Entanglement-Assisted Quantum Error-Correcting Codes over Local Frobenius Rings

Tania Sidana and Navin Kashyap

2022 IEEE International Symposium on Information Theory (ISIT) | 978-1-6654-2159-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/ISIT50566.2022.9834381

***Abstract*—In this paper, we provide a framework for constructing entanglement-assisted quantum error-correcting codes (EAQECCs) from classical additive codes over a finite commutative local Frobenius ring. We give a formula for the minimum number of entanglement qudits required to construct an EAQECC from an additive code over a finite Galois ring. This significantly extends known results for EAQECCs over finite fields.**

I. Introduction

Quantum error-correcting codes (QECCs) protect quantum states against decoherence caused by the interaction between quantum states and their environment. The stabilizer framework, proposed by Gottesman [5], is one of the main mechanisms for constructing QECCs. The construction is based on abelian subgroups of the Pauli group, and the resulting QECCs are called quantum stabilizer codes. The stabilizer framework encompasses the first QECC constructed by Shor [13], as well as the construction from classical error-correcting codes, discovered independently by Calderbank and Shor [3] and Steane [15]. The Calderbank-Shor-Steane (CSS) construction uses dual-containing (or self-orthogonal) classical codes to form QECCs. Originally developed for qubits, the stabilizer framework was subsequently extended to higher-dimensional qudit spaces. The (Pauli) error group in this case is generated by unitary operators whose actions on qudits are defined by the algebra of an underlying finite field or ring. The extension of the stabilizer framework to error groups defined via finite fields was executed by Ashikhmin and Knill [1], and Ketkar et al. [9], while the same was done for finite commutative Frobenius rings by Nadella and Klappenecker [11], and Gluesing-Luerssen and Pllaha [7].

The stabilizer formalism was extended in a different direction by Brun et al. [2], who gave a method of constructing QECCs (over qubits) from *non-abelian* subgroups of the Pauli group. The idea here was to add more dimensions to the Pauli group, so as to introduce extra degrees of freedom that can be used to "abelianize" the original non-abelian subgroup. The code construction required the existence of a small number of pre-shared entanglement qubits between the sender and receiver, where the receiver-end qubits are assumed to be error-free throughout. As a consequence, these codes were called entanglement-assisted quantum error correcting codes (EAQECCs). Within this framework, *any* classical binary linear code can be used as the starting point for constructing an EAQECC. Wilde and Brun [16] determined the minimal number of shared qubits required to construct an EAQECC starting from a given binary linear code, and more generally, starting from a given non-abelian subgroup of the Pauli group.

The theory of EAQECCs extends readily to qudit spaces for which the (Pauli) error groups are defined by finite fields. Indeed, Wilde and Brun observe in [16, Remark 1] that their formula for the minimum number of shared qudits also applies to EAQECCs constructed from linear codes over any prime field; a formal proof of this was given by Luo et al. [10]. Later, Galindo et al. [4] verified that this formula also applied to EAQECCs obtained from linear codes over an arbitrary finite field $\mathbb{F}_q$. More recently, Nadkarni and Garani [12] derived an analogous formula for EAQECCs constructed from $\mathbb{F}_p$-additive codes over $\mathbb{F}_q$, where p is the characteristic of $\mathbb{F}_q$.

In this paper, we extend the EAQECC formalism to qudit spaces on which error actions are defined by finite local commutative Frobenius rings. This enables us to construct EAQECCs starting from classical additive codes over such rings, which are overall a much richer class of (classical) codes. It must be pointed out here that Lee and Klappenecker [6] have previously studied EAQECCs over finite commutative (but not necessarily local) Frobenius rings. However, their EAQECC construction relies crucially on Theorem 5 of their paper, in the proof of which we found a gap that could not readily be filled — see Remark III.1. By restricting our attention further to local rings, we prove the necessary result (Theorem III.1) for the construction of EAQECCs. Thus, one of the contributions of this paper is to provide a coding-theoretic framework to construct EAQECCs over finite commutative local Frobenius rings from first principles.

We also attempt to obtain the minimum number of pre-shared entanglement qudits required to construct an EAQECC, starting from an additive code over such a ring. We succeed in deriving this number for the special case of EAQECCs over finite Galois rings. To get to the answer, we had to first derive it for the basic case of the integer rings $\mathbb{Z}_{p^s}$, which itself turned out to be a non-trivial task.

This paper is organized as follows. In Section II, we establish the basic definitions and notation needed to describe the construction of quantum stabilizer codes and EAQECCs. This section also contains statements of our main results. In Section III, we provide the means to construct EAQECCs from any additive code over a finite commutative local Frobenius ring. In Section IV, we derive our formula for the minimum number of pre-shared entanglement qudits required to construct an

The authors are with the Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore 560012. Email: {taniasidana,nkashyap}@iisc.ac.in. This work was supported an IISc-IoE postdoctoral fellowship awarded to the first author.

EAQECC over the ring $\mathbb{Z}_{p^a}$. Some directions of future work are suggested in Section V.

II. Preliminaries

Let R be a finite commutative ring with unity. Let $\mathrm{Hom}(R, \mathbb{C}^*)$ be the set of all additive characters of R, i.e., the set of group homomorphisms from $(R, +)$ to $\mathbb{C}^*$. A ring R is called a Frobenius ring if there exists an additive character χ such that $\mathrm{Hom}(R, \mathbb{C}^*) = R.\chi$. Any additive character with this property is called a generating character of R. Finite fields, the rings $\mathbb{Z}_N$ of integers modulo N, Galois rings and finite chain rings are a few examples of finite Frobenius rings.

Throughout this section, let $\mathcal{R}$ be a finite commutative local Frobenius ring with generating character χ. Further, as $\mathcal{R}$ is a finite commutative local ring, the characteristic, char$\mathcal{R}$, of $\mathcal{R}$ is a power of a prime number, and the cardinality, $|\mathcal{R}|$, of $\mathcal{R}$ is also a power of prime number. Let $|\mathcal{R}| = p^a = q$, and char$\mathcal{R} = p^b$, where p is a prime. Furthermore, let $\zeta \in \mathbb{C}^*$ be a primitive p^b-th root of unity. Then $\chi(r) \in \langle\zeta\rangle = \{1, \zeta, \zeta^2, \ldots, \zeta^{p^b-1}\}$ for each $r \in \mathcal{R}$.

