

# Concatenated quantum codes can attain the quantum Gilbert-Varshamov bound

Yingkai Ouyang

*Department of Combinatorics and Optimization,*

*Institute of Quantum Computing,*

*University of Waterloo,*

*200 University Avenue West,*

*Waterloo, Ontario N2L 3G1, Canada.*

*y3ouyang@math.uwaterloo.ca*

## Abstract

A family of quantum codes of increasing block length with positive rate is asymptotically good if the ratio of its distance to its block length approaches a positive constant. The asymptotic quantum Gilbert-Varshamov (GV) bound states that there exist  $q$ -ary quantum codes of sufficiently long block length  $N$  having fixed rate  $R$  with distance at least  $NH_{q^2}^{-1}((1-R)/2)$ , where  $H_{q^2}$  is the  $q^2$ -ary entropy function. For  $q < 7$ , only random quantum codes are known to asymptotically attain the quantum GV bound. However, random codes have little structure. In this paper, we generalize the classical result of Thommesen [1] to the quantum case, thereby demonstrating the existence of concatenated quantum codes that can asymptotically attain the quantum GV bound. The outer codes are quantum generalized Reed-Solomon codes, and the inner codes are random independently chosen stabilizer codes, where the rates of the inner and outer codes lie in a specified feasible region.

## I. INTRODUCTION

A family of  $q$ -ary quantum codes [2] of increasing block length with positive rate is defined to be *asymptotically good* if the ratio of its distance to its block length approaches a positive constant. Designing good quantum codes is highly nontrivial, just as it is in the classical case. The quantum Gilbert-Varshamov (GV) bound [3–8] is a lower bound on an achievable relative distance of a quantum code of a fixed rate, and is attainable for various families of random quantum codes [3, 5, 7]. Explicit families of quantum codes, both unconcatenated [9, 10] and concatenated [11–14], have been studied, but do not attain the quantum GV bound for  $q < 7$  [15]. We show that concatenated quantum codes can attain the quantum GV bound.

We are motivated by the historical development of the idea of concatenating a sequence of increasingly long classical Reed-Solomon (RS) outer codes with various types of classical inner codes. In both cases where the inner codes are all identical [16] or all distinct [17], the resultant sequence of concatenated codes while asymptotically good nonetheless fail to attain the GV bound. A special case of Thommesen’s result [1] shows that even if the inner codes all have a rate of one, if they are chosen uniformly at random, the resultant sequence of concatenated codes almost surely attains the GV bound. Our work extends this classical observation to the quantum case.

We show the quantum analog of Thommesen’s result – the sequence of concatenated quantum codes with the outer code being a quantum generalized RS code [14, 18–20] and random inner stabilizer codes almost surely attains the quantum GV bound when the rates of the inner and outer codes lie in feasible region (III.1) with an example depicted in Figure 2. The property of the outer code that we need is that the normalizer of its stabilizer is classical maximal distance separable (MDS) code [20]. Our work is closest in spirit to that of Fujita [12], where quantum equivalents of the Zyablov and the Blokh-Zyablov bounds are obtained (not attaining the quantum GV bound) by choosing a quantum RS code with essentially random inner codes.

In the proof of the classical result, Thommesen uses a random coding argument to compute the probability that any codeword of weight less than the target minimum distance belongs to the random code. Subsequently, he uses the union bound, the spectral property

of the Reed-Solomon outer code, and properties of the  $q$ -ary entropy function (defined in II.1), to prove that the proposed random code almost surely does not contain any codeword of weight less than the prescribed minimum distance.

The proof of our quantum result follows a similar strategy, with codewords replaced by elements of the normalizer not in the stabilizer. However the feasible region for the rates of the inner and outer codes for the classical and the quantum result are not analogous, because the monotonicity of the  $q$ -ary entropy function applies in a different feasible region from that of the classical case.

The organization of this paper is as follows: Section II introduces the notation and preliminary material used in this paper. This section lays out the formalism of concatenating stabilizer codes, which is crucial to the proof of the main result. We state our main result in Theorem III.1 of Section III, and the remainder of the paper is dedicated to its proof.

## II. PRELIMINARIES

Let  $L(\mathbb{C}^q)$  denote the set of complex  $q$  by  $q$  matrices. Define  $\mathbb{1}_q$  to be a size  $q$  identity matrix and  $\omega_q := e^{2\pi i/q}$  to be a primitive  $q$ -th root of unity, where  $q \geq 2$  is an prime power. Define  $0 \log_q 0 := 0$ . Define the  $q$ -ary entropy function and its inverse to be  $H_q : [0, 1] \rightarrow [0, 1]$  and  $H_q^{-1} : [0, 1] \rightarrow [0, \frac{q-1}{q}]$  respectively where

$$H_q(x) := x \log_q(q-1) - x \log_q x - (1-x) \log_q(1-x). \quad (\text{II.1})$$

The  $q$ -ary entropy function is important here because it helps us to count the size of sets with  $q$  symbols. The base- $q$  logarithm of the number of vectors from  $\mathbb{F}_q^n$  that differ in at most  $xn$  components from the zero-vector is dominated by  $nH_q(x)$  as  $n$  becomes large.

For a ground set  $\Omega$  and  $n$ -tuples  $\mathbf{x} \in \Omega^n$ , define  $x_j$  to be  $j$ -th element of the  $n$ -tuple  $\mathbf{x}$ . Given tuples  $\mathbf{x} \in \Omega^n$  and  $\mathbf{y} \in \Omega^m$ , define the pasting of the tuples  $\mathbf{x}$  and  $\mathbf{y}$  to be  $(\mathbf{x}|\mathbf{y}) := (x_1, \dots, x_n, y_1, \dots, y_m)$ . When  $M_1$  and  $M_2$  are matrices with the same number of columns, define  $(M_1; M_2) := \begin{pmatrix} M_1 \\ M_2 \end{pmatrix}$ . For positive integer  $\ell$ , define  $[\ell] := \{1, \dots, \ell\}$ . Define the Hamming distance  $d_H(\mathbf{x}, \mathbf{y})$  between  $\mathbf{x} \in \Omega^n$  and  $\mathbf{y} \in \Omega^n$  as the number of indices on which  $\mathbf{x}$  and  $\mathbf{y}$  differ. Define the minimum distance of any subset  $C \subset \Omega^n$  to be  $\text{mindist}(C) := \min_{\mathbf{x}, \mathbf{y} \in C} \{d_H(\mathbf{x}, \mathbf{y}) : \mathbf{x} \neq \mathbf{y}\}$ .

