IEEE Transactions on Quantum Engineering

Received March 30, 2021; revised May 1, 2021; accepted May 4, 2021; date of publication May 14, 2021; date of current version.

Digital Object Identifier 10.1109/TQE.2021.3078152

$\mathbb{F}_p$-Linear and $\mathbb{F}_{p^m}$-Linear Qudit Codes From Dual-Containing Classical Codes

PRIYA J. NADKARNI (Member, IEEE), AND SHAYAN SRINIVASA GARANI (Senior Member, IEEE)

Department of Electronic Systems Engineering, Indian Institute of Science, Bangalore 560012, India

Corresponding author: Shayan Srinivasa Garani (e-mail: shayangs@iisc.ac.in).

The work of Priya. J. Nadkarni was supported by a fellowship from the Ministry of Electronics and Information Technology, Government of India. The work of Shayan Srinivasa Garani was supported by the Ministry of Human Resource Development, Government of India.

ABSTRACT Quantum code construction from two classical codes $D_1[n, k_1, d_1]$ and $D_2[n, k_2, d_2]$ over the field $\mathbb{F}_{p^m}$ (p is prime and m is an integer) satisfying the dual containing criteria $D_1^{\perp} \subset D_2$ using the Calderbank–Shor–Steane (CSS) framework is well-studied. We show that the generalization of the CSS framework for qubits to qudits yields two different classes of codes, namely, the $\mathbb{F}_p$-linear CSS codes and the well-known $\mathbb{F}_{p^m}$-linear CSS codes based on the check matrix-based definition and the coset-based definition of CSS codes over qubits. Our contribution to this article are three-folds. 1) We study the properties of the $\mathbb{F}_p$-linear and $\mathbb{F}_{p^m}$-linear CSS codes and demonstrate the tradeoff for designing codes with higher rates or better error detection and correction capability, useful for quantum systems. 2) For $\mathbb{F}_{p^m}$-linear CSS codes, we provide the explicit form of the check matrix and show that the minimum distances d_x and d_z are equal to d_2 and d_1, respectively, if and only if the code is nondegenerate. 3) We propose two classes of quantum codes obtained from the codes D_1 and D_2, where one code is an $\mathbb{F}_{p^l}$-linear code (l divides m) and the other code is obtained from a particular subgroup of the stabilizer group of the $\mathbb{F}_{p^m}$-linear CSS code. Within each class of codes, we demonstrate the tradeoff between higher rates and better error detection and correction capability.

INDEX TERMS $\mathbb{F}_{p^m}$-linear Calderbank–Shor–Steane (CSS) codes, $\mathbb{F}_{p^m}$-linear CSS codes, CSS-like codes, dual containing codes, quantum error correction, qudit codes.

I. INTRODUCTION

Quantum codes can be constructed from classical linear block codes satisfying the dual containing criterion using the well-known stabilizer framework [1], [2]. As classical linear block codes are used in almost all classical transmission and data storage systems requiring guaranteed burst error correction capability, quantum codes obtained along these lines would be useful for building reliable quantum transmission and data storage systems.

In this article, we show that the generalization of the Calderbank–Shor–Steane (CSS) codes over qubits [3],[4] to qudits yields two classes of codes, namely the $\mathbb{F}_{p^m}$-linear CSS codes, also well-known as the CSS codes over qudits, and the $\mathbb{F}_p$-linear CSS codes. Both $\mathbb{F}_{p^m}$-linear CSS codes and $\mathbb{F}_p$-linear CSS codes are constructed from two classical codes satisfying the dual containing criteria.

The $\mathbb{F}_p$-linear CSS code over qudits is obtained using the check matrix-based construction [5] of the CSS code over qubits. Ezerman *et al.* [6] proposed the construction of CSS-like codes from nested subfield-linear codes. We show that the $\mathbb{F}_p$-linear CSS codes are a class of CSS-like codes proposed in [6]. The $\mathbb{F}_{p^m}$-linear CSS code over qudits is obtained using the coset-based construction, generalizing the work from [3] of the CSS code over qubits.

We analyze the properties of both $\mathbb{F}_{p^m}$-linear CSS codes and $\mathbb{F}_p$-linear CSS codes in detail and study the differences between them. We obtain the closed form expressions for the minimum distances of the $\mathbb{F}_p$-linear and $\mathbb{F}_{p^m}$-linear CSS codes based on the codes D_{Hd1} and D_{Hd2} and based on codes D_1 and D_2, respectively, where D_{Hd1} and D_{Hd2} are additive

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see http://creativecommons.org/licenses/by/4.0/

codes obtained based on D_1 and D_2. We show that the minimum distances d_x and d_z based on the $\mathrm{X}^{(p^m)}(\cdot)$ and $\mathrm{Z}^{(p^m)}(\cdot)$ operators are equal to the minimum distances of D_1 and D_2 for the $\mathbb{F}_{p^m}$-linear CSS code if and only if the quantum code is nondegenerate. We provide similar results for $\mathbb{F}_p$-linear CSS codes with respect to the minimum distances of D_{Hd1} and D_{Hd2}.