A subset $\mathcal{C}$ of $\mathcal{R}^n$ is called an additive code over $\mathcal{R}$ of length n if $\mathcal{C}$ is an additive subgroup of $\mathcal{R}^n$. Clearly, $\mathcal{C} \subseteq \mathcal{R}^n$ is an additive code if and only if $\mathcal{C} \subseteq \mathcal{R}^n$ is a module over $\mathbb{Z}_{p^b}$. The rank of $\mathcal{C}$ is defined as the minimum number of generators of $\mathcal{C}$ as a $\mathbb{Z}_{p^b}$-module, and is denoted by rank$(\mathcal{C})$.

The symplectic weight of a vector $(x, y) = (x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n) \in \mathcal{R}^{2n}$, denoted by $\mathrm{wt}_s(x, y)$, is defined as $\mathrm{wt}_s(x, y) = |\{i \mid (x_i, y_i) \neq 0\}|$. The minimum symplectic distance $d_s(A)$ of a subset A of $\mathcal{R}^{2n}$ is defined as $d_s(A) = \min\{\mathrm{wt}_s(a) \mid a \in A \setminus \{0\}\}$. The symplectic inner product on $\mathcal{R}^{2n}$ is defined as $\langle(a, b)|(a', b')\rangle_s := ba' - b'a$ for $a, b, a', b' \in \mathcal{R}^n$. (Here ba' and $b'a$ are the dot products in $\mathcal{R}^n$.)

Definition II.1. For an additive code $\mathcal{C}$ of $\mathcal{R}^{2n}$, the symplectic dual $\mathcal{C}^{\perp_s}$ of $\mathcal{C}$ is defined by

$$\mathcal{C}^{\perp_s} = \{v \in \mathcal{R}^{2n} \mid \langle c|v\rangle_s = 0 \text{ for all } c \in \mathcal{C}\}.$$

We also define

$$\mathcal{C}^{\perp_\chi} = \{v \in \mathcal{R}^{2n} \mid \chi(\langle c|v\rangle_s) = 1 \text{ for all } c \in \mathcal{C}\}.$$

Note that $\mathcal{C}^{\perp_\chi}$ is also an additive code of $\mathcal{R}^{2n}$.

Definition II.2. Let $\mathcal{C} \subseteq \mathcal{R}^{2n}$ be an additive code over $\mathcal{R}$.

- A code $\mathcal{C}' \subseteq \mathcal{R}^{2(n+c)}$ is called a χ-self-orthogonal extension of $\mathcal{C}$ if $\mathcal{C}' \subseteq \mathcal{C}'^{\perp_\chi}$, and $\mathcal{C}$ can be obtained from $\mathcal{C}'$ by puncturing $\mathcal{C}'$ at the coordinates $n+1, n+2, \ldots, n+c, 2n+1, 2n+2, \ldots, 2n+2c$. The number c is called the entanglement degree.
- A χ-self-orthogonal extension of the code $\mathcal{C}$ with the least entanglement degree among all such extensions is called a minimal χ-self-orthogonal extension of $\mathcal{C}$. The entanglement degree of a minimal χ-self-orthogonal extension of $\mathcal{C}$ is called the minimum entanglement degree of $\mathcal{C}$.

Briefly, the reason for the nomenclature of "entanglement degree" is that this is the number of entanglement qudits needed in the construction of an EAQECC from $\mathcal{C}$.

Lemma II.1 ([11], Lemma 6)**.** *For an additive code $\mathcal{C} \subseteq \mathcal{R}^{2n}$, we have $|\mathcal{C}||\mathcal{C}^{\perp_\chi}| = |\mathcal{R}^{2n}|$.*

A. Quantum stabilizer codes over local Frobenius rings

Let $\mathcal{B} = \{|x\rangle \mid x \in \mathcal{R}\}$ be an orthonormal basis of $\mathbb{C}^q$. The state of a unit system, a qudit, is a superposition of these basis states of the system and is given by

$$|\psi\rangle = \sum_{x\in\mathcal{R}} a_x|x\rangle, \text{ where } a_x \in \mathbb{C} \text{ and } \sum_{x\in\mathcal{R}} |a_x|^2 = 1.$$

An orthonormal basis of the quantum state space of n qudits $\mathbb{C}^{q^n} = (\mathbb{C}^q)^{\otimes n}$ is given by $\mathcal{B}^{\otimes n} = \{|x\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle \mid x = (x_1, x_2, \ldots, x_n) \in \mathcal{R}^n\}$.

For $a \in \mathcal{R}$, define two linear maps $X(a)$ and $Z(b)$ on $\mathbb{C}^q$ by their action on the basis $\mathcal{B}$ as $X(a)(|x\rangle) = |x + a\rangle$ and $Z(a)(|x\rangle) = \chi(ax)|x\rangle$ for all $x \in \mathcal{R}$. Extend these maps to unitary maps on $\mathbb{C}^{q^n}$ as $X(a) = X(a_1) \otimes X(a_2) \otimes \cdots \otimes X(a_n)$ and $Z(a) = Z(a_1) \otimes Z(a_2) \otimes \cdots \otimes Z(a_n)$ for $a = (a_1, a_2, \ldots, a_n) \in \mathcal{R}^n$. Clearly, $X(a)(|x\rangle) = |x + a\rangle$ and $Z(a)(|x\rangle) = \chi(ax)|x\rangle$ for all $a, x \in \mathcal{R}^n$, where $ax = \sum_{i=1}^{n} a_i x_i$ is the dot product in $\mathcal{R}^n$. A set $\mathcal{E}_n(\mathcal{R}) := \{X(a)Z(b)|a, b \in \mathcal{R}^n\}$ is called an error basis of the n-qudit error group. To define the n-qudit error group, called as the Pauli group, let us fix some notations first. Let

$$N = \begin{cases} p^b & \text{if } p \text{ is odd;} \\ 2p^b & \text{if } p \text{ is even.} \end{cases}$$

Further, let $\omega \in \mathbb{C}^*$ be a primitive N-th root of unity.

