For a subgroup G of the error group E_n, we use the bar notation $\overline{G}$ to denote $G/Z(E_n)$.

A key element in the construction of subsystem codes is the decomposition of the inertia group of the character χ into a central product (the groups L and M in Theorem 2). The next lemma shows that this is always possible when N is a nice ring.

Without loss of generality, we may assume that the normal subgroup M of the error group E_n contains the center $Z(E_n)$ of the error group. If M does not contain $Z(E_n)$, then simply use the larger group $MZ(E_n)$,

Lemma 6. *Let N be a finite nice ring. If E_n is a set $\{\chi(c)X(a)Z(b)|a, b \in N^n, c \in N\}$ and M is a normal subgroup of E_n, then $C_{E_n}(Z(M)) = MC_{E_n}(M)$.*

Proof: We first notice that $MC_{E_n}(M)$ is a subgroup of $C_{E_n}(Z(M))$, and that both groups contain the center $Z(E_n)$ of the error group. Thus, it suffices to show that the cardinality of the quotient groups $\overline{MC_{E_n}(M)}$ and $\overline{C_{E_n}(Z(M))}$ are the same. We have

$$\begin{aligned} |\overline{MC_{E_n}(M)}| &= |\overline{M} + \overline{M}^{\perp}| \\ &= |\overline{M}||\overline{M}^{\perp}|/|\overline{M} \cap \overline{M}^{\perp}| \\ &= |\overline{M}||\overline{M}^{\perp}|/|\overline{Z(M)}| \\ &= |N^{2n}|/|\overline{Z(M)}| \\ &= |\overline{Z(M)}^{\perp}| \\ &= |\overline{C_{E_n}(Z(M))}|, \end{aligned}$$

which proves our claim. ∎

From the previous two results, we can conclude the following theorem about the construction of subsystem codes over a nice ring.

Theorem 7. *Let N be a finite nice ring. Suppose the error group E_n is a set $\{\chi(c)X(a)Z(b)|a, b \in N^n, c \in N\}$. If C is a Clifford code with data (E_n, ρ, M, χ) with $M \neq 1$, then C is a subsystem code $C = A \otimes B$ such that*

1) $\dim A = |Z(E_n) \cap M||E_n : Z(E_n)|^{1/2}|M : Z(M)|^{1/2}/|M|$,
2) $\dim B = |M : Z(M)|^{1/2}$.

An error e in E_n is detectable by subsystem A if and only if e is contained in the set $E_n - (MC_{E_n}(M) - M)$.

Proof: By Lemma 3, the error group E_n satisfies $E_n' \subseteq Z(E_n)$. Thus, the inertia group $I_{E_n}(\chi) = C_{E_n}(Z(M))$. By Lemma 6, we have $C_{E_n}(Z(M)) = MC_{E_n}(M)$. Since $C_{E_n}(M) \leq E_n$ and $[C_{E_n}(M), M] = 1$, the resulting Clifford code is a subsystem code $C = A \otimes B$ with $\dim A$ and $\dim B$ as given in Theorem 2.

In addition, since $Z(E_n) \leq M$ and $[C_{E_n}(M), M] = 1$, $\overline{Z(C_{E_n}(M))} \subseteq \overline{C_{E_n}(M)} \cap \overline{C_{E_n}(M)}^{\perp} \subseteq \overline{M}^{\perp} \cap \overline{M} \subseteq \overline{M}$. Thus, we have the relation $M \subseteq Z(C_{E_n}(M))M \subseteq M$, which means $Z(C_{E_n}(M))M = M$. Therefore, an error e in E_n is detectable if and only if $e \in E_n - (MC_{E_n}(M) - M)$. ∎

Now we are ready to construct subsystem codes from classical additive codes over a nice ring.

Theorem 8. *Let N be a nice ring with q elements. Let X be a classical additive subcode of N^{2n} such that $X \neq \{0\}$ and let Y denote its subcode $Y = X \cap X^{\perp}$. Let $x = |X|$ and $y = |Y|$. Then, there exists a subsystem code $C = A \otimes B$ such that*

1) $\dim A = q^n/(xy)^{1/2}$,
2) $\dim B = (x/y)^{1/2}$.