We further provide the explicit form of the check matrix of the $\mathbb{F}_{p^m}$-linear CSS code.[1] An explicit form of the check matrix is useful for realizing practical quantum error correction circuits towards syndrome computation and encoding [7], [8]. Also, the isomorphism between check matrices and stabilizer generators is helpful to visualize the connections within a graph-theoretic setup for modified graph state codes, useful for developing entanglement-assisted coded quantum networks resilient to a single node failure [9].

We note that the $\mathbb{F}_{p^m}$-linear CSS codes over qudits have been proposed earlier in [10]. Other recent works on qudit CSS codes include [11]–[14] and [15]. Shao *et al.* [12] used the $\mathbb{F}_{p^m}$-linear CSS framework to construct the entanglement-assisted low-density parity-check codes over qudits. While they provide the code parameters based on the $\mathbb{F}_{p^m}$-linear CSS codes, the check matrix they provide is the check matrix of the $\mathbb{F}_p$-linear CSS code. This is technically *incorrect* as the $\mathbb{F}_{p^m}$-linear CSS codes and the $\mathbb{F}_p$-linear CSS codes yield different codes when $m \neq 1$. Thus, the study of $\mathbb{F}_{p^m}$-linear and $\mathbb{F}_p$-linear CSS codes, their differences, and the check matrix of the $\mathbb{F}_{p^k}$-linear CSS code proposed in this article becomes important.

We show that the minimum distances d_x and d_z of the $\mathbb{F}_p$-linear CSS code are lesser than those of the $\mathbb{F}_{p^m}$-linear CSS code while the rate of the $\mathbb{F}_p$-linear CSS code is larger than that of the $\mathbb{F}_{p^m}$-linear CSS code. Thus, there is a tradeoff between better error detection and correction capability and higher coding rate, and the choice between the $\mathbb{F}_p$-linear and $\mathbb{F}_{p^m}$-linear CSS code is based on the application. We note that for qudits of prime dimension, i.e., $m = 1$ and $q = p$, $\mathbb{F}_p$-linear and $\mathbb{F}_{p^m}$-linear CSS code are the same.

Finally, we provide two classes of quantum codes based on codes D_1 and D_2 and study their properties. One class of codes, called the *$\mathbb{F}_{p^l}$-linear CSS-like codes*, involves obtaining $\mathbb{F}_{p^l}$-linear quantum codes from D_1 and D_2, where l divides m. The other class of codes, called the *normal basis based CSS-like codes*, is obtained by considering particular subgroups of the stabilizer group of $\mathbb{F}_{p^m}$-linear codes based on the normal basis of $\mathbb{F}_{p^m}$ as the stabilizer groups and constructing the codes. Within both these classes of code construction, we provide a tradeoff for designing codes with higher rates or better error detection and correction, useful for quantum systems. We demonstrate the same using an example. The $\mathbb{F}_p$-linear and $\mathbb{F}_{p^m}$-linear CSS codes are special cases of both these proposed classes of codes. We also provide a procedure to obtain a lower bound on the X-distance and Z-distance of the proposed codes.

The problem of obtaining two classical codes C_1 and C_2 over $\mathbb{F}_p$ that satisfy the dual-containing criteria $C_1^{\perp} \subset C_2$ is a well-studied problem in quantum coding theory, especially for $p = 2$. In this article, we provide a procedure for the construction of large distance $\mathbb{F}_{p^l}$-linear CSS-like quantum codes and normal basis based CSS-like quantum codes over qudits of dimension $\mathbb{F}_{p^m}$ from classical codes over $\mathbb{F}_p$ that satisfy the dual-containing criteria and provide a few examples for the same.

This article is organized as follows. In Section II, we briefly review classical additive and linear codes, stabilizer codes over qudits, and CSS codes over qubits, useful towards the rest of the article. In Section III, we discuss the construction and code properties of $\mathbb{F}_{p^m}$-linear CSS codes and $\mathbb{F}_p$-linear CSS codes over qudits along with an explicit structure of their check matrices and illustrative examples. In Section IV, we propose two classes of quantum codes based on classical codes satisfying the dual-containing criterion and demonstrate the tradeoff between higher coding rate and better error detection and correction capability within each class. Finally, Section V concludes this article.

II. PRELIMINARIES

A. CLASSICAL ADDITIVE CODES AND LINEAR CODES

A classical code C over $\mathbb{F}_{p^m}$ is said to be *additive* if the sum of any two codewords $\boldsymbol{c_1}$ and $\boldsymbol{c_2}$ in C is also a codeword in C. A classical code C over $\mathbb{F}_{p^m}$ is said to be *linear* if the linear combination $\beta_1\boldsymbol{c_1} + \beta_2\boldsymbol{c_2}$ is also a codeword in C, where $\beta_1, \beta_2 \in \mathbb{F}_{p^m}$. Thus, every linear code over $\mathbb{F}_{p^m}$ is an additive code over $\mathbb{F}_{p^m}$, but every additive code need not be linear.