Definition II.3. [7] The Pauli group $\mathcal{P}_n(\mathcal{R})$ is defined as

$$\mathcal{P}_n(\mathcal{R}) := \{\omega^\ell X(a)Z(b) \mid 0 \leq \ell \leq N-1, a, b \in \mathcal{R}^n\}.$$

Define a map $\Psi : \mathcal{P}_n(\mathcal{R}) \to \mathcal{R}^{2n}$ as $\Psi(\omega^\ell X(a)Z(b)) = (a, b)$. The map Ψ is a surjective group homomorphism with $\ker \Psi = \{\omega^\ell I \mid 0 \leq \ell \leq N-1\}$.

The weight of an operator $\omega^\ell X(a)Z(b) = \omega^\ell X(a_1) \otimes X(a_2) \otimes \cdots \otimes X(a_n)Z(a_1) \otimes Z(a_2) \otimes \cdots \otimes Z(a_n) \in \mathcal{P}_n(\mathcal{R})$ is defined as $\mathrm{wt}(\omega^\ell X(a)Z(b)) = |\{i \mid (a_i, b_i) \neq 0\}|$. That is, the weight of an operator is defined as the number of non-scalar components of the tensor product that forms the operator.

A quantum error correcting code is a K-dimensional subspace of $\mathbb{C}^{q^n}$. A quantum code has minimum distance D if it can detect all errors of weight less than equal to $D-1$ and cannot detect some error of weight D. A quantum code $\mathcal{Q} \subseteq \mathbb{C}^{q^n}$ of dimension K and minimum distance D is referred to as an $((n, K, D))_q$ quantum code. The subscript q may be dropped if there is no ambiguity.

Definition II.4. [7]

(a) A subgroup $\mathcal{S}$ of $\mathcal{P}_n(\mathcal{R})$ is called a stabilizer group if $\mathcal{S}$ is abelian and $\mathcal{S} \cap \ker \Psi = \{I_{q^n}\}$.

(b) A subspace $\mathcal{Q}$ of $\mathbb{C}^{q^n}$ is called a quantum stabilizer code if there exists a stabilizer group $\mathcal{S}$ such that $\mathcal{Q} = \mathcal{Q}(\mathcal{S}) := \{|x\rangle \in \mathbb{C}^{q^n} \mid V|x\rangle = |x\rangle \text{ for all } V \in \mathcal{S}\}$.

It is well known that set of undetectable errors for a quantum stabilizer code $\mathcal{Q}(\mathcal{S})$ are those which commute with all the elements of $\mathcal{S}$ but are not the elements of $\mathcal{S}$ (by ignoring the overall phase factor of the error and of the elements of $\mathcal{S}$).

B. EAQECCs over local Frobenius rings

Quantum stabilizer codes can be constructed only from abelian subgroups of $\mathcal{P}_n(\mathcal{R})$. To construct QECCs from non-abelian subgroups of $\mathcal{P}_n(\mathcal{R})$, there is a framework of entanglement-assisted quantum error correcting codes (EAQECCs), which involves the use of maximally entangled states shared between the transmitter and the receiver. Brun et al. [2] first proposed this construction from non-abelian subgroups of $\mathcal{P}_n(\mathbb{Z}_2)$. The basic idea of Brun et al. can be extended to construct EAQECCs from non-abelian subgroups of $\mathcal{P}_n(\mathcal{R})$. For this, we need a method to extend a non-abelian subgroup of $\mathcal{P}_n(\mathcal{R})$ into an appropriate higher dimensional space to form an abelian group. To this end, we first note that if $\mathcal{S}$ is a subgroup of $\mathcal{P}_n(\mathcal{R})$, then $\Psi(\mathcal{S}) \subseteq \mathcal{R}^{2n}$ is an additive code over $\mathcal{R}$. Moreover, by Lemma 3.2 of Gluesing-Luerssen and Pllaha [7], we see that an operator $P = \omega^\ell X(a)Z(b) \in \mathcal{P}_n(\mathcal{R})$ commutes with elements of the subgroup $\mathcal{S}$ if and only if $\chi(ba' - b'a) = 1$ for each $\omega^{\ell'} X(a')Z(b') \in \mathcal{S}$. From this, we observe that if $V_1 \in \mathcal{P}_n(\mathcal{R})$ commutes with all elements of $\mathcal{S}$, then $\Psi(V_1) \in \Psi(\mathcal{S})^{\perp_\chi}$.

Thus, extending $\mathcal{S}$ to make it an abelian subgroup $\mathcal{S}'$ of $\mathcal{P}_{n+c}(\mathcal{R})$ for some c is equivalent to extending $\mathcal{C} := \Psi(\mathcal{S})$ to $\mathcal{C}' := \Psi(\mathcal{S})' \subseteq \mathcal{R}^{2(n+c)}$ such that $\mathcal{C}' \subseteq \mathcal{C}'^{\perp_\chi}$, In other words, it is equivalent to constructing a χ-self-orthogonal extension $\mathcal{C}' \subseteq \mathcal{R}^{2(n+c)}$ of the additive code $\mathcal{C} \subseteq \mathcal{R}^{2n}$. In Theorem III.2, we provide a method to construct such a χ-self-orthogonal extension. Then, in Theorem III.3, we give a construction of an $((n+c, q^{n+c}/|\mathcal{C}|))$ quantum stabilizer code from $\mathcal{C}'$, which will be the desired EAQECC. As in the Brun et al. framework, the c extra qudits involved in the construction are entanglement qudits assumed to be residing error-free at the receiver end. This quantum code is referred to as an $((n, q^{n+c}/|\mathcal{C}|; c))$ EAQECC over $\mathcal{R}$.