The minimum distance of subsystem A is given by $d = \mathrm{swt}((X + X^{\perp}) - X) = \mathrm{swt}(Y^{\perp} - X)$. *Thus, the subsystem A can detect all errors in* E_n *of weight less than d, and can correct all errors in* E_n *of weight* $\leq \lfloor (d-1)/2 \rfloor$.

Proof: Let E_n be the nice error group given earlier in this paper, and let M be the full preimage of $\overline{M} = X$ in E_n under the canonical quotient map. Then, we can apply Theorem 7 to prove the theorem.

Since $\overline{Z(M)} = X \cap X^{\perp} = Y$, $|M : Z(M)| = |\overline{M} : \overline{Z(M)}| = x/y$. Thus, $\dim B = (x/y)^{1/2}$. From the fact that $Z(E_n) \leq M$ by definition, $|Z(E_n) \cap M|/|M| = 1/\overline{M} = 1/x$. Therefore, $\dim A = |E_n : Z(E_n)|^{1/2}/(xy)^{1/2} = q^n/(xy)^{1/2}$.

Since $\mathrm{wt}(e) = \mathrm{swt}(\overline{e})$ for an error $e \in E_n$, the minimum distance of subsystem A is $\mathrm{wt}(MC_{E_n}(M) - M) = \mathrm{swt}(\overline{MC_{E_n}(M) - M}) = \mathrm{swt}((X + X^{\perp}) - X)$. Equivalently, $\mathrm{wt}(C_{E_n}(Z(M)) - M) = \mathrm{swt}(\overline{C_{E_n}(Z(M)) - M}) = \mathrm{swt}(Y^{\perp} - X)$. ∎

Let N be a nice ring. Suppose $K = \dim A$, $L = \dim B$ and d is a minimum distance of subsystem A. Then, a subsystem code Q over a nice ring is called an $((n, K, L, d))_N$ subsystem code. We also write $[[n, k, l, d]]_N$ for an $((n, q^k, q^l, d))_N$ subsystem code, where q is the number of elements in N. By slight abuse of language, we will also refer to d as the minimum distance of the subsystem code Q, cf. [1].

Next, we will derive a special case of Theorem 8, which constructs a subsystem code over a nice ring with the help of two classical linear codes over a nice ring of the same length n. This generalizes a result from [1] by allowing finite rings instead of finite fields.

Let a, b, a', b' be in N^n. We define a form $\langle \cdot | \cdot \rangle_s : N^{2n} \times N^{2n} \to N$ by

$$\langle (a|b)|(a'|b') \rangle_s = b \cdot a' - b' \cdot a.$$

Suppose u and v are in N^{2n} such that $u = (a|b)$ and $v = (a'|b')$. Then, we define the orthogonality $u \perp_s v$ if and only if $\langle u|v \rangle_s = 0$.

Lemma 9. *Let* C_1 *and* C_2 *be two linear codes over a nice ring* N *such that* $C_1 \leq N^n$ *and* $C_2 \leq N^n$. *The product code* $C_1 \times C_2 = \{(a|b) | a \in C_1, b \in C_2\}$ *has length* $2n$ *and its dual is given by*

$$(C_1 \times C_2)^{\perp_s} = C_2^{\perp_s} \times C_1^{\perp_s}$$

Proof: If $(a|b) \in C_1 \times C_2$ and $(b'|a') \in C_2^{\perp_s} \times C_1^{\perp_s}$, then $\langle (a|b)|(b'|a') \rangle = b \cdot b' - a' \cdot a = 0$. Thus, $C_2^{\perp_s} \times C_1^{\perp_s} \subseteq (C_1 \times C_2)^{\perp_s}$. Since $|(C_1 \times C_2)^{\perp_s}| = |N|^{2n}/|C_1 \times C_2| = |N|^{2n}/|C_1||C_2| = |N|^n/|C_2| \cdot |N|^n/|C_1| = |C_2^{\perp_s} \times C_1^{\perp_s}|$, we can conclude that $(C_1 \times C_2)^{\perp_s} = C_2^{\perp_s} \times C_1^{\perp_s}$. ∎