A code over a vector field  $\mathbb{F}_q^n$  is  $q$ -ary linear code of length  $n$  if it is a subspace of  $\mathbb{F}_q^n$ . An additive code is a subgroup of the field under the field addition operation. A classical  $q$ -ary linear code [16] of block length  $n$  and  $k$  generators with minimum distance of  $d$  is said to be an  $[n, k]_q$  code or an  $[n, k, d]_q$  code. A classical  $[n, k, d]_q$  code is maximally distance separated (MDS) if  $d = n - k + 1$ . A quantum  $q$ -ary stabilizer code [2] of block length  $n$  encoding  $k$  qudits is said to be an  $[[n, k]]_q$  code. The rates of an  $[[n, k]]_q$  code and an  $[n, k]_q$  code are both defined to be  $\frac{k}{n}$ .

### A. Finite Fields and $q$ -ary Error Bases

We briefly review  $q$ -ary error bases [5]. Given a prime number  $p$ , let  $q = p^k$  where  $k$  is a positive integer. Let generalizations of the qubit Pauli matrices be

$$\begin{aligned} X &:= \sum_{j=0}^{p-1} |(j+1) \bmod p\rangle\langle j| \\ Z &:= \sum_{j=0}^{p-1} (\omega_p)^j |j\rangle\langle j| \end{aligned} \quad (\text{II.2})$$

which satisfy the commutation property  $X^a Z^b = (\omega_p)^{ab} Z^b X^a$  for non-negative integers  $a$  and  $b$ . We define the matrix

$$X_{\mathbf{a}} Z_{\mathbf{b}} := X^{a_1} Z^{b_1} \otimes \dots \otimes X^{a_k} Z^{b_k} \quad (\text{II.3})$$

as a single qudit  $q$ -ary error basis element. We define a  $q$ -ary error basis on a single qudit as the set  $\mathcal{E}_q := \{X_{\mathbf{a}} Z_{\mathbf{b}} : \mathbf{a}, \mathbf{b} \in \mathbb{Z}_p^k\}$ . A  $q$ -ary error basis on  $n$  qudits is defined as  $\mathcal{E}_q^{\otimes n}$  and its basis elements have the form

$$X_{\mathbf{a}^{(1)}} Z_{\mathbf{b}^{(1)}} \otimes \dots \otimes X_{\mathbf{a}^{(n)}} Z_{\mathbf{b}^{(n)}} = X_{(\mathbf{a}^{(1)}|\dots|\mathbf{a}^{(n)})} Z_{(\mathbf{b}^{(1)}|\dots|\mathbf{b}^{(n)})}.$$

Now let  $t$  be any positive integer. Observe that for  $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d} \in \mathbb{Z}_p^t$ , the matrices  $X_{\mathbf{a}} Z_{\mathbf{b}}$  and  $X_{\mathbf{c}} Z_{\mathbf{d}}$  satisfy the commutation relation

$$(X_{\mathbf{a}} Z_{\mathbf{b}})(X_{\mathbf{c}} Z_{\mathbf{d}}) = (X_{\mathbf{c}} Z_{\mathbf{d}})(X_{\mathbf{a}} Z_{\mathbf{b}})(\omega_p)^{\sum_{i=1}^t a_i d_i - b_i c_i}.$$

Hence the symplectic scalar product

$$\langle (\mathbf{a}|\mathbf{b}), (\mathbf{c}|\mathbf{d}) \rangle_s := \sum_{i=1}^t a_i d_i - b_i c_i = \mathbf{a} \mathbf{d}^T - \mathbf{b} \mathbf{c}^T$$

quantifies the commutation relation between the matrices  $X_{\mathbf{a}}Z_{\mathbf{b}}$  and  $X_{\mathbf{c}}Z_{\mathbf{d}}$ . When this scalar product is zero, we say that the vectors  $(\mathbf{a}|\mathbf{b})$  and  $(\mathbf{c}|\mathbf{d})$  are  $s$ -orthogonal, and the matrices  $X_{\mathbf{a}}Z_{\mathbf{b}}$  and  $X_{\mathbf{c}}Z_{\mathbf{d}}$  commute under matrix multiplication.

We now elucidate the connection between  $q$ -ary error bases and finite fields. Define the trace function from the field  $\mathbb{F}_q$  to  $\mathbb{F}_p$  to be  $\text{Tr} : x \mapsto \sum_{i=0}^{k-1} x^{p^i}$ . Also let  $\{\gamma, \gamma^q\}$  be a basis of  $\mathbb{F}_{q^2}$  over  $\mathbb{F}_q$ , where  $\gamma$  and  $\gamma^q$  are the distinct roots of an irreducible degree-2 polynomial over  $\mathbb{F}_q$ . Now let  $\mathfrak{a} := (\alpha_1, \dots, \alpha_k)$  and  $\mathfrak{b} := (\beta_1, \dots, \beta_k)$  be dual bases of  $\mathbb{F}_q$  so that  $\mathfrak{a}^T \mathfrak{b}$  is a size  $k$  identity matrix. Also let  $\mathbf{a}, \mathbf{b}, \mathbf{c}$ , and  $\mathbf{d}$  be vectors from  $\mathbb{Z}_p^k$ . Then  $\text{Tr}((\mathfrak{a}\mathfrak{a}^T)(\mathfrak{b}\mathfrak{b}^T)) = \text{Tr}(\mathfrak{a}\mathfrak{a}^T \mathfrak{b}\mathfrak{b}^T) = \mathbf{a}\mathbf{b}^T$ , which implies that

$$\text{Tr}((\mathfrak{a}\mathfrak{a}^T)(\mathfrak{d}\mathfrak{d}^T) - (\mathfrak{b}\mathfrak{b}^T)(\mathfrak{c}\mathfrak{c}^T)) = \mathbf{a}\mathbf{d}^T - \mathbf{b}\mathbf{c}^T. \quad (\text{II.4})$$

Given the vectors  $\mathbf{x}$  and  $\mathbf{y}$  in  $\mathbb{F}_{q^2}^n$ , the Hermitian scalar product (see (28) of [5]) between  $\mathbf{x}$  and  $\mathbf{y}$  is

$$\langle \mathbf{x}, \mathbf{y} \rangle_h := \sum_{i=1}^n (x_i)^q y_i.$$

When this Hermitian scalar product is zero, we say that  $\mathbf{x}$  and  $\mathbf{y}$  are  $h$ -orthogonal. This scalar product is called Hermitian because taking an element of  $\mathbb{F}_{q^2}$  to the  $q$ -th power is analogous to conjugation over the complex field. For any subset  $C \subset \mathbb{F}_{q^2}^n$ , we also define its Hermitian dual to be  $C^{\perp_h} := \{\mathbf{y} \in \mathbb{F}_{q^2}^n : \langle \mathbf{x}, \mathbf{y} \rangle_h = 0, \mathbf{x} \in C\}$ .