As the receiver-end qudits are assumed to be maintained error-free, we note that if $E = \omega^\ell X(a, a')Z(b, b') \in \mathcal{P}_{n+c}(\mathcal{R})$, with $a, b \in \mathcal{R}^n$, $a', b' \in \mathcal{R}^c$, is an error operating on the transmitted codeword, then we must have $a' = b' = (0, 0, \ldots, 0) \in \mathcal{R}^c$. Thus, only errors of the form $\omega^\ell X(a, 0)Z(b, 0) \in \mathcal{P}_{n+c}(\mathcal{R})$, with $a, b \in \mathcal{R}^n$, are assumed to occur in this model. We then say that an $((n, q^{n+c}/|\mathcal{C}|; c))$ EAQECC has minimum distance D if it can detect all errors of the form $\omega^\ell X(a, 0)Z(b, 0) \in \mathcal{P}_{n+c}(\mathcal{R})$, with $a, b \in \mathcal{R}^n$, of weight at most $D - 1$, but it cannot detect some error of this form of weight D. Such a quantum code is referred to as an $((n, q^{n+c}/|\mathcal{C}|, D; c))$ EAQECC over $\mathcal{R}$.

C. A summary of our main results

In this paper, we provide a coding-theoretic framework to construct EAQECCs over $\mathcal{R}$. To do that, we provide a method to construct EAQECCs over $\mathcal{R}$ from classical additive codes over $\mathcal{R}$, and the main result is as follows:

Theorem II.1. *Let $\mathcal{C} \subseteq \mathcal{R}^{2n}$ be an additive code, i.e., $\mathcal{C}$ is a module over $\mathbb{Z}_{p^b}$. From $\mathcal{C}$, we can construct an $((n, K, D; c))$ EAQECC over $\mathcal{R}$, where the number of entanglement qudits needed is $c = \frac{1}{2}\operatorname{rank}(\mathcal{C}/(\mathcal{C} \cap \mathcal{C}^{\perp_\chi}))$, the minimum distance is*

$$D = \begin{cases} d_{\mathrm{s}}(\mathcal{C}^{\perp_\chi}) & \text{if } \mathcal{C}^{\perp_\chi} \subseteq \mathcal{C} \\ d_{\mathrm{s}}(\mathcal{C}^{\perp_\chi} \setminus \mathcal{C}) & \text{otherwise}, \end{cases}$$

and the dimension K is bounded as $q^{n+c}/(|\mathcal{C}|\, p^{\sum_{t=1}^{b-1}(b-t)\rho_t}) \leq K \leq q^{n+c}/|\mathcal{C}|$, the ρ_t's being numbers determined by a certain chain of subcodes of $\mathcal{C}$. Additionally, if $\mathcal{C}$ is free (i.e., it is a free module over $\mathbb{Z}_{p^b}$), then $K = q^{n+c}/|\mathcal{C}|$.

This result is a direct consequence of Theorems III.2 and III.3 stated in the next section, and proved in the extended version of this paper [14]. The precise expression for the numbers ρ_t can also be found in [14].

Our second main result is an explicit formula for the minimum number of pre-shared entanglement qudits required to construct an EAQECC from an additive code over a Galois ring. This theorem significantly extends the results of Galindo et al. [4] and Nadkarni and Garani [12] obtained for EAQECCs from additive codes over finite fields.

Theorem II.2. *Let $\mathcal{C} \subseteq GR(p^b, m)^{2n}$ be an additive code over the Galois ring $GR(p^b, m)$. From $\mathcal{C}$, we can construct an $((n, K, D; c))$ EAQECC over $GR(p^b, m)$, where the minimum number, c, of entanglement qudits needed for the construction is equal to $\left\lceil \frac{1}{2m}\operatorname{rank}(\mathcal{C}/(\mathcal{C} \cap \mathcal{C}^{\perp_{\mathrm{Tr}}})) \right\rceil$, the minimum distance is*

$$D = \begin{cases} d_{\mathrm{s}}(\mathcal{C}^{\perp_{\mathrm{Tr}}}) & \text{if } \mathcal{C}^{\perp_{\mathrm{Tr}}} \subseteq \mathcal{C} \\ d_{\mathrm{s}}(\mathcal{C}^{\perp_{\mathrm{Tr}}} \setminus \mathcal{C}) & \text{otherwise}, \end{cases}$$

and the dimension K is bounded as $p^{bm(n+c)}/(|\mathcal{C}|\, p^{\sum_{t=1}^{b-1}(b-t)\rho_t}) \leq K \leq p^{bm(n+c)}/|\mathcal{C}|$, the ρ_t's being numbers determined by a certain chain of subcodes of $\mathcal{C}$. Additionally, if $\mathcal{C}$ is free, then $K = p^{bm(n+c)}/|\mathcal{C}|$.

In the statement of the theorem above, $\mathcal{C}^{\perp_{\mathrm{Tr}}} = \{v \in \mathrm{GR}(p^b, m)^{2n} : \mathrm{Tr}(\langle v|c\rangle_{\mathrm{s}}) = 0 \ \forall\, c \in \mathcal{C}\}$ is the trace-symplectic dual of $\mathcal{C}$, defined with respect to the generalized trace map $\mathrm{Tr} : \mathrm{GR}(p^b, m) \to \mathbb{Z}_{p^b}$. The proof of the theorem relies on the machinery of the generalized trace map Tr, and the existence of bases of $\mathrm{GR}(p^b, m)$ as a free module over $\mathbb{Z}_{p^b}$, that are dual with respect to Tr. We refer the reader to the extended version of this paper [14] for the details of the proof, along with an exact expression for the numbers ρ_t in the statement of the theorem. For the special case of the integer ring $\mathbb{Z}_{p^a}$, we sketch a proof of the result (Theorem IV.1) in Section IV.

III. Constructing EAQECCs over Local Frobenius Rings

In this section, we sketch out the method for constructing EAQECCs from additive codes over a finite commutative local Frobenius ring $\mathcal{R}$ with generating character χ. At the heart of the construction is a mechanism to obtain a χ-self-orthogonal extension $\mathcal{C}'$ of an additive code $\mathcal{C}$. We start with some definitions.

Definition III.1. A subset $\{a_{11}, a_{12}, a_{21}, a_{22}, \ldots, a_{e1}, a_{e2}\}$ of $\mathcal{R}^{2n}$ is said to be a symplectic subset of $\mathcal{R}^{2n}$ if $\chi(\langle a_{i1} \mid a_{j1}\rangle_s) = \chi(\langle a_{i2} \mid a_{j2}\rangle_s) = \chi(\langle a_{i1} \mid a_{k2}\rangle_s) = 1$ and $\chi(\langle a_{i1} \mid a_{i2}\rangle_s) \neq 1$ for all $i, j, k \in \{1, 2, \ldots, e\}$ with $i \neq k$.