Corollary 10. *Let* N *be a nice ring with* q *elements. Let* C_i *be* $[n, k_i]$ *linear codes in* N^n *for* $i \in \{1, 2\}$. *Then, there exists an* $((n, K, L, d))_N$ *subsystem code with*

1) $K = q^{n-(k_1+k_2)/2}/|D|^{1/2}$,
2) $L = q^{(k_1+k_2)/2}/|D|^{1/2}$,
3) $d = \min\{\mathrm{wt}((C_1^{\perp_s} \cap C_2)^{\perp_s} \backslash C_1), \mathrm{wt}((C_2^{\perp_s} \cap C_1)^{\perp_s} \backslash C_2)\}$,

where $|D| = |C_1 \cap C_2^{\perp_s}||C_2 \cap C_1^{\perp_s}|$.

Proof: Let $C = C_1 \times C_2$, then by Lemma 9, $C^{\perp_s} = C_2^{\perp_s} \times C_1^{\perp_s}$. Using C and $C^{\perp_s}$, we get $D = C \cap C^{\perp_s} = (C_1 \cap C_2^{\perp_s}) \times (C_2 \cap C_1^{\perp_s})$. Since $|C| = |C_1||C_2| = q^{k_1+k_2}$, we can obtain that $K = q^{n-(k_1+k_2)/2}/|D|^{1/2}$ and $L = q^{(k_1+k_2)/2}/|D|^{1/2}$ by Theorem 8. The distance of the code is provided in Theorem 8 by

$$\begin{aligned} d &= \mathrm{swt}(D^{\perp_s} \backslash C) \\ &= \mathrm{swt}((C_2 \cap C_1^{\perp_s})^{\perp_s} \times (C_1 \cap C_2^{\perp_s})^{\perp_s} \backslash (C_1 \times C_2)), \end{aligned}$$

which can be simplified to

$$d = \min\{\mathrm{wt}((C_2 \cap C_1^{\perp_s})^{\perp_s} \backslash C_1), \mathrm{wt}((C_1 \cap C_2^{\perp_s})^{\perp_s} \backslash C_2)\}.$$

Therefore, we can have an $((n, K, L, d))_N$ subsystem code from C_1 and C_2. ∎

In particular, an subsystem code $((n, K, L, d))_N$ with simplified code parameters can be obtained by setting $C_1 = C_2$, where $K = q^{n-k}/|D|$, $L = q^k/|D|$, $|D| = |C_1 \cap C_1^{\perp_s}|$ and $d = wt((C_1 \cap C_1^{\perp_s})^{\perp_s} \backslash C_1)$.

V. Subsystem Codes over a Ring and a Field

Now, we will discuss a finite chain ring to show how to derive the subsystem code over a field from the subsystem code over a ring. A finite chain ring is a well-known ring structure for a classical code [9], [8]. Since ideals of a finite chain ring construct a form of a chain, it has a unique maximal ideal. A finite chain ring is Frobenius ring, which implies that a finite chain ring is a nice distributively generated nearring [3]. In order to discuss the relation between the subsystem code over a ring and a finite field, we restrict our focus into a finite chain ring.

Let R be a finite chain ring with the Jacobson radical $J(R)$ and the nilpotency index ν. Then, $J(R)$ is the maximal ideal of R since a finite chain ring is a local ring and it has a unique maximal ideal. Thus, the quotient ring $R/J(R)$ becomes a field. Let F be such a residue field. Suppose that a field $R/J(R)$ has q elements. Then, we have $|R| = q^{\nu}$ and $|J(R)| = q^{\nu-1}$ [9].

Let $c \in R^n$. We denote by $\overline{c}$ the image of c under the canonical projection from R^n to F^n. Let $C \subseteq R^n$. Then, we denote $\overline{C} = \{\overline{c} | c \in C\}$.