The following proposition shows that if two error basis elements are to commute, it suffices for their  $q^2$ -ary finite field counterparts to be  $h$ -orthogonal.

**Proposition II.1** ([5]). *Let  $\mathbf{x}, \mathbf{y} \in \mathbb{F}_{q^2}^n$ , and suppose that  $\langle \mathbf{x}, \mathbf{y} \rangle_h = 0$ . For all  $i \in [n]$ , let  $x_i$  and  $y_i$  have the decompositions*

$$\begin{aligned} x_i &= x_{i,1}\gamma + x_{i,2}\gamma^q = \mathbf{a}^{(i)}\mathfrak{a}^T\gamma + \mathbf{b}^{(i)}\mathfrak{b}^T\gamma^q, \\ y_i &= y_{i,1}\gamma + y_{i,2}\gamma^q = \mathbf{c}^{(i)}\mathfrak{a}^T\gamma + \mathbf{d}^{(i)}\mathfrak{b}^T\gamma^q, \end{aligned}$$

where  $x_{i,1}, x_{i,2}, y_{i,1}, y_{i,2} \in \mathbb{F}_q$  and  $\mathbf{a}^{(i)}, \mathbf{b}^{(i)}, \mathbf{c}^{(i)}, \mathbf{d}^{(i)} \in \mathbb{Z}_p^k$ . Then the matrices  $X_{(\mathbf{a}^{(1)}|\dots|\mathbf{a}^{(n)})}Z_{(\mathbf{b}^{(1)}|\dots|\mathbf{b}^{(n)})}$  and  $X_{(\mathbf{c}^{(1)}|\dots|\mathbf{c}^{(n)})}Z_{(\mathbf{d}^{(1)}|\dots|\mathbf{d}^{(n)})}$  from the set  $\mathcal{E}_q^{\otimes n}$  commute under matrix multiplication.

*Proof.* Since  $\langle \mathbf{x}, \mathbf{y} \rangle_h = (\langle \mathbf{y}, \mathbf{x} \rangle_h)^q$  and  $0^q = 0$ , we have  $\langle \mathbf{x}, \mathbf{y} \rangle_h = 0$  implying that  $\langle \mathbf{y}, \mathbf{x} \rangle_h = 0$ .

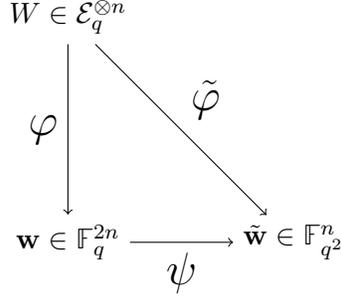


FIG. 1: Equivalent representations of an  $n$ -qudit  $q$ -ary error basis element.

Thus  $\langle \mathbf{x}, \mathbf{y} \rangle_h - \langle \mathbf{y}, \mathbf{x} \rangle_h = 0$ , which implies that  $\sum_{i=1}^n x_i^q y_i - y_i^q x_i = 0$ . Hence

$$\begin{aligned}
0 &= \sum_{i=1}^n ((x_{i,1}\gamma^q + x_{i,2}\gamma)(y_{i,1}\gamma + y_{i,2}\gamma^q) - (y_{i,1}\gamma^q + y_{i,2}\gamma)(x_{i,1}\gamma + x_{i,2}\gamma^q)) \\
&= (\gamma - \gamma^2) \sum_{i=1}^n (x_{i,1}y_{i,2} - x_{i,2}y_{i,1}). \tag{II.5}
\end{aligned}$$

If  $\gamma = \gamma^2$ , then  $\gamma = \gamma^q$  which is a contradiction. Hence  $\gamma \neq \gamma^2$  which implies that

$$\sum_{i=1}^n (x_{i,1}y_{i,2} - x_{i,2}y_{i,1}) = 0.$$

Let  $\mathbf{a} = (\mathbf{a}^{(1)} | \dots | \mathbf{a}^{(n)})$ ,  $\mathbf{b} = (\mathbf{b}^{(1)} | \dots | \mathbf{b}^{(n)})$ ,  $\mathbf{c} = (\mathbf{c}^{(1)} | \dots | \mathbf{c}^{(n)})$ , and  $\mathbf{d} = (\mathbf{d}^{(1)} | \dots | \mathbf{d}^{(n)})$ . Tracing both sides of the above equation gives  $\langle (\mathbf{a} | \mathbf{b}), (\mathbf{c} | \mathbf{d}) \rangle_s = 0$ , which implies that the matrices  $X_{\mathbf{a}} Z_{\mathbf{b}}$  and  $X_{\mathbf{c}} Z_{\mathbf{d}}$  commute.

In view of Proposition II.1 and (II.4), each element of a  $q$ -ary error basis over  $n$  qubits  $W = X_{(\mathbf{a}^{(1)} | \dots | \mathbf{a}^{(n)})} Z_{(\mathbf{b}^{(1)} | \dots | \mathbf{b}^{(n)})}$  can be represented by the codewords  $\varphi(W) := \mathbf{w} \in \mathbb{F}_q^{2n}$  and  $\tilde{\varphi}(W) := \tilde{\mathbf{w}} \in \mathbb{F}_{q^2}^n$ , where for  $i \in [n]$ ,

$$\begin{aligned}
w_i &= \mathbf{a}^{(i)} \mathfrak{a}^T, \\
w_{i+n} &= \mathbf{b}^{(i)} \mathfrak{b}^T, \\
\tilde{w}_i &= w_i \gamma + w_{i+n} \gamma^q.
\end{aligned}$$

We define the map  $\psi$  to take  $\mathbf{w}$  to  $\tilde{\mathbf{w}}$ . Let the maps  $\psi$ ,  $\varphi$  and  $\tilde{\varphi}$  act component-wise on sets and matrices. Consequently, elements of an error basis can be studied in their different finite field representations, with the bijective maps  $\varphi$ ,  $\tilde{\varphi}$  and  $\psi$  depicted in Figure 1.