For classical additive codes over $\mathbb{F}_p$, where p is prime, $g_1\boldsymbol{c_1}$ and $g_2\boldsymbol{c_2}$ are obtained by adding $\boldsymbol{c_1}$ and $\boldsymbol{c_2}$ to themselves g_1 and g_2 times ($\because g_1, g_2 \in \mathbb{F}_p$), respectively. Thus, if $\boldsymbol{c_1}, \boldsymbol{c_2} \in C$, then $g_1\boldsymbol{c_1} + g_2\boldsymbol{c_2} \in C$ and every linear code over $\mathbb{F}_p$ is an additive linear code over $\mathbb{F}_p$. However, for a classical code C over $\mathbb{F}_{p^m}$, if $\boldsymbol{c_1}, \boldsymbol{c_2} \in C$, then by adding the codewords, only $g_1\boldsymbol{c_1} + g_2\boldsymbol{c_2} \in C$, where $g_1, g_2 \in \mathbb{F}_p$. If α is the primitive element of $\mathbb{F}_{p^m}$, then $\alpha\boldsymbol{c_1}$ cannot be obtained by adding $\boldsymbol{c_1}$ to itself multiple times. Thus, any linear combination $\beta_1\boldsymbol{c_1} + \beta_2\boldsymbol{c_2}$ need not belong to C, where $\beta_1, \beta_2 \in \mathbb{F}_{p^m}$. Thus, there exist additive codes over $\mathbb{F}_{p^m}$ that are not linear over $\mathbb{F}_{p^m}$. For codes defined over $\mathbb{F}_{p^m}$, the set of linear codes is only a subset of the set of additive codes. We note that additive codes are also called as $\mathbb{F}_p$-linear codes.

Stabilizer codes discussed in Section II-B are also known as additive quantum codes [5]. The $\mathbb{F}_{p^m}$-linear CSS codes and $\mathbb{F}_p$-linear CSS codes studied in this article are classes of stabilizer codes.

B. STABILIZER CODES OVER QUDITS

As the stabilizer codes are based on finite fields, and the size of a finite field is always a power of a prime [16], in this article, we consider qudits with $q = p^m$, where p is prime

[1] A part of this work was presented as an invited talk at the IEEE Information Theory and Applications Workshop at San Diego in February 2019.

and $m \in \mathbb{Z}^+$. A p^m-dimensional qudit is represented as $|\phi\rangle = \sum_{i\in\mathbb{F}_{p^m}} a_i|i\rangle$, where $a_i \in \mathbb{C}$ and $\sum_{i\in\mathbb{F}_{p^m}} |a_i|^2 = 1$. The qudit is also represented as $|\phi\rangle = [a_0\ a_1 \ldots a_{(p^m-1)}] \in \mathbb{C}^{p^m}$. Thus, the state of the qudit is a normalized vector in $\mathbb{C}^{p^m}$. The operators acting on a single qudit are from the unitary group $\mathrm{U}(p^m)$ [17].

Let the field trace $\mathrm{Tr}_{p^m/p^l}(\cdot)$ be the $\mathbb{F}_{p^l}$-linear function $\mathrm{Tr}_{p^m/p^l}(\beta) = \sum_{i=0}^{\frac{m}{l}-1} \beta^{(p^l)^i}$ from an element $\beta \in \mathbb{F}_{p^m}$ to an element of $\mathbb{F}_{p^l}$, where l divides m. The operators in the unitary group $\mathrm{U}(p^m)$ can be represented as a linear combination of the following unitary basis of $\mathbb{C}^{p^m\times p^m}$:

$$\mathcal{G}_{p^m}^{(b)} = \left\{\mathrm{X}^{(p^m)}(\beta)\mathrm{Z}^{(p^m)}(\gamma)|\beta, \gamma \in \mathbb{F}_{p^m}\right\} \tag{1}$$

where $\mathrm{X}^{(p^m)}(\beta)|\varepsilon\rangle = |\varepsilon + \beta\rangle$, $\mathrm{Z}^{(p^m)}(\gamma)|\varepsilon\rangle = \omega^{\mathrm{Tr}_{p^m/p}(\gamma\varepsilon)}|\varepsilon\rangle$, for every $\varepsilon \in \mathbb{F}_{p^m}$, $\omega = \mathrm{e}^{\mathrm{i}\frac{2\pi}{p}}$, and $\mathrm{i} = \sqrt{-1}$ [18]. The field isomorphic equivalent form of operator $\mathrm{X}^{(p^m)}(\beta)\mathrm{Z}^{(p^m)}(\gamma)$ is $[\beta|\gamma]_{p^m}$. The error group is [18]

$$\mathcal{G}_{p^m} = \left\{\kappa^j\omega^l\mathrm{X}^{(p^m)}(\beta)\mathrm{Z}^{(p^m)}(\gamma)\middle|\beta,\gamma \in \mathbb{F}_{p^m}, l\in\mathbb{Z}_p, j \in \mathbb{Z}_4\right\} \tag{2}$$

where $\kappa = \mathrm{i}^{1_{p=2}}$ and $1_{p=2}$ is an indicator function which is equal to 1 when $p = 2$, else it is equal to 0.