We define the submodule quotient $(C : r)$ as a set $\{e \in R^{2n} | re \in C\}$ for any code $C \leq R^{2n}$ and any $r \in R$. The submodule quotient and its image under the projection have following chain conditions [9]

$$C = (C : \gamma^0) \subseteq \cdots \subseteq (C : \gamma^i) \subseteq \cdots \subseteq (C : \gamma^{\nu-1}),$$

and its projection to F,

$$\overline{C} = \overline{(C : \gamma^0)} \subseteq \cdots \subseteq \overline{(C : \gamma^i)} \subseteq \cdots \subseteq \overline{(C : \gamma^{\nu-1})}.$$

In order to know the relation between the subsystem code over a ring and that over a field, we need to first show the relation of the symplectic weights of a code over a ring and that over its residue field.

Lemma 11. *Let R be a finite chain ring, γ a generator of the Jacobson radical $J(R)$ and ν the nilpotency index. Let X be a classical additive code of R^{2n} and Y its subcode $Y = X \cap X^{\perp_s}$. Then,*

$$\mathrm{swt}(Y^{\perp_s} - X) \leq \mathrm{swt}(\overline{Y^{\perp_s} - (X : \alpha)}),$$

where $\alpha = \gamma^{\nu-1}$.

Proof: Let us consider $x \in Y^{\perp_s} - (X : \alpha)$. Then, we know $\alpha x \in Y^{\perp_s} - X$. This means that $\alpha(Y^{\perp_s} - (X : \alpha)) \subseteq Y^{\perp_s} - X$. Therefore, $\mathrm{swt}(Y^{\perp_s} - X) \leq \mathrm{swt}(\alpha(Y^{\perp_s} - (X : \alpha)))$.

We define the map $\varphi : \alpha R^{2n} \to F^{2n}$ given by $\varphi(\alpha x) = \overline{x}$. Since φ is an isomorphism and preserves the weight [8], we can say that this map also preserves the symplectic weight. Thus, we have the relation that $\mathrm{swt}(\alpha(Y^{\perp_s} - (X : \alpha))) = \mathrm{swt}(\overline{Y^{\perp_S} - (X : \alpha)})$. Then,

$$\begin{aligned}\mathrm{swt}(Y^{\perp_s} - X) \leq & \mathrm{swt}(\alpha(Y^{\perp_s} - (X : \alpha))) \\ = & \mathrm{swt}(\overline{Y^{\perp_s} - (X : \alpha)})\end{aligned}$$

Therefore, we can conclude that $\mathrm{swt}(Y^{\perp_s} - X) \leq \mathrm{swt}(\overline{Y^{\perp_s} - (X : \alpha)})$. ∎

For the simpler analysis of the relation between the subsystem code over a ring and a field, we will focus on the free code. The free code over a ring has the following properties [9].

Let C be a free code over R. Then, the dual code $C^{\perp_s}$ is also a free code. The number of rows in a generator matrix in standard form $k(C)$ is $k_0(C)$, which is the number of rows not divisible by γ^i for $1 \leq i \leq \nu - 1$. In addition, $\overline{C} = \overline{(C : \gamma)} = \cdots = \overline{(C : \gamma^{\nu-1})}$.

Theorem 12. *If an $((n, K, L, d))_R$ free subsystem code exists over a finite chain ring with the Jacobson radical $J(R)$ and the nilpotency index ν, then there exists an $((n, K^{1/\nu}, L^{1/\nu}, \geq d))_q$ subsystem code over a field $R/J(R)$ with q elements.*

Proof: By Theorem 8, there are the classical additive code $X \subseteq R^{2n}$ and its subcode $Y = X \cap X^{\perp_s}$, which are associated with an $((n, K, L, d))_R$ subsystem code. Since an $((n, K, L, d))_R$ subsystem code is a free code, X and Y are free codes. Suppose that generator matrices of X and Y have the numbers of rows k_0 and k_0', respectively. Then, $|X| = q^{\nu k_0}$ and $|Y| = q^{\nu k_0'}$ [9]. Therefore, $K = |R|^n / q^{\nu(k_0+k_0')/2} = q^{\nu(n-(k_0+k_0')/2)}$ and $L = q^{\nu(k_0-k_0')/2}$.