## B. Stabilizer Codes

Given a prime number  $p$ , let  $q = p^k$  where  $k$  is a positive integer. Given a subset  $S \subset \mathcal{E}_q^{\otimes n}$  where  $\varphi(S)$  is an additive group with  $s$  independent additive generators, the maximal subspace of  $(\mathbb{C}^q)^{\otimes n}$  left invariant under the action of all elements of  $S$  is called an  $[[n, n - \frac{s}{k}]_q$  stabilizer code. The sets  $S$ ,  $\varphi(S)$  and  $\tilde{\varphi}(S)$  are the stabilizers of our stabilizer code in the matrix representation, the  $\mathbb{F}_q^{2n}$ -representation and the  $\mathbb{F}_{q^2}^n$ -representation respectively. We study stabilizer codes in the language of finite fields [3, 5].

Consider the full rank generator matrix  $G = (G_{\text{stb}}; G_{\mathbf{x}}; G_{\mathbf{z}})$  over  $\mathbb{F}_q$  with  $(2kn - s)$  rows and  $2n$  columns where the stabilizer generator  $G_{\text{stb}} = (\mathbf{s}^{(1)}; \dots; \mathbf{s}^{(s)})$ , the logical-X generator  $G_{\mathbf{x}} = (\mathbf{x}^{(1)}; \dots; \mathbf{x}^{(kn-s)})$ , and the logical-Z generator  $G_{\mathbf{z}} = (\mathbf{z}^{(1)}; \dots; \mathbf{z}^{(kn-s)})$  are submatrices of  $G$ . We also require  $G = (G_{\text{stb}}; G_{\mathbf{x}}; G_{\mathbf{z}})$  to have the properties:

1. Each row of  $G_{\text{stb}}$  is  $s$ -orthogonal to every row of  $G$ .
2. For all  $i, j \in [kn - s]$ ,  $\langle \mathbf{x}^{(i)}, \mathbf{z}^{(j)} \rangle_s = \delta_{i,j}$ , where  $\delta_{i,j}$  is the Kronecker delta.

The error basis elements corresponding to the rows of  $G_{\mathbf{x}}$  and  $G_{\mathbf{z}}$  are generators for logical operations that can be applied on the stabilizer code.

We denote the additive (not necessarily linear) classical codes generated by  $G_{\text{stb}}$  and  $G$  under field addition by  $C_{\text{stb}}$  and  $C_{\text{nrn}}$  respectively. The set of all elements in  $\mathbb{F}_q^{2n}$  that are  $s$ -orthogonal to all elements in  $C_{\text{stb}}$  is  $C_{\text{nrn}}$ . The minimum distance of our stabilizer code is the minimum distance of the punctured code  $\tilde{C}_{\text{pnc}} := \{x \in \psi(C_{\text{nrn}}) : x \notin \psi(C_{\text{stb}})\}$  [5]. We denote an  $[[n, n - \frac{s}{k}]_q$  stabilizer code with distance  $d$  as  $[[n, n - \frac{s}{k}, d]_q$ . The rate of the stabilizer code is  $1 - \frac{s}{kn}$  and its relative distance is  $\frac{d}{n}$ .

We define a *random*  $[[n, n - \frac{s}{k}]_q$  stabilizer code to be a stabilizer code corresponding to a generator matrix  $G = (G_{\text{stb}}; G_{\mathbf{x}}; G_{\mathbf{z}})$  chosen uniformly at random from all possible generator matrices with  $(2kn - s)$  rows and  $2n$  columns over the vector field  $\mathbb{F}_q^{2n}$ .

Let the rates and relative distances of an infinite code sequence of  $\{[[n, nr_n, n\delta_n]_q\}_n$  converge to the positive numbers  $r$  and  $\delta$  respectively. If

$$\delta \geq H_{q^2}^{-1} \left( \frac{1-r}{2} \right), \quad (\text{II.6})$$

we say that the code sequence attains the asymptotic quantum  $q$ -ary GV bound.

### C. Concatenation of Stabilizer Codes

Concatenation makes a longer code from an appropriately chosen set of shorter codes. We consider only the concatenation of stabilizer codes. Let  $q = p^k$  where  $p$  is prime.

The quantum message that we wish to encode into a concatenated quantum code is a  $q^K$ -dimension quantum state which is first encoded into an  $[[N, K]]_q$  *outer code*. Let our  $[[N, K]]_q$  outer code be generated by  $G^{(\text{out})} = (G_{\text{stb}}^{(\text{out})}; G_{\mathbf{x}}^{(\text{out})}; G_{\mathbf{z}}^{(\text{out})})$ . The outer code comprises of  $N$  blocks of dimension  $q$  complex Euclidean spaces, with each of these  $N$  blocks further encoded as an  $[[n, k]]_p$  *inner code*. Let the  $j$ -th  $[[n, k]]_p$  inner code be generated by  $G^{(j)} = (G_{\text{stb}}^{(j)}; G_{\mathbf{x}}^{(j)}; G_{\mathbf{z}}^{(j)})$ , with  $G_{\mathbf{x}}^{(j)} = (\mathbf{x}^{(j),1}; \dots; \mathbf{x}^{(j),k})$  and  $G_{\mathbf{z}}^{(j)} = (\mathbf{z}^{(j),1}; \dots; \mathbf{z}^{(j),k})$  for  $j \in [N]$ . The resultant code is a concatenated code with parameters  $[[nN, kK]]_p$  generated by  $G^{(\text{concat})} = (G_{\text{stb}}^{(\text{concat})}; G_{\mathbf{x}}^{(\text{concat})}; G_{\mathbf{z}}^{(\text{concat})})$ .

We now elucidate the construction of the generator of the concatenated code  $G^{(\text{concat})}$  using the generator of the outer code  $G^{(\text{out})}$  and the generators of the inner codes  $G^{(j)}$  for  $j \in [N]$ .