Definition III.2. Let $\mathcal{C} \subseteq \mathcal{R}^{2n}$ be an additive code, i.e., $\mathcal{C} \subseteq \mathcal{R}^{2n}$ be a module over $\mathbb{Z}_{p^b}$. Further, let $\mathcal{G}$ be a minimal generating set of $\mathcal{C} \subseteq \mathcal{R}^{2n}$ as a $\mathbb{Z}_{p^b}$-module.

- A generator $g \in \mathcal{G}$ is called an isotropic generator if $\chi(\langle g|h\rangle_s) = 1$ for all $h \in \mathcal{G}$.
- Two generators $g, g' \in \mathcal{G}$ are called a hyperbolic pair if $\chi(\langle g|g'\rangle_s) \neq 1$, $\chi(\langle g|h\rangle_s) = 1$ for all $h \in \mathcal{G} \setminus \{g'\}$, and $\chi(\langle g'|h\rangle)_s) = 1$ for all $h \in \mathcal{G} \setminus \{g\}$.

Note that a generator is isotropic iff it belongs to $\mathcal{C}^{\perp_\chi}$. Thus, an additive code $\mathcal{C} \subseteq \mathcal{R}^{2n}$ with a generating set $\mathcal{G}$ is χ-self-orthogonal iff all the generators in $\mathcal{G}$ are isotropic.

Proposition III.1. *Let $\mathcal{C} \subseteq \mathcal{R}^{2n}$ be an additive code with a generating set containing e hyperbolic pairs, u_{i1}, u_{i2}, $i = 1, 2, \ldots, e$, with the remaining generators being isotropic. Then, $\mathcal{C}$ has a χ-self-orthogonal extension $\mathcal{C}' \subseteq \mathcal{R}^{2(n+c)}$ if and only if there is a symplectic subset $\{a_{11}, a_{12}, a_{21}, a_{22}, \ldots, a_{e1}, a_{e2}\} \subset \mathcal{R}^{2c}$ of cardinality $2e$ such that $\chi(\langle u_{i1} \mid u_{i2}\rangle_s) = \chi(\langle a_{i1} \mid a_{i2}\rangle_s)$ for $i = 1, 2, \ldots, e$.*

Proof. Let $\mathcal{G} = \{u_{11}, u_{12}, \ldots, u_{e1}, v_{e2}, z_1, \ldots, z_d\}$ be a generating set of $\mathcal{C}$, with $z_1, \ldots, z_d$ being the isotropic generators. As the generators live in $\mathcal{R}^{2n}$, we can write them as

$$u_{i1} = (v_i, w_i) \text{ and } u_{i2} = (x_i, y_i) \text{ for } i = 1, 2, \ldots, e,$$

and $z_j = (v_{e+j}, w_{e+j})$ for $j = 1, 2 \ldots, d$, where each of the components u_i, v_i, x_i, y_i lies in $\mathcal{R}^n$.

Now, suppose that $\{a_{11}, a_{12}, a_{21}, a_{22}, \ldots, a_{e1}, a_{e2}\} \subset \mathcal{R}^{2c}$ is a symplectic subset such that $\chi(\langle u_{i1} \mid u_{i2}\rangle_s) = \chi(\langle a_{i1} \mid a_{i2}\rangle_s)$ for $i = 1, 2, \ldots, e$. Let $a_{i1} = (b_i, c_i)$ and $a_{i2} = (r_i, s_i)$, the components being from $\mathcal{R}^c$. We then extend the components u_i, v_i, x_i, y_i of the generators in $\mathcal{G}$ to $u_i', v_i', x_i', y_i' \in \mathcal{R}^{n+c}$ as follows: $v_i' = (v_i, -b_i)$, $w_i' = (w_i, c_i)$, $x_i' = (x_i, -r_i)$, $y_i' = (y_i, s_i)$ for $i = 1, 2, \ldots, e$, and and $v_i' = (v_i, 0)$, $w_i' = (w_i, 0)$ for $i = e{+}1, \ldots, e{+}d$, where 0 is the zero element of $\mathcal{R}^c$. Finally, set $u_{i1}' := (v_i', w_i')$ and $u_{i2}' = (x_i', y_i')$ for $i = 1, 2, \ldots, c$, and $z_j' = (v_{e+j}', w_{e+j}')$ for $j = 1, 2 \ldots, d$. Then, $\mathcal{G}' = \{u_{11}', u_{12}', \ldots, u_{e1}', v_{e2}', z_1', \ldots, z_d'\}$ generates an additive code $\mathcal{C}' \subseteq \mathcal{R}^{2(n+c)}$, and the generators in $\mathcal{G}'$ are all isotropic. For instance, $\langle u_{i1}' \mid u_{i2}'\rangle_s = v_i'y_i' - w_i'x_i' = v_iy_i - b_is_i - (w_ix_i - c_ir_i) = \langle u_{i1} \mid u_{i2}\rangle_s - \langle a_{i1} \mid a_{i2}\rangle_s$, so that

$$\chi(\langle u_{i1}' \mid u_{i2}'\rangle_s) = \chi(\langle u_{i1} \mid u_{i2}\rangle_s) \cdot \big(\chi(\langle a_{i1} \mid a_{i2}\rangle_s)\big)^{-1} = 1.$$

It follows that $\mathcal{C}'$ is a χ-self-orthogonal extension of $\mathcal{C}$.

The straightforward proof of the converse part can be found in the extended version of this paper [14]. □

From the above proof, we see that a χ-self-orthogonal extension $\mathcal{C}' \subseteq \mathcal{R}^{2(n+c)}$ of an additive code $\mathcal{C} \subseteq \mathcal{R}^{2n}$ can be constructed in two steps:

(1) Find a generating set $\mathcal{G}$ of the additive code $\mathcal{C} \subseteq \mathcal{R}^{2n}$ as a $\mathbb{Z}_{p^b}$-module, consisting of a set of hyperbolic pairs of generators and a set of isotropic generators.
(2) Find a symplectic subset of $\mathcal{R}^{2c}$, for some suitable choice of c, satisfying the property required by Proposition III.1. The desired code $\mathcal{C}'$ can be generated by the set $\mathcal{G}'$ obtained by extending the generators in $\mathcal{G}$ by $2c$ coordinates as prescribed in the proof of the proposition.