For $\beta \in \mathbb{F}_{p^m}$, the qudit state and the operators acting on it can be represented as a tensor product of m states and operators for p-dimensional qudits, respectively [19]. Let α be the primitive element of $\mathbb{F}_{p^m}$. Let the representation of β in terms of $\{1, \alpha, \ldots, \alpha^{m-1}\}$ be $\beta = b_0 + b_1\alpha + \cdots + b_{m-1}\alpha^{(m-1)} \equiv [b_0\ b_1\ \ldots\ b_{m-1}]$, where $b_0, b_1, \ldots, b_{m-1} \in \mathbb{F}_p$. Then

$$|\beta\rangle_{p^m} = |b_{m-1}\rangle_p \otimes |b_{m-2}\rangle_p \otimes \cdots \otimes |b_0\rangle_p \tag{3}$$

$$\mathrm{X}^{(p^m)}(\beta) = \mathrm{X}^{(p)}(b_{m-1}) \otimes \mathrm{X}^{(p)}(b_{m-2}) \otimes \cdots \otimes \mathrm{X}^{(p)}(b_0) \tag{4}$$

$$\mathrm{Z}^{(p^m)}(\gamma) = \mathrm{Z}^{(p)}(\mathrm{Tr}_{p^m/p}(\gamma\alpha^{(m-1)})) \otimes \mathrm{Z}^{(p)}(\mathrm{Tr}_{p^m/p}(\gamma\alpha^{(m-2)})) \otimes \cdots \otimes \mathrm{Z}^{(p)}(\mathrm{Tr}_{p^m/p}(\gamma)) \tag{5}$$

where the field trace $\mathrm{Tr}_{p^m/p}(\cdot)$ is obtained by considering $l = 1$ in $\mathrm{Tr}_{p^m/p^l}(\cdot)$.

We call each of the p-dimensional components as *subqudits* [19]. Thus, a qudit of dimension p^m has m subqudits, each of dimension p.

A subset of a group is called its *minimal generating set* if no element of the set can be generated from compositions of other elements of the set and the set generates the whole group. The elements of the minimal generating set of a group are called the *minimal generators* of the group. The minimal generating set of a group is analogous to a basis of a vector space.

Let S be an abelian subgroup of $\mathcal{G}_{p^m}^{\otimes n}$ that does not contain any element of the form $\kappa^j\omega^l\mathrm{I}_{p^m}$ with $\kappa^j\omega^l \neq 1$, where $n \in \mathbb{Z}^+$, $l\in\mathbb{Z}_p$, $j \in \mathbb{Z}_4$, and $\kappa = \mathrm{i}^{1_{p=2}}$. Let the minimal generators of S be $S_1, S_2, \ldots, S_\rho$, where $\rho \leq mn$. The stabilizer code $\mathcal{Q}_S$ over qudits is obtained as the set of all quantum states over n qudits that are stabilized by the elements of S, i.e.

$$\mathcal{Q}_S = \left\{|\psi\rangle \in \mathbb{C}^{p^{mn}}\middle|S_i|\psi\rangle = |\psi\rangle\ \forall i \in \{1, 2, \ldots, \rho\}\right\}. \tag{6}$$

The group S is called the *stabilizer group* of the code $\mathcal{Q}_S$.

The dimension of $\mathcal{Q}_S$ is $p^{mn-\rho}$ [10], [17]. The minimum distance d is the minimum of the weight of all nonidentity undetectable errors that transform one codeword to another. An error E is detectable if its eigenvalue-based syndrome $\boldsymbol{s} = [s_1\ s_2\ \ldots\ s_\rho]$ is nonzero, where s_i is obtained from $S_iE = \omega^{s_i}ES_i$, for $i \in \{1, \ldots, \rho\}$. For E to be an undetectable error, $\boldsymbol{s} = \boldsymbol{0}$; hence, $s_i = 0$ and E commutes with all minimal stabilizer generators, i.e., $S_iE = ES_i$.

The normalizer $\mathcal{N}_S$ of the stabilizer group S is the set of all elements in $\mathcal{G}_{p^m}^{\otimes n}$ that commute with the elements of S [1]. As the elements of the stabilizer group stabilize the codewords and $S \subset \mathcal{N}_S$, the set $\mathcal{N}_S \setminus S$ is the set of undetectable errors. The rest of the errors in $\mathcal{G}_{p^m}^{\otimes n} \setminus \mathcal{N}_S$ are detectable errors. The minimum distance d of $\mathcal{Q}_S$ is the minimum of the weight of the elements of $\mathcal{N}_S \setminus S$, where the weight of an operator O is the number of qudits on which it performs nonidentity operations [1]. Thus, from S, an $((n, p^{mn-\rho}, d))_{p^m}$ stabilizer code is obtained. This stabilizer code can detect $(d-1)$ qudits in error and correct $\lfloor\frac{d-1}{2}\rfloor$ qudits in error.

For symmetric stabilizer codes, the error detection/correction capability for $\mathrm{X}^{(p^m)}(\cdot)$ and $\mathrm{Z}^{(p^m)}(\cdot)$ errors are the same. *Asymmetric stabilizer codes* are associated with two distances, namely the X-distance d_x and Z-distance d_z, that are related to the error detection/correction capability of $\mathrm{X}^{(p^m)}(\cdot)$ and $\mathrm{Z}^{(p^m)}(\cdot)$ errors, respectively. An asymmetric stabilizer code that can detect $\mathrm{X}^{(p^m)}(\cdot)$ errors affecting at most $(d_x - 1)$ qudits and detect $\mathrm{Z}^{(p^m)}(\cdot)$ errors affecting at most $(d_z - 1)$ qudits is represented by $((n, p^{mn-\rho}, d_z/d_x))_{p^m}$. The code can correct $\mathrm{X}^{(p^m)}(\cdot)$ errors affecting at most $\lfloor(d_x - 1)/2\rfloor$ qudits and correct $\mathrm{Z}^{(p^m)}(\cdot)$ errors affecting at most $\lfloor(d_z - 1)/2\rfloor$ qudits.