Now we consider $\overline{X}$ and $\overline{Y}$, which are the subset of F^{2n}. Since $dim(\overline{X}) = k_0$ and $dim(\overline{Y}) = k_0'$ [9], we have $|\overline{X}| = q^{k_0}$ and $|\overline{Y}| = q^{k_0'}$. By [4, Theorem 5], we can have an $((n, K', L', d'))_q$ subsystem code using $\overline{X}$ and $\overline{Y}$, where $K' = q^{n-(k_0+k_0')/2}$ and $L' = q^{(k_0-k_0')/2}$. Since $K' = K^{1/\nu}$ and $L' = L^{1/\nu}$, we conclude that there exsits an $((n, K^{1/\nu}, L^{1/\nu}, d'))_q$ subsystem code over a finite field with q elements.

Since a free code has a property that $\overline{X} = \overline{(X : \alpha)}$ [9], the minimum distance $d' = \mathrm{swt}(\overline{Y^{\perp_s} - X}) = \mathrm{swt}(\overline{Y^{\perp_s} - (X : \alpha)}) \geq \mathrm{swt}(Y^{\perp_s} - X) = d$, where the inequality is from Lemma 11. ∎

Changing a notation to a simpler one, the derived subsystem code over a finite field has same parameters as the free subsystem code over a finite chain ring except for their distances.

Corollary 13. *If an $[[n, k, l, d]]_R$ free subsystem code exists over a finite chain ring, then there exists an $[[n, k, l, \geq d]]_q$ subsystem code over a finite field.*

Proof: From the proof of Theorem 12, an $((n, K, L, d))_R$ free subsystem code can be called an $[[n, n-(k_0+k_0')/2, (k_0-k_0')/2, d]]_R$ free subsystem code since $|R| = q^\nu$. Using the fact that $|F| = q$, an $((n, K^{1/\nu}, L^{1/\nu}, \geq d))_q$ subsystem code can be called an $[[n, n-(k_0+k_0')/2, (k_0-k_0')/2, \geq d]]_q$ subsystem code. By letting $k = n - (k_0 + k_0')/2$ and $l = (k_0 - k_0')/2$, we can conclude that an $[[n, k, l, \geq d]]_q$ code can be derived from an $[[n, k, l, d]]_R$ code. ∎

VI. Conclusion

In this paper, we gave a construction of subsystem code over nice nearrings. Furthermore, in the case of rings, we derived a construction of subsystem codes from classical linear codes over finite Frobenius rings. For the much smaller class of free subsystem codes over finite chain rings, we were able to show that there exists a free subsystem code over a finite field that has the same rate and at least same minimum distance.

Acknowledgment

We thank Sushma Nadella for fruitful discussions. This research was supported by NSF grant CCF 1018500.

References

[1] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. Subsystem codes. In *44th Annual Allerton Conference on Communication, Control, and Computing*, volume 44(1), sep 2006.

[2] I. M. Isaacs. *Finite Group Theory*, volume 92 of *Graduate Studies in Mathematics*. American Mathematical Society, 2008.

[3] A. Klappenecker. Nice nearrings. In *2012 IEEE International Symposium on Information Theory Proceedings (ISIT)*, pages 170 –173, july 2012.

[4] A. Klappenecker and P. K. Sarvepalli. Clifford code constructions of operator quantum error-correcting codes. *IEEE Transactions on Information Theory*, 54(12):5760 –5765, dec. 2008.

[5] D. Kribs, R. Laflamme, and D. Poulin. Unified and generalized approach to quantum error correction. *Phys. Rev. Lett.*, 94(18):180501, May 2005.

[6] D. W. Kribs, R. Laflamme, D. Poulin, and M. Lesosky. Operator quantum error correction. *Quantum Info. Comput.*, 6(4):382–399, July 2006.

[7] S. Nadella and A. Klappenecker. Stabilizer codes over frobenius rings. In *2012 IEEE International Symposium on Information Theory Proceedings (ISIT)*, pages 165 –169, july 2012.

[8] G. H. Norton and A. Salagean. On the hamming distance of linear codes over a finite chain ring. *IEEE Transactions on Information Theory*, 46(3):1060 –1067, may 2000.

[9] G. H. Norton and A. Salagean. On the structure of linear and cyclic codes over a finite chain ring. *Applicable Algebra in Engineering, Communication and Computing*, 10:489–506, 2000.