In the following theorem, we provide a method to obtain a generating set of the form required by Step (1) above.

Theorem III.1. *Let $\mathcal{C} \subseteq \mathcal{R}^{2n}$ be an additive code. There exists a generating set of $\mathcal{C}$ as a $\mathbb{Z}_{p^b}$-module, that consists only of isotropic generators and hyperbolic pairs, and the number, c, of hyperbolic pairs satisfies $2c = \operatorname{rank}(\mathcal{C}/(\mathcal{C} \cap \mathcal{C}^{\perp_\chi}))$.*

Remark III.1. We point out here that Lee and Klappenecker stated a result [6, Theorem 5] that is analogous to our theorem. However, we found a gap in the proof of [6, Theorem 5] that could not readily be filled, namely, that replacing $\mathbf{w}_k$ with $\mathbf{w}_{k-2}' = e_{k,i}\mathbf{w}_k - \cdots$ may not result in a basis of R^{2n}, as $e_{k,i}$ may not be a unit in the ring R.

Proof of Theorem III.1. Let $\pi : \mathcal{C} \to \mathcal{C}/(\mathcal{C} \cap \mathcal{C}^{\perp_\chi})$ be the canonical projection map that takes $(v, w) \in \mathcal{C}$ to the coset $(v, w) + (\mathcal{C} \cap \mathcal{C}^{\perp_\chi})$. Let $\mathcal{T} = \{(a_1, b_1), (a_2, b_2), \ldots, (a_f, b_f)\} \subseteq \mathcal{C}$ be such that $\pi(\mathcal{T}) := \{\pi((a_1, b_1)), \pi((a_2, b_2)), \ldots, \pi((a_f, b_f))\}$ is a minimal generating set of $\mathcal{C}/(\mathcal{C} \cap \mathcal{C}^{\perp_\chi})$ as a $\mathbb{Z}_{p^b}$-module. Thus, $|\mathcal{T}| = |\pi(\mathcal{T})| = \operatorname{rank}(\mathcal{C}/(\mathcal{C} \cap \mathcal{C}^{\perp_\chi}))$. Further, let $\mathcal{S}$ be a minimal generating set of the additive code $\mathcal{C} \cap \mathcal{C}^{\perp_\chi} \subseteq \mathcal{R}^{2n}$ as a $\mathbb{Z}_{p^b}$-module. It is easy to verify that $\mathcal{S} \cup \mathcal{T}$ generates $\mathcal{C}$.

Since the generators in $\mathcal{S}$ belong to $\mathcal{C}^{\perp_\chi}$, they are all isotropic. We will not tamper with $\mathcal{S}$; instead, we will bring $\mathcal{T}$ into hyperbolic-pair form. For $1 \leq i, j \leq f$, $\chi(b_ia_j - b_ja_i)$ is a p^b-th root of unity, so let $\chi(b_ia_j - b_ja_i) = \zeta^{\ell_{i,j}}$, where $\zeta = \exp(\frac{2\pi i}{p^b})$ and $0 \leq \ell_{i,j} < p^b$. Further, for $1 \leq i, j \leq f$, we note that $\chi(b_ja_i - b_ia_j) = \chi(b_ia_j - b_ja_i)^{-1}$, which gives $\ell_{i,j} \equiv -\ell_{j,i} \pmod{p^b}$. For each $i \in \{1, 2, \ldots, f\}$, we must have $\ell_{i,j} \neq 0$ for some $j \in \{1, \ldots, f\}$; otherwise, (a_i, b_i) is in $\mathcal{C} \cap \mathcal{C}^{\perp_\chi}$, so that $\pi((a_i, b_i)) = \mathcal{C} \cap \mathcal{C}^{\perp_\chi}$, contradicting the minimality of $\pi(\mathcal{T})$.

Let $\ell_{t,u}$ with $t, u \in \{1, 2, \ldots, f\}$ be such that

$$\gcd(\ell_{t,u}, p^b) = \min\{\gcd(\ell_{i,j}, p^b) : \ell_{i,j} \neq 0 \text{ and } 1 \leq i, j \leq f\}.$$

Clearly, $\gcd(\ell_{t,u}, p^b)$ divides $\gcd(\ell_{i,j}, p^b)$ for $1 \leq i, j \leq f$. As $\ell_{t,u} \neq 0$, we have $\chi(b_ta_u - b_ua_t) \neq 1$. Swap (a_1, b_1) and (a_2, b_2) with (a_t, b_t) and (a_u, b_u), respectively. For $3 \leq i \leq f$, replace (a_i, b_i) with $(a_i', b_i') = (a_i, b_i) + u_i\,(a_1, b_1) + v_i\,(a_2, b_2)$, where u_i and v_i are solutions of the linear equations

$$\ell_{1,2}u_i \equiv \ell_{2,i} (\text{mod } p^b) \quad \text{and} \quad \ell_{1,2}v_i \equiv -\ell_{1,i} (\text{mod } p^b).$$

Such u_i and v_i always exist, since $\gcd(\ell_{1,2}, p^b)$ divides $\ell_{2,i}$ and $\ell_{1,i}$. By doing this, we get a new set $\mathcal{T}_1 = \{(a_1, b_1), (a_2, b_2), (a_3', b_3'), \ldots, (a_f', b_f')\}$ such that $\chi(b_2a_1 - b_1a_2) \neq 1$, $\chi(b_j'a_1 - b_1a_j') = 1$, and

$\chi(b_j'a_2 - b_2a_j') = 1$ for $j \in \{3,4,\ldots,f\}$. In other words, (a_1,b_1) and (a_2,b_2) form a hyperbolic pair. Since $\mathcal{T}$ is recoverable from $\mathcal{T}_1$, we see that $\mathcal{S} \cup \mathcal{T}_1$ also generates $\mathcal{C}$. Moreover, $\pi(\mathcal{T})$ is recoverable from $\pi(\mathcal{T}_1) := \{\pi((a_1,b_1)), \pi((a_2,b_2)), \pi((a_3',b_3')), \ldots, \pi((a_f',b_f'))\}$, so $\pi(\mathcal{T}_1)$ is also a minimal generating set of $\mathcal{C}/(\mathcal{C}\cap\mathcal{C}^{\perp_\chi})$. In particular, $|\mathcal{T}_1| = |\pi(\mathcal{T}_1)| = \operatorname{rank}(\mathcal{C}/(\mathcal{C}\cap\mathcal{C}^{\perp_\chi}))$.