Let $S_i \equiv [[x_{ij}]_{j=1}^n|[z_{ij}]_{j=1}^n]_{p^m}$ be the field isomorphic equivalent of the minimal stabilizer generator S_i, where $i \in \{1, \ldots, \rho\}$. The *check matrix* $\mathcal{H}_S$ of $\mathcal{Q}_S$ is obtained by stacking these field isomorphic equivalents of S_is as follows:

$$\mathcal{H}_S = [\mathcal{H}_\mathrm{X}|\mathcal{H}_\mathrm{Z}]_{p^m} \tag{7}$$

where $\mathcal{H}_\mathrm{X} = [x_{ij}]$ and $\mathcal{H}_\mathrm{Z} = [z_{ij}]$ with $i \in \{1, \ldots, \rho\}$ and $j \in \{1, \ldots, n\}$.

The commutativity relation between two operators $O_1 \equiv [\boldsymbol{\nu}|\boldsymbol{\chi}]$ and $O_2 \equiv [\boldsymbol{\varepsilon}|\boldsymbol{\zeta}]$, where $\boldsymbol{\nu}, \boldsymbol{\chi}, \boldsymbol{\varepsilon}, \boldsymbol{\zeta} \in \mathbb{F}_{p^m}^n$, is $O_1O_2 = \omega^{\mathrm{Symp}(O_1,O_2)}O_2O_1$, where $\mathrm{Symp}(O_1, O_2)$ is the symplectic product of O_1 and O_2, given by

$$\mathrm{Symp}(O_1, O_2) = \mathrm{symp}([\boldsymbol{\nu}|\boldsymbol{\chi}], [\boldsymbol{\varepsilon}|\boldsymbol{\zeta}]) = \mathrm{Tr}_{p^m/p}(\boldsymbol{\chi}\boldsymbol{\varepsilon}^\mathrm{T} - \boldsymbol{\nu}\boldsymbol{\zeta}^\mathrm{T}). \tag{8}$$

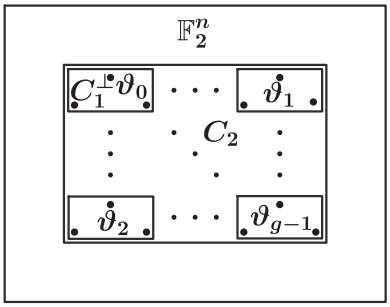

FIG. 1. Dual of code $C_1[n, k_1, d_1]$ is a subset of the code $C_2[n, k_2, d_2]$. We note that $|C_1^\perp| = 2^{(n-k_1)}$ and $|C_2| = 2^{k_2}$. This leads to the formation of g cosets of $C_1^\perp$ in C_2, where $g = 2^{(k_1+k_2-n)}$. The cosets are labeled as $\vartheta_0, \vartheta_1, \ldots, \vartheta_{g-1}$. The dots inside the cosets represent their elements.

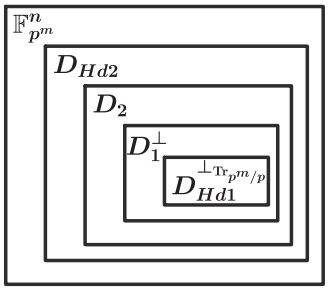

FIG. 2. Containment of various subspaces of $\mathbb{F}_{p^m}$ related to H_{d1} and H_{d2}. Cosets of each subspace can be formed in a larger subspace of $\mathbb{F}_{p^m}$ within which it is contained.

C. CSS CODES OVER QUBITS

CSS proposed the construction of an $[[n, k_1 + k_2 - n, d_z/d_x]]_2$ quantum code $\mathcal{Q}_{\mathrm{CSS}}$ over qubits ($q = 2$) from two binary classical codes $C_1[n, k_1, d_1]$ and $C_2[n, k_2, d_2]$ that satisfy $C_1^\perp \subset C_2$, where $d_z \geq d_1$ and $d_x \geq d_2$ [3], [4]. The dual containment property $C_1^\perp \subset C_2$ is a result of the abelian restriction on the stabilizer group S.

Let H_1 and H_2 be the parity check matrices of the classical codes C_1 and C_2, respectively. Then, the check matrix of the CSS code [5] is

$$\mathcal{H} = \left[\begin{array}{c|c} H_1 & \mathbf{0} \\ \mathbf{0} & H_2 \end{array}\right]. \tag{9}$$

As $C_1^\perp \subset C_2$, cosets of $C_1^\perp$ are formed in C_2, as shown in Fig. 1. The basis codewords of the CSS code $\mathcal{Q}$ are the normalized superposition of all the elements in a particular coset of $C_1^\perp$ in C_2. As $C_1^\perp$ has $2^{(n-k_1)}$ elements and C_2 has 2^{k_2} elements, we obtain C_2 to contain $(2^{k_2})/(2^{(n-k_1)}) = 2^{(k_1+k_2-n)}$ cosets of $C_1^\perp$. As each coset corresponds to a basis codeword, $\mathcal{Q}$ has a dimension of $2^{(k_1+k_2-n)}$.