Using the notation defined in Section II A, let the letter  $w \in \mathbb{F}_{q^2}$  have the decomposition  $w = \mathbf{a}\mathbf{0}^T\gamma + \mathbf{b}\mathbf{b}^T\gamma^q$  where  $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_p^k$ . We define the image of  $w$  over the smaller field  $\mathbb{F}_{p^2}$  with respect to the  $j$ -th inner code to be the  $\psi(C_{\text{stb}}^{(j)})$ -coset representative given by

$$\pi^{(j)}(w) := \sum_{\ell=1}^k (a_{\ell}\mathbf{x}^{(j),\ell} + b_{\ell}\mathbf{z}^{(j),\ell}). \quad (\text{II.7})$$

Given vectors  $\mathbf{s} \in [N]^m$  and  $\mathbf{w} \in \mathbb{F}_{q^2}^m$ , we define  $\pi^{\mathbf{s}}(\mathbf{w}) := (\pi^{(s_1)}(w_1) | \dots | \pi^{(s_m)}(w_m))$ . As a shorthand we define  $\pi := \pi^{(1, \dots, N)}$ . Let  $\pi$  also act component-wise on both matrices and sets. Then the  $\mathbb{F}_{p^2}$ -representations of the stabilizer generator, the X-logical generator and the Z-logical generator of our concatenated code are given by

$$\psi(G_{\text{stb}}^{(\text{concat})}) = \left( \pi(\psi(G_{\text{stb}}^{(\text{out})})); \begin{pmatrix} \psi(G_{\text{stb}}^{(1)}) & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \psi(G_{\text{stb}}^{(2)}) & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \ddots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \psi(G_{\text{stb}}^{(N)}) \end{pmatrix} \right) \\ \psi(G_{\mathbf{x}}^{(\text{concat})}) = \pi(\psi(G_{\mathbf{x}}^{(\text{out})})), \quad \psi(G_{\mathbf{z}}^{(\text{concat})}) = \pi(\psi(G_{\mathbf{z}}^{(\text{out})})) \quad (\text{II.8})$$

respectively. The  $\mathbb{F}_{p^2}$ -representations of the stabilizer and the normalizer of the concatenated code are  $\psi(C_{\text{stb}}^{(\text{concat})}) := \pi(\psi(C_{\text{stb}}^{(\text{out})})) + \psi(C_{\text{stb}}^{(1)} \times \dots \times C_{\text{stb}}^{(N)})$  and  $\psi(C_{\text{norm}}^{(\text{concat})}) := \pi(\psi(C_{\text{norm}}^{(\text{out})})) + \psi(C_{\text{stb}}^{(\text{concat})})$  respectively.

In this paper, we use some of the  $q$ -ary quantum codes of Li, Xing and Wang [20] as the outer codes of our concatenated codes. The stabilizers and normalizers of these codes are classical MDS codes in the  $\mathbb{F}_{q^2}$ -representation, which is not necessarily the case for other quantum codes [19].

**Theorem II.2** (Li, Xing, Wang [20]). *Let  $N$  be a prime power and  $K$  be an even integer in  $[0, N]$  such that  $\frac{N-K}{2}$  is also an integer. Then there exists a quantum generalized Reed-Solomon code with parameters  $[[N, K, \frac{N-K}{2} + 1]]_N$ . Moreover, the stabilizer  $\psi(C_{\text{stb}})$  and normalizer  $\psi(C_{\text{norm}})$  of this code in the  $\mathbb{F}_{N^2}$ -representation are classical generalized Reed-Solomon codes (are hence classical MDS codes), with  $\psi(C_{\text{norm}}) = \psi(C_{\text{stb}})^{\perp h}$ .*

### III. THE MAIN RESULT

Our main result is that our sequence of concatenated  $p$ -ary quantum codes asymptotically attains the quantum GV bound. The outer code is a quantum generalized RS code with  $\psi(C_{\text{norm}}) = \psi(C_{\text{stb}})^{\perp h}$  given by [20], and the inner codes are independently chosen random stabilizer codes. Theorem III.1 is our main result.

**Theorem III.1.** *Let  $r, R \in \mathbb{Q} \cap [0, 1]$  be the rates of the inner and outer code respectively. Let  $p$  be a prime number and  $n$  be a positive integer such that  $rn, N = p^{rn}$ , and  $\frac{1-R}{2}N \in \mathbb{Z}$  are also integers. Also suppose that*

$$R < \min \{1 - 2H_{p^2}(1 - p^{r-1}), 1\}. \quad (\text{III.1})$$

*Let  $[[nN, rRnN, d]]_p$  be a concatenated quantum code with a  $[[N, RN]]_N$  outer code of given by Theorem II.2 concatenated with  $N$  independent and identically distributed random  $[[n, rn]]_p$  inner quantum codes. Then with probability at least  $1 - \frac{1}{p^2-1}p^{-2N(\frac{1-R}{2})}$ ,*

$$\frac{d}{nN} > H_{p^2}^{-1} \left( \frac{1 - rR}{2} \right) - \frac{3c(p^2, \frac{1+r}{2})}{2n}$$

*where  $c(p^2, \frac{1+r}{2})$  is a continuity constant as defined in the Appendix in equation (IV.4).*

**Corollary III.2.** *Let  $p$  be a prime and  $r, R \in [0, 1]$  such that the inequality (III.1) holds. For all positive integers  $n$ , let  $k_n = \lceil nr \rceil$ ,  $N_n = p^{k_n}$  and  $K_n = N_n - 2^{\lceil \frac{1-R}{2} \rceil}$ . Let  $C_n$  be a code formed by concatenating an  $[[N_n, K_n]]_{N_n}$  outer code given by Theorem II.2 with  $N_n$  independent and identically distributed random  $[[n, k_n]]_p$  stabilizer codes. Then the code sequence  $\{C_n\}_{n \in \mathbb{Z}^+}$  asymptotically attains the quantum Gilbert-Varshamov bound.*