Repeatedly applying the above process to the generators $(a_3',b_3'),\ldots,(a_f',b_f')$, we will eventually obtain a set $\mathcal{T}' = \{(v_1,w_1),\ldots,(v_c,w_c),(x_1,y_1),\ldots,(x_c,y_c)\}$ such that (v_i,w_i) and (x_i,y_i), $i = 1,2,\ldots,c$, are hyperbolic pairs, $\mathcal{S}\cup\mathcal{T}'$ generates $\mathcal{C}$, and $\pi(\mathcal{T}')$ is a minimal generating set of $\mathcal{C}/(\mathcal{C}\cap\mathcal{C}^{\perp_\chi})$. In particular, $2c = |\mathcal{T}'| = |\pi(\mathcal{T}')| = \operatorname{rank}(\mathcal{C}/(\mathcal{C}\cap\mathcal{C}^{\perp_\chi}))$. □

For the second step in the construction of a χ-self-orthogonal extension of an additive code $\mathcal{C}$, we need a suitable symplectic subset. Such a subset can always be obtained from the generating set of $\mathcal{C}$ guaranteed by Theorem III.1, a fact that is shown the proof of the theorem below.

Theorem III.2. *Let $\mathcal{C} \subseteq \mathcal{R}^{2n}$ be an additive code, i.e., a module over $\mathbb{Z}_{p^b}$. Then there exists a χ-self-orthogonal extension $\mathcal{C}' \subseteq \mathcal{R}^{2(n+c)}$ of $\mathcal{C}$ with entanglement degree c equal to $\frac{1}{2}\operatorname{rank}(\mathcal{C}/(\mathcal{C}\cap\mathcal{C}^{\perp_\chi}))$, whose size can be bounded as $|\mathcal{C}| \le |\mathcal{C}'| \le |\mathcal{C}|\cdot p^{\sum_{t=1}^{b-1}(b-t)\rho_t}$, the ρ_t's being numbers determined by a certain chain of subcodes of $\mathcal{C}$. Moreover, if $\mathcal{C}$ is a free module over $\mathbb{Z}_{p^b}$, then $|\mathcal{C}'| = |\mathcal{C}|$.*

Proof. See the extended version of this paper [14]. □

Finally, the proof of the next theorem provides the formal construction of an EAQECC from the χ-self-orthogonal extension of $\mathcal{C}$ guaranteed by Theorem III.2.

Theorem III.3. *Let $\mathcal{C} \subseteq \mathcal{R}^{2n}$ be an additive code over $\mathcal{R}$, and let $\mathcal{C}' \subseteq \mathcal{R}^{2(n+c)}$ be the χ-self-orthogonal extension of $\mathcal{C}$ with entanglement degree c, as constructed in Theorem III.2. Then, there exists an $((n, q^{n+c}/|\mathcal{C}'|, D; c))$ EAQECC, where*

$$D = \begin{cases} d_{\mathrm{s}}(\mathcal{C}^{\perp_\chi}) & \text{if } \mathcal{C}^{\perp_\chi} \subseteq \mathcal{C}\,; \\ d_{\mathrm{s}}(\mathcal{C}^{\perp_\chi}\setminus\mathcal{C}) & \text{otherwise}\,. \end{cases}$$

Proof. See the extended version of this paper [14]. □

Observe that Theorem II.1 follows immediately from Theorems III.2 and III.3.

IV. EAQECCs over the Ring $\mathbb{Z}_{p^a}$

The aim of this section is to sketch a proof of the following special case of Theorem II.2.

Theorem IV.1. *Let $\mathcal{C} \subseteq \mathbb{Z}_{p^a}^{2n}$ be a submodule. From $\mathcal{C}$, we can construct an $((n,K,D;c))$ EAQECC over $\mathbb{Z}_{p^a}$, where the minimum number, c, of entanglement qudits needed for the construction is equal to $\frac{1}{2}\operatorname{rank}(\mathcal{C}/(\mathcal{C}\cap\mathcal{C}^{\perp_{\mathrm{s}}}))$, the minimum distance is*

$$D = \begin{cases} d_{\mathrm{s}}(\mathcal{C}^{\perp_{\mathrm{s}}}) & \text{if } \mathcal{C}^{\perp_{\mathrm{s}}} \subseteq \mathcal{C} \\ d_{\mathrm{s}}(\mathcal{C}^{\perp_{\mathrm{s}}}\setminus\mathcal{C}) & \text{otherwise}\,, \end{cases}$$

and the dimension K is bounded as $p^{a(n+c)}/(|\mathcal{C}|\,p^{\sum_{t=1}^{b-1}(b-t)\rho_t}) \le K \le p^{a(n+c)}/|\mathcal{C}|$, the ρ_t's being numbers determined by a certain chain of subcodes of $\mathcal{C}$. Additionally, if $\mathcal{C}$ is free, then $K = p^{a(n+c)}/|\mathcal{C}|$.

To prove the result, we need an upper bound on the cardinality of a symplectic subset of $\mathbb{Z}_{p^a}^{2n}$. In fact, we give an upper bound for the more general notion of a quasi-symplectic subset of $\mathbb{Z}_{p^a}^{2n}$, defined below. Note that $\chi(z) = e^{\frac{2\pi i}{p^a}z}$ is a generating character of the ring $\mathbb{Z}_{p^a}$, and in particular, $\chi(z) = 1$ iff $z = 0$. Thus, a symplectic subset (Definition III.1) of $\mathbb{Z}_{p^a}$ is a special case of a quasi-symplectic subset, obtained by setting $\mathcal{J} = \emptyset$ in the following definition.