Let $\vartheta_0, \vartheta_1, \ldots, \vartheta_{g-1}$ be the cosets of $C_1^\perp$ in C_2, where $g = 2^{(k_1+k_2-n)}$. Let $\boldsymbol{w_0}, \ldots, \boldsymbol{w_{g-1}}$ be the coset representatives of the cosets $\vartheta_0, \ldots, \vartheta_{g-1}$. The basis codeword of the CSS code corresponding to the coset ϑ_i ($i \in \{0, 1, \ldots, g-1\}$) is

$$|\psi_i\rangle = \frac{1}{2^{((n-k_1)/2)}} \sum_{\boldsymbol{l} \in C_1^\perp} |\boldsymbol{l} + \boldsymbol{w_i}\rangle. \tag{10}$$

III. GENERALIZATION OF CSS CODES TO QUDITS

The CSS codes over qubits were defined in two ways: 1) based on the check matrix in (9); and 2) based on the codewords obtained from the coset formation in (10). The quantum codes obtained from both these definitions are the same for qubits. However, in this section, we show that we obtain two different codes when we construct quantum codes based on these two definitions for qudits of dimension $q = p^m$ and we study their properties.

Let us consider two classical linear codes $D_1[n, k_1, d_1]$ and $D_2[n, k_2, d_2]$ over $\mathbb{F}_{p^m}$ with parity check matrices H_{d1} and H_{d2}, respectively, where $D_1^\perp \subset D_2$. Let $\rho_1 = n - k_1$ and $\rho_2 = n - k_2$. Let $\mathcal{T}$ be a transformation on a matrix $A = [a_{ij}]$, where $a_{ij} \in \mathbb{F}_{p^m}$, that transforms A to the matrix $\mathcal{T}(A) = [\mathrm{Tr}_{p^m/p}(a_{ij})]$.

We define the trace inner product of vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ as $\mathrm{Tr}_{p^m/r}(\boldsymbol{a}\boldsymbol{b}^{\mathrm{T}})$, where $\mathbb{F}_r$ is a subfield of $\mathbb{F}_{p^m}$. The Euclidean or the standard inner product of $\boldsymbol{a}$ and $\boldsymbol{b}$ is $\boldsymbol{a}\boldsymbol{b}^{\mathrm{T}}$. $D_1^{\perp_{\mathrm{Tr}_{p^m/r}}}$ is the dual of D_1 with respect to the trace inner product.

We define the following two spaces based on H_{d1} and H_{d2}.

1) D_{Hd2} is defined to be the set of all vectors $\boldsymbol{v}$ in $\mathbb{F}_{p^m}^n$ such that $\mathcal{T}(H_{d2}\boldsymbol{v}^{\mathrm{T}}) = \mathbf{0}$.
2) $D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}$ is defined to be the set of all vectors $\boldsymbol{w}$ in $\mathbb{F}_{p^m}^n$ that are obtained by adding the rows of H_{d1}. Let D_{Hd1} be the set of all vectors $\boldsymbol{v}$ in $\mathbb{F}_{p^m}^n$ such that $\mathcal{T}(H_{d1}\boldsymbol{v}^{\mathrm{T}}) = \mathbf{0}$. We note that $D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}$ is the dual space of D_{Hd1} with respect to the trace inner product.

We note that D_{Hd1} and D_{Hd2} are $\mathbb{F}_p$-linear codes over $\mathbb{F}_{p^m}$. For a vector $\boldsymbol{c} \in D_2$, $H_{d2}\boldsymbol{c}^{\mathrm{T}} = \mathbf{0}$; hence, $\mathcal{T}(H_{d2}\boldsymbol{c}^{\mathrm{T}}) = \mathbf{0}$ and $\boldsymbol{c} \in D_{Hd2} \Rightarrow D_2 \subset D_{Hd2}$. As the set $D_1^\perp$ is obtained by considering the linear combination of the rows of H_{d1}, the set $D_1^\perp$ also contains the sum of the rows of H_{d1}. Thus, $D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}} \subset D_1^\perp$. As $D_1^\perp \subset D_2$, we obtain

$$D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}} \subset D_1^\perp \subset D_2 \subset D_{Hd2} \tag{11}$$

as shown in Fig. 2 . Using the two definitions of CSS codes over qubits, we construct the following quantum codes from D_1 and D_2.

1) *Construction based on the cosets of $\boldsymbol{D_1^\perp}$ in $\boldsymbol{D_2}$*: The codewords of this quantum code are obtained by considering a normalized superposition of all the elements of a particular coset of $D_1^\perp$ in D_2. We call this code as the $\mathbb{F}_{p^m}$-linear CSS code, or simply the CSS code over qudits as it is an $[[n, k_1 + k_2 - n, d_z \geq d_1/d_x \geq d_2]]$-quantum code, similar to the CSS code over qubits. However, the check matrix of this quantum code, which is later provided in this section in Theorem 1, is different from the check matrix of the CSS code

over qubits in (9). We discuss this code in detail in Section III-A.