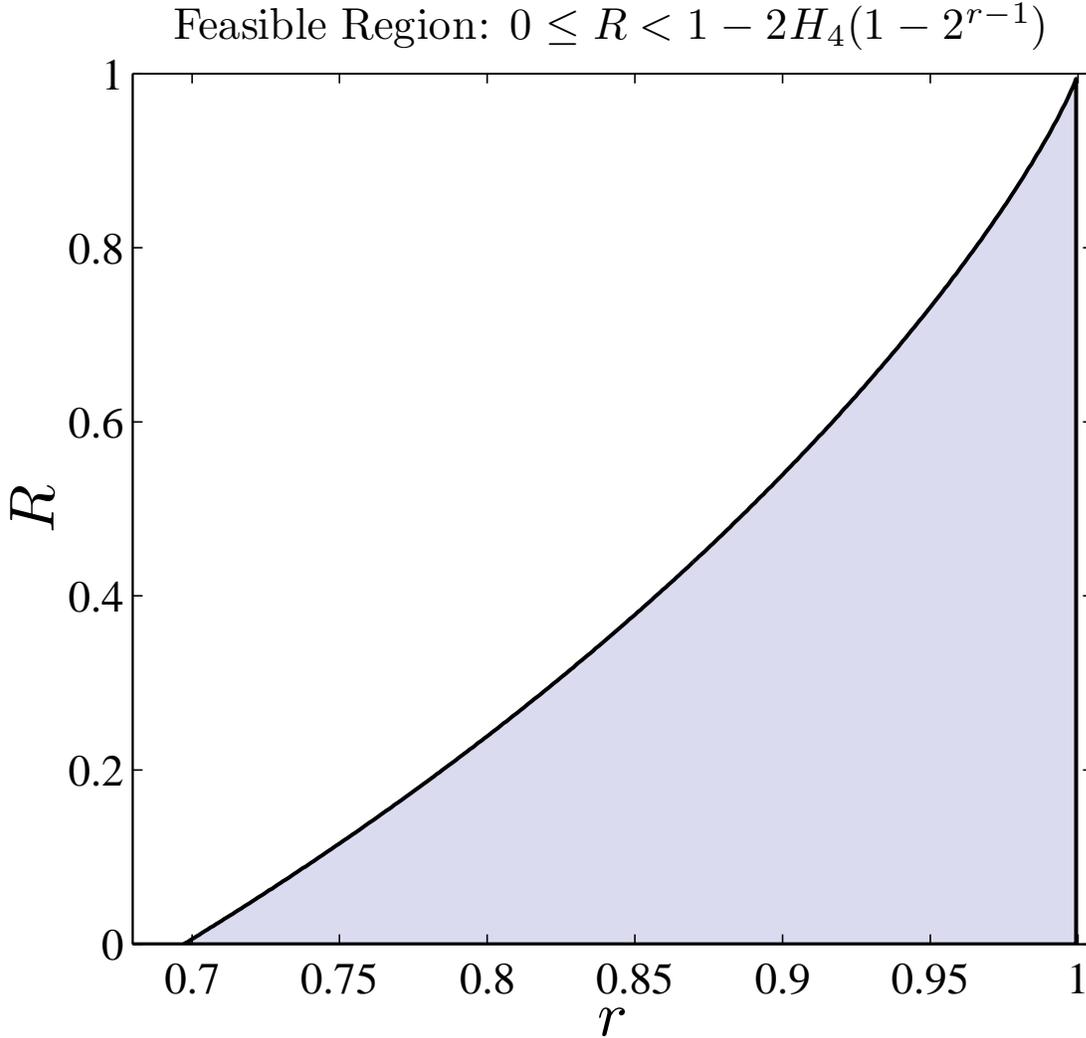


FIG. 2: When  $p = 2$ , the shaded region depicts the rates  $r$  and  $R$  for which Theorem III.1 applies.

We proceed to introduce Proposition III.3 and Lemma III.4, which are used in the random coding aspects of the proof of Theorem III.1.

**Proposition III.3.** *Let  $\mathbf{w}$  be any nonzero element of  $\mathbb{F}_{p^2}^n$ . Let  $\psi(C_{\text{norm}})$  and  $\psi(C_{\text{stb}})$  be the normalizer and stabilizer over  $\mathbb{F}_{p^2}$  of a random  $[[n, k]]_p$  stabilizer code, and*

let the corresponding punctured code be  $\tilde{C}_{\text{pnc}} := \{\mathbf{w} \in \psi(C_{\text{nrnm}}) : \mathbf{w} \notin \psi(C_{\text{stb}})\}$ . Then  $\Pr[\mathbf{w} \in \tilde{C}_{\text{pnc}}] < p^{-(n+k)}$ .

*Proof.* Let  $U \subset \mathbb{F}_p^{2n}$  be a set of independent mutually  $s$ -orthogonal vectors. Then the number of vectors in  $\mathbb{F}_p^{2n}$  that are  $s$ -orthogonal to all elements of  $U$  is  $p^{2n-|U|}$ . Hence  $\Pr[\mathbf{w} \in \psi(C_{\text{nrnm}})] = \frac{\prod_{i=0}^{n-k-1} (p^{2n-1-i} - p^i)}{\prod_{i=0}^{n-k-1} (p^{2n-i} - p^i)} < p^{-(n-k)}$ . The number of cosets of  $C_{\text{stb}}$  in  $C_{\text{nrnm}}$  distinct from  $C_{\text{stb}}$  is  $p^{2k} - 1$ . Hence  $\Pr[\mathbf{w} \in \tilde{C}_{\text{pnc}}] < p^{-(n-k)} \frac{1}{p^{2k}-1} < p^{n+k}$ .

**Lemma III.4.** Let  $\mathbf{W}$  be any nonzero vector in  $\mathbb{F}_{q^2}^N$  of weight  $w$ , and  $h$  be a positive integer no greater than  $\frac{p^2-1}{p^2}nw$ . Let  $S = \pi(\mathbf{W}) + \psi(C_{\text{stb}}^{(1)} \times \dots \times C_{\text{stb}}^{(N)})$  be a random coset. Then  $\Pr[\text{minwt}(S) \leq h] < (p^2)^{nwH_{p^2}(\frac{h}{nw})} p^{-(n+k)w}$ .

*Proof.* The minimum weight of  $S$  is equal to the minimum weight of the random coset  $S' = \pi((W_1, \dots, W_w)) + \psi(C_{\text{stb}}^{(1)} \times \dots \times C_{\text{stb}}^{(w)})$ , where  $W_1, \dots, W_w$  are the nonzero letters of  $\mathbf{W}$ . When  $h \leq \frac{p^2-1}{p^2}nw$ , there are at most  $(p^2)^{nwH_{p^2}(\frac{h}{nw})}$  members of  $\mathbb{F}_{p^2}^n$  of weight no more than  $h$  (see [16]). Let  $\mathbf{w} = (\mathbf{v}_1 | \dots | \mathbf{v}_w)$  be any such member of  $\mathbb{F}_{p^2}^{nw}$ , where  $\mathbf{v}_1, \dots, \mathbf{v}_w \in \mathbb{F}_{p^2}^n$ . If  $\mathbf{w}$  is also an element of  $S'$ , each  $\mathbf{v}_i$  is necessarily an element of the non-trivial random coset  $\pi^{(i)}(W_i) + \psi(C_{\text{stb}}^{(i)})$ , the probability of which is less than  $p^{-(n+k)}$  by the Proposition III.3. Hence the probability that  $\mathbf{w}$  is an element of the random set  $S'$  is less than  $p^{-(n+k)w}$ . Subsequently, applying the union bound on the number of  $\mathbf{w}$  with a weight no more than  $h$  gives the result.

Now we proceed to prove our main result, Theorem III.1.

*Proof of Theorem III.1.* To prove our main result, we have to find a designed distance  $h > 0$  such that:

1. The probability that the distance of our concatenated quantum code is less than  $h$  is negligible.
2. The designed relative distance  $\frac{h}{nN}$  asymptotically attains the quantum GV bound.