Definition IV.1. A subset $\{a_{11},a_{12},a_{21},a_{22},\ldots,a_{e1},a_{e2}\}$ of $\mathbb{Z}_{p^a}^{2n}$ is said to be a quasi-symplectic subset if

(a) $\langle a_{i1},a_{j1}\rangle_s = \langle a_{i1},a_{k2}\rangle_s = 0$ for all $i,j,k \in \{1,2,\ldots,e\}$ with $i \ne k$.
(b) there exists a subset $\mathcal{J}$ of $\{1,2,\ldots,e\}$ such that $\langle a_{i1},a_{i2}\rangle_s \ne 0$ for all $i \notin \mathcal{J}$, and $\{a_{j1} \bmod p\}_{j\in\mathcal{J}}$ is a linearly independent set over $\mathbb{Z}_p$.

In the following theorem, we provide an upper bound on the size of a quasi-symplectic subset of $\mathbb{Z}_{p^a}^{2n}$.

Theorem IV.2. *If $\{a_{11},a_{12},a_{21},a_{22},\ldots,a_{e1},a_{e2}\}$ is a quasi-symplectic subset of $\mathbb{Z}_{p^a}^{2n}$ (and in particular, if it is a symplectic subset), then $e \le n$.*

Proof. The proof is by induction on a — see [14]. □

From this, we obtain an explicit formula for the minimum entanglement degree of a submodule $\mathcal{C} \subseteq \mathbb{Z}_{p^a}^{2n}$.

Theorem IV.3. *Any minimal χ-self-orthogonal extension of a submodule $\mathcal{C} \subseteq \mathbb{Z}_{p^a}^{2n}$ has entanglement degree equal to $\frac{1}{2}[\mathit{rank}(\mathcal{C}/(\mathcal{C}\cap\mathcal{C}^{\perp_s}))]$.*

Proof. For the generating character χ defined by $\chi(z) = e^{2\pi i z/p^a}$, we have $\chi(z) = 1$ iff $z = 0$. Hence, $\mathcal{C}^{\perp_\chi} = \mathcal{C}^{\perp_s}$.

Let $c_{\min}$ be the entanglement degree of a minimal χ-self-orthogonal extension, $\mathcal{C}'$, of $\mathcal{C}$. By Theorem II.1, we have $c_{\min} \le \frac{1}{2}[\operatorname{rank}(\mathcal{C}/(\mathcal{C}\cap\mathcal{C}^{\perp_s}))]$. On the other hand, from Theorem III.1, $\mathcal{C}$ has a generating set with $c = \frac{1}{2}[\operatorname{rank}(\mathcal{C}/(\mathcal{C}\cap\mathcal{C}^{\perp_s}))]$ hyperbolic pairs. Then, by Proposition III.1, there is a symplectic subset of $\mathbb{Z}_{p^a}^{2c_{\min}}$ of cardinality $2c$. Hence, by Theorem IV.2, we have $c \le c_{\min}$, as desired. □

Observe that Theorem IV.1 follows immediately from Theorems III.3 and IV.3.

V. Future Work

An interesting direction of future work would be to extend our formula for the minimum number of pre-shared entanglement qudits to EAQECCs over general finite commutative local Frobenius rings (beyond Galois rings). It would also be useful to find constructions of EAQECCs over Frobenius rings with good parameters, for example, codes that saturate the generalized quantum Singleton bound applicable to EAQECCs [8]. Finally, it would be of considerable interest to extend the EAQECC framework to non-local Frobenius rings.

REFERENCES

[1] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes", *IEEE Trans. Inf. Theory*, 47 (2001), pp. 3065–3072.

[2] T. Brun, I. Devetak and M. Hsieh, "Correcting quantum errors with entanglement", *Science*, 314 (2006), pp. 436–439.

[3] A. R. Calderbank and P. Shor, "Good quantum error-correcting codes exist", *Phys. Rev. A*, 54 (1996), pp. 1098–1105.

[4] C. Galindo, F. Hernando, R. Matsumoto and D. Ruano, "Entanglement-assisted quantum error-correcting codes over arbitrary finite fields", *Quantum Inf. Process.*, 18 (2019), 116.

[5] D. Gottesman, *Stabilizer Codes and Quantum Error Correction*, Ph.D. dissertation, CalTech, 1997.

[6] S. Lee and A. Klappenecker, "Entanglement-assisted quantum error correcting codes over nice rings", in *Proc. 52nd Annual Allerton Conference on Communication, Control, and Computing*, 2014, pp. 1362–1367.

[7] H. Gluesing-Luerssen and T. Pllaha, "On quantum stabilizer codes derived from local Frobenius rings", *Finite Fields Appl.*, 58 (2019) pp. 145–173.

[8] M. Grassl, F. Huber, and A. Winter, "Entropic proofs of Singleton bounds for quantum error-correcting codes," arXiv:2010.07902.

[9] A. Ketkar, A. Klappenecker, S. Kumar, and P. Sarvepalli, "Nonbinary stabilizer codes over finite fields", *IEEE Trans. Inf. Theory*, 52 (2006), pp. 4892-4914.

[10] L. Luo, Z. Ma, Z. Wei, and R. Leng, "Non-binary entanglement-assisted quantum stabilizer codes", *Sci. China Inf. Sci.*, 60 (2017), 42501.

[11] S. Nadella and A. Klappenecker, "Stabilizer codes over Frobenius rings", in *Proc. 2012 IEEE International Symposium on Information Theory (ISIT 2012)*, pp. 165–169.

[12] P. J. Nadkarni, S. S. Garani, "Non-binary entanglement-assisted stabilizer codes", *Quantum Inf. Process.*, 20 (2021), 256.

[13] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory", *Phys. Rev. A*, 52 (1995), pp. 2493–2496.

[14] T. Sidana and N. Kashyap, "Entanglement-assisted quantum error-correcting codes over local Frobenius rings," arXiv:2202.00248.

[15] A. Steane, "Error-correcting codes in quantum theory", *Phys. Rev. Lett.*, 77 (1996), pp. 793–797.

[16] M. M. Wilde and T. A. Brun, "Optimal entanglement formulas for entanglement-assisted quantum coding", *Phys. Rev. A*, 77 (2008), 064302.