2) *Construction based on the check matrix using $\boldsymbol{H_{d1}}$ and $\boldsymbol{H_{d2}}$*: The quantum code is obtained by considering the following check matrix:

$$\mathcal{H}_{\text{pCSS}} = \left[\begin{array}{c|c} H_{d1} & \mathbf{0} \\ \mathbf{0} & H_{d2} \end{array}\right]. \tag{12}$$

We call this code as the $\mathbb{F}_p$-linear CSS code over qudits as its check matrix is similar to the check matrix of the CSS code over qubits and is based on the $\mathbb{F}_p$-linear codes D_{Hd1} and D_{Hd2}. The $\mathbb{F}_{p^m}$-linear CSS code is a subset of the $\mathbb{F}_p$-linear CSS code. The $\mathbb{F}_p$-linear CSS code is an $((n, p^{((m-2)n+k_1+k_2)}, d_z \geq y_1/d_x \geq y_2)))$ code, where y_1 and y_2 are minimum distances of D_{Hd1} and D_{Hd2}, respectively. The basis codewords of this code are obtained as a normalized superposition of the elements of a particular coset of $D_{Hd1}^{\perp_{\text{Tr}_{p^m/p}}}$ in D_{Hd2}. We discuss this code in detail in Section III-B.

We note that when the dimension of the qudit is a prime, i.e., $m=1 \Rightarrow p^m = p$, $\mathbb{F}_{p^m}$-linear CSS codes and $\mathbb{F}_p$-linear CSS codes are the same.

From Fig. 2, it is evident that the $\mathbb{F}_p$-linear CSS code has a larger dimension compared to the $\mathbb{F}_{p^m}$-linear CSS code obtained from H_{d1} and H_{d2} as the number of cosets of $D_{Hd1}^{\perp_{\text{Tr}_{p^m/p}}}$ in D_{Hd2} is larger compared to the number of cosets of $D_1^{\perp}$ in D_2 as $D_{Hd1}^{\perp_{\text{Tr}_{p^m/p}}} \subset D_1^{\perp} \subset D_2 \subset D_{Hd2}$. Later in this section, in Theorem 3, we show that the minimum distance of the $\mathbb{F}_p$-linear CSS code is lesser than or equal to the minimum distance of the $\mathbb{F}_{p^m}$-linear CSS code.

The choice between the $\mathbb{F}_{p^m}$-linear CSS code and the $\mathbb{F}_p$-linear CSS code is application based as follows.

1) When the application needs better error detection and correction capability over better coding rate, the $\mathbb{F}_{p^m}$-linear CSS code should be used as ferror detection and correction capability depends on the code's minimum distance.
2) When the application needs higher coding rate over better error detection and correction capability, the $\mathbb{F}_p$-linear CSS code should be used as the coding rate depends on the code dimension.[2]

The $\mathbb{F}_{p^m}$-linear CSS code is widely referred to as the CSS code in prior literature [10], [12]. We next discuss the structure and properties of the $\mathbb{F}_{p^m}$-linear CSS code and the $\mathbb{F}_p$-linear CSS code over qudits in detail.

A. $\mathbb{F}_{p^m}$-LINEAR CSS CODE OVER QUDITS

The $\mathbb{F}_{p^m}$-linear CSS code over qudits is obtained from the classical codes D_1 and D_2 by using the coset-based approach for obtaining the basis codewords.

[2]The number of physical qudits in both the codes are the same.

1) COSET-BASED CONSTRUCTION OF THE $\mathbb{F}_{p^m}$-LINEAR CSS CODE

As $D_1^{\perp}$ is a subset of D_2, there exist cosets of $D_1^{\perp}$ in D_2. The size of $D_1^{\perp}$ and D_2 are $p^{m\rho_1}$ and p^{mk_2}, respectively; hence, the number of cosets of $D_1^{\perp}$ in D_2 is $s = (p^{mk_2}/p^{k\rho_1}) = p^{m(k_2-\rho_1)} = p^{m(k_1+k_2-n)}$. Thus, the dimension of the quantum code obtained is $(p^m)^{(k_1+k_2-n)}$, similar to the CSS code over qubits whose dimension is $2^{(k_1+k_2-n)}$.

Let $\tau_0, \tau_1, \ldots, \tau_{s-1}$ be the s cosets of $D_1^{\perp}$ in D_2. Let $\boldsymbol{t_0}$, $\boldsymbol{t_1}, \ldots, \boldsymbol{t_{s-1}}$ be the coset representatives of $\tau_0, \tau_1, \ldots, \tau_{s-1}$, respectively. The basis codeword $|\psi_i^{(p^m)}\rangle$ ($i \in \{0, 1, \ldots, s-1\}$) of the $\mathbb{F}_{p^m}$-linear CSS code over qudits obtained from the coset τ_i is

$$|\psi_i^{(p^m)}\rangle = \frac{1}{p^{(m\rho_1/2)}} \sum_{\boldsymbol{l} \in D_1^{\perp}} |\boldsymbol{l} + \boldsymbol{t_i}\rangle. \tag{13}$$

As the $\mathbb{F}_{p^m}$-linear CSS codes are obtained from the cosets of the classical linear code $D_1^{\perp}$ in the classical linear code D_2, the $\mathbb{F}_{p^m}$-linear CSS codes can also be called linear CSS codes.

2) CHECK MATRIX OF THE $\mathbb{F}_{p^m}$-LINEAR CSS CODE

We next provide the check matrix of the $\mathbb{F}_{p^m}$-linear CSS code over qudits.