We first determine a sufficient condition for  $\Pr[d \leq h]$  to vanish as  $n$  becomes large. Now our outer code's normalizer  $\psi(C_{\text{nrnm}}^{(\text{out})})$  is a classical MDS code [20] with parameters  $[N, NR_{\text{nrnm}}, D]_{q^2}$  where  $D = N(1 - R_{\text{nrnm}}) + 1$  and  $R_{\text{nrnm}} := \frac{1+R}{2}$ . The MDS property of

our outer code's normalizer implies that the spectrum of the normalizer  $A_w$ , defined as the number of codewords in  $\psi(C_{\text{nrnm}}^{(\text{out})})$  with weight  $w \in [D, N]$ , is at most  $\binom{N}{w} (p^{2k})^{w-D+1}$  (see the references [1, 16]). Let  $\tilde{C}_{\text{pnc}}^{(\text{concat})} := \{\mathbf{W} \in \psi(C_{\text{nrnm}}^{(\text{concat})}) : \mathbf{W} \notin \psi(C_{\text{stb}}^{(\text{concat})})\}$ . Our upper bound on the spectrum  $A_w$ , the union bound and Lemma III.4 imply that

$$\begin{aligned} \Pr[d \leq h] &= \Pr[\text{minwt}(\tilde{C}_{\text{pnc}}^{(\text{concat})}) \leq h] \\ &\leq \sum_{\substack{\mathbf{W} \in \psi(C_{\text{nrnm}}^{(\text{out})}) \\ \mathbf{W} \neq \mathbf{0}}} \Pr \left[ \text{minwt}(\pi(\mathbf{W}) + \psi(C_{\text{stb}}^{(1)}) \times \dots \times C_{\text{stb}}^{(N)}) \leq h \right] \\ &< \sum_{w=D}^N 2^N (p^{2k})^{w-D+1} (p^2)^{nw H_{p^2}(\frac{h}{nw}) - \frac{n+k}{2}w} \leq \sum_{w=D}^{\infty} (p^2)^{-nw\eta}, \end{aligned}$$

where

$$\eta := -\frac{N}{2nw} - r \left(1 - \frac{D}{w} + \frac{1}{w}\right) - H_{p^2} \left(\frac{h}{nw}\right) + \frac{1+r}{2}. \quad (\text{III.2})$$

Now let  $\theta = 1 - \frac{D}{w} + \frac{1}{w}$  and observe that  $0 \leq \theta < R_{\text{nrnm}}$  for our feasible values of  $w$ . If  $\eta \geq \frac{1}{n}$  for all  $w \in [D, N]$ , then  $\Pr[d \leq h] \leq (p^2)^{-D} \frac{1}{1-p^{-2}}$ . We will determine feasible values of the designed distance  $h$  for which the inequality  $\eta \geq \frac{1}{n}$  holds.

Since the inverse entropy function is monotone increasing on the open unit interval, it suffices to require that our choice of  $h$  satisfies the inequality

$$\frac{h}{nN} \leq \frac{w}{N} H_{p^2}^{-1} \left( \frac{1+r}{2} - r\theta - \frac{N}{2nw} - \frac{1}{n} \right). \quad (\text{III.3})$$

It suffices to have  $\frac{h}{nN}$  equal to some lower bound on the right hand side of the inequality (III.3). Continuity of the inverse entropy (Lemma IV.1) and the substitution  $\frac{w}{N} = \frac{1-R_{\text{nrnm}}}{1-\theta}$  gives

$$\begin{aligned} &\frac{1-R_{\text{nrnm}}}{1-\theta} H_{p^2}^{-1} \left( \frac{1+r}{2} - r\theta - \frac{1}{n} \left( \frac{N}{2w} + 1 \right) \right) \\ &\geq \frac{1-R_{\text{nrnm}}}{1-\theta} H_{p^2}^{-1} \left( \frac{1+r}{2} - r\theta \right) - \left( \frac{1}{2} + \frac{w}{N} \right) \frac{c(p^2, \frac{1+r}{2} - r\theta)}{n}. \end{aligned} \quad (\text{III.4})$$

The inequality (III.1) together with our restriction that  $r, R \in [0, 1]$  imply that  $r$  and  $R$  satisfy the requirements of Lemma IV.1. Hence Lemma IV.1 implies that  $\frac{1-R_{\text{nrnm}}}{1-\theta} H_{p^2}^{-1} \left( \frac{1+r}{2} - r\theta \right)$  is a monotonic non-increasing function of  $\theta$ . Since  $\frac{c(p^2, \frac{1+r}{2} - r\theta)}{n}$  is also a monotonic non-increasing function of  $\theta$  for feasible values of  $r$  and  $R$ , the right hand side of (III.4) is at least  $H_{p^2}^{-1} \left( \frac{1+r}{2} \right) - \frac{3c(p^2, \frac{1+r}{2})}{2n}$  by setting  $\theta$  to be  $R_{\text{nrnm}}$ . We set  $\frac{h}{nN}$  to be this lower bound so that the inequality (III.3) holds, from which the result follows.

#### IV. APPENDIX : THE Q-ARY ENTROPY AND ITS INVERSE

In this section, we derive properties of the  $q$ -ary entropy function and its inverse. Since  $H_q$  is a strictly increasing concave function on  $(0, \frac{q-1}{q})$ ,  $H_q^{-1}$  is a strictly increasing convex function on the open interval  $(0, 1)$ . Observe that for  $x \in (0, 1)$ ,

$$H'_q(x) := \frac{d}{dx} H_q(x) = \log_q(q-1) - \log_q x + \log_q(1-x), \quad (\text{IV.1})$$

$$(1-x)H'_q(1-x) = H_q(1-x) + \log_q x. \quad (\text{IV.2})$$

Since  $H_q(y)$  is a continuously differentiable function for  $y \in (0, 1 - \frac{1}{q})$ , by the inverse function theorem, we have that

$$(H_q^{-1})'(y) = \frac{1}{H'_q(H_q^{-1}(y))} \quad (\text{IV.3})$$

for  $y \in (0, 1)$ , where  $(H_q^{-1})'(y) := \frac{d}{dy} H_q^{-1}(y)$ . These technical properties of the  $q$ -ary entropy function are used to obtain Lemma IV.1 which pertains to the monotonicity of  $\frac{1}{1-\theta} H_q^{-1}(\frac{1+r}{2} - r\theta)$  with respect to  $\theta$ , and Lemma IV.2 which is about continuity.

Now define  $f := 1 - H_q^{-1}(\frac{1+r}{2} - r\theta)$ . Observe that  $\frac{df}{d\theta} = r(H_q^{-1})'(\frac{1+r}{2} - r\theta) = \frac{r}{H'_q(H_q^{-1}(\frac{1+r}{2} - r\theta))} = \frac{r}{H'_q(1-f)}$ . We now introduce Lemma IV.1 which makes an assertion on the monotonicity of the function  $\frac{1-f}{1-\theta}$ .

**Lemma IV.1.** *[Monotonicity] Let  $p$  be prime,  $q = p^2$ , and  $r, R \in [0, 1]$  such that (III.1) holds. Then  $\frac{1-f}{1-\theta}$  is a non-increasing function with respect to  $\theta \in [0, \frac{1+R}{2}]$ .*

*Proof.* Now  $\frac{d}{d\theta} \frac{1-f}{1-\theta} = \frac{1-f}{(1-\theta)^2} - \frac{1}{1-\theta} \frac{df}{d\theta}$  and  $\frac{df}{d\theta} = \frac{r}{H'_q(1-f)}$ . Hence  $\frac{d}{d\theta} \frac{1-f}{1-\theta} \leq 0$  if and only if  $(1-f)H'_q(1-f) \leq r(1-\theta)$ . From (IV.2), we get

$$(1-f)H'_q(1-f) = H_q(1-f) + \log_q f = \left( \frac{1+r}{2} - r\theta \right) + \log_q f.$$

Thus  $(1-f)H'_q(1-f) \leq r(1-\theta)$  holds if and only if  $r \geq 1 + 2 \log_q f$ , the latter inequality of which holds because of (III.1).

**Lemma IV.2.** *[Continuity] Let  $x, y \in (0, \frac{q-1}{q})$  where the integer  $q$  is greater than 2 and  $x > y$ . Then  $H_q^{-1}(y) \geq H_q^{-1}(x) - (x-y)c(q, x)$ , where our continuity constant is*

$$c(q, x) := \left( \log_q(q-1) + \log_q \left( \frac{1}{H_q^{-1}(x)} - 1 \right) \right)^{-1}. \quad (\text{IV.4})$$

*Proof.* The convexity and continuous differentiability of  $H_q^{-1}$  on the unit open interval imply that  $H_q^{-1}(y) \geq H_q^{-1}(x) - (x - y)(H_q^{-1})'(x)$ . Use of (IV.1) with (IV.3) then gives the result.

- 
- [1] C. Thommesen, “The existence of binary linear concatenated codes with Reed-Solomon outer codes which asymptotically meet the Gilbert-Varshamov bound,” *IEEE Transactions on Information Theory*, vol. 29, no. 6, pp. 850–853, 1983.
  - [2] E. Rains, “Nonbinary quantum codes,” *IEEE Transactions on Information Theory*, vol. 45, pp. 1827–1832, Sep 1999.
  - [3] D. Gottesman, *Stabilizer Codes and Quantum Error Correction*. PhD thesis, California Institute of Technology, 1997. quant-ph/9705052.
  - [4] A. Ashikhmin, A. Barg, E. Knill, and S. Litsyn, “Quantum error detection .II. bounds,” *IEEE Transactions on Information Theory*, vol. 46, pp. 789–800, May 2000.
  - [5] A. Ashikhmin and E. Knill, “Nonbinary quantum stabilizer codes,” *IEEE Transactions on Information Theory*, vol. 47, pp. 3065–3072, Nov 2001.
  - [6] K. Feng and Z. Ma, “A finite Gilbert-Varshamov bound for pure stabilizer quantum codes,” *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3323–3325, 2004.
  - [7] Y. Ma, “The asymptotic probability distribution of the relative distance of additive quantum codes,” *Journal of Mathematical Analysis and Applications*, vol. 340, pp. 550–557, 2008.
  - [8] L. Jin and C. Xing, “Quantum Gilbert-Varshamov bound through symplectic self-orthogonal codes,” in *IEEE International Symposium on Information Theory Proceedings (ISIT)*, pp. 455–458, Aug 2011.
  - [9] A. Ashikhmin, S. Litsyn, and M. A. Tsfasman, “Asymptotically good quantum codes,” *Phys. Rev. A*, vol. 63, p. 032311, Feb 2001.
  - [10] R. Matsumoto, “Improvement of Ashikhmin-Litsyn-Tsfasman bound for quantum codes,” *IEEE Transactions on Information Theory*, vol. 48, pp. 2122–2124, Jul 2002.
  - [11] H. Chen, S. Ling, and C. Xing, “Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound,” *IEEE Transactions on Information Theory*, vol. 47, pp. 2055–2058, Jul 2001.

- [12] H. Fujita, “Several classes of concatenated quantum codes: Constructions and bounds,” *IEIC Technical Report (Institute of Electronics, Information and Communication Engineers)*, vol. 105, no. 662, pp. 195–200, 2006.
- [13] M. Hamada, “Concatenated quantum codes constructible in polynomial time: Efficient decoding and error correction,” *IEEE Transactions on Information Theory*, vol. 54, pp. 5689–5704, Dec 2008.
- [14] Z. Li, L. Xing, and X. Wang, “A family of asymptotically good quantum codes based on code concatenation,” *IEEE Transactions on Information Theory*, vol. 55, pp. 3821–3824, Aug 2009.
- [15] A. Nohage, “Nonbinary quantum Goppa codes exceeding the quantum Gilbert-Varshamov bound,” *Quantum Information Processing*, vol. 6, no. 3, pp. 143–158, 2007.
- [16] F. J. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*. North-Holland publishing company, first ed., 1977.
- [17] J. Justesen, “Class of constructive asymptotically good algebraic codes,” *IEEE Transactions on Information Theory*, vol. 18, pp. 652–656, Sep 1972.
- [18] M. Grassl, W. Geiselmann, and T. Beth, “Quantum Reed-Solomon codes,” *Proceedings Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-13), Springer Lecture Notes in Computer Science*, p. 1719, 1999.
- [19] M. Grassl, T. Beth, and M. Roetteler, “On optimal quantum codes,” *International Journal of Quantum Information*, vol. 2, no. 1, pp. 55–64, 2004.
- [20] Z. Li, L.-J. Xing, and X.-M. Wang, “Quantum generalized Reed-Solomon codes: Unified framework for quantum maximum-distance-separable codes,” *Phys. Rev. A*, vol. 77, p. 012308, Jan 2008.