We first show that the set of equations $\{\text{Tr}_{p^m/p}(\alpha^i\beta) = 0\}_{i=0}^{m-1}$ are satisfied for $\beta \in \mathbb{F}_{p^m}$ if and only if $\beta = 0$. This result is helpful towards obtaining the check matrix and the minimum distance of the $\mathbb{F}_{p^m}$-linear CSS code.

Lemma 1: For $\beta \in \mathbb{F}_{p^m}$, $\text{Tr}_{p^m/p}(\alpha^i\beta) = 0 \quad \forall i \in \{0, 1, \ldots, m-1\}$ if and only if $\beta = 0$ [20].

The proof of Lemma 1 is provided in the Appendix. Using Lemma 1, we obtain the check matrix of the $\mathbb{F}_{p^m}$-linear CSS code.

Theorem 1: The check matrix for the $\mathbb{F}_{p^m}$-linear CSS code obtained from D_1 and D_2, whose basis codewords are provided in (13), is given by

$$\mathcal{H}_{\text{CSS}} = \left[\begin{array}{c|c} H_{d1} & \\ \alpha H_{d1} & \\ \vdots & \mathbf{0} \\ \alpha^{m-1} H_{d1} & \\ & H_{d2} \\ & \alpha H_{d2} \\ \mathbf{0} & \vdots \\ & \alpha^{m-1} H_{d2} \end{array}\right] \tag{14}$$

where α is the primitive element of $\mathbb{F}_{p^m}$ [20].

Proof: The dimension of the $\mathbb{F}_{p^m}$-linear CSS code is $p^{m(k_1+k_2-n)}$. The $\mathbb{F}_{p^m}$-linear CSS code over qudits whose codewords are given in (13) has $m(n-k_1) + m(n-k_2)$ minimal stabilizer generators as a stabilizer code of dimension $p^{mn-\rho}$ has ρ minimal stabilizer generators. Thus, the check matrix of the $\mathbb{F}_{p^m}$-linear CSS code comprises of $m(n-k_1) + m(n-k_2)$ minimal stabilizer generators.

For $l \in \{1, \ldots, m(n-k_1)+m(n-k_2)\}$, the minimal stabilizer generators are of the form $S_l = \bigotimes_{j=1}^{n} \mathrm{X}^{(p^m)}(\beta_j)\mathrm{Z}^{(p^m)}(\gamma_j)$ as they belong to $\mathcal{G}_{p^m}^{\otimes n}$, where $\beta_j, \gamma_j \in \mathbb{F}_{p^m}$. Let $\boldsymbol{\beta} = [\beta_j]_{j=1}^n$ and $\boldsymbol{\gamma} = [\gamma_j]_{j=1}^n$. As $S_l|\psi_i^{(p^m)}\rangle = |\psi_i^{(p^m)}\rangle$ for all codewords $\{|\psi_i^{(p^m)}\rangle\}_{i=0}^{(s-1)}$ provided in (13), we have

$$\begin{aligned}
&S_l|\psi_i^{(p^m)}\rangle = |\psi_i^{(p^m)}\rangle \\
&\Rightarrow \left(\bigotimes_{j=1}^{n} \mathrm{X}^{(p^m)}(\beta_j)\mathrm{Z}^{(p^m)}(\gamma_j)\right) \frac{1}{p^{(m\rho_1/2)}} \sum_{\boldsymbol{l_1}\in D_1^{\perp}} |\boldsymbol{l_1}+\boldsymbol{t_i}\rangle \\
&\quad = \frac{1}{p^{(m\rho_1/2)}} \sum_{\boldsymbol{l_2}\in D_1^{\perp}} |\boldsymbol{l_2}+\boldsymbol{t_i}\rangle \\
&\Rightarrow \left(\bigotimes_{j=1}^{n} \mathrm{X}^{(p^m)}(\beta_j)\right)\left(\bigotimes_{y=1}^{n} \mathrm{Z}^{(p^m)}(\gamma_y)\right) \sum_{\boldsymbol{l_1}\in D_1^{\perp}} |\boldsymbol{l_1}+\boldsymbol{t_i}\rangle \\
&\quad = \sum_{\boldsymbol{l_2}\in D_1^{\perp}} |\boldsymbol{l_2}+\boldsymbol{t_i}\rangle \\
&\Rightarrow \left(\bigotimes_{j=1}^{n} \mathrm{X}^{(p^m)}(\beta_j)\right) \sum_{\boldsymbol{l_1}\in D_1^{\perp}} \omega^{\mathrm{Tr}_{p^m/p}((\boldsymbol{l_1}+\boldsymbol{t_i})\boldsymbol{\gamma}^{\mathrm{T}})} |\boldsymbol{l_1}+\boldsymbol{t_i}\rangle \\
&\quad = \sum_{\boldsymbol{l_2}\in D_1^{\perp}} |\boldsymbol{l_2}+\boldsymbol{t_i}\rangle \\
&\Rightarrow \sum_{\boldsymbol{l_1}\in D_1^{\perp}} \omega^{\mathrm{Tr}_{p^m/p}((\boldsymbol{l_1}+\boldsymbol{t_i})\boldsymbol{\gamma}^{\mathrm{T}})} |\boldsymbol{l_1}+\boldsymbol{t_i}+\boldsymbol{\beta}\rangle = \sum_{\boldsymbol{l_2}\in D_1^{\perp}} |\boldsymbol{l_2}+\boldsymbol{t_i}\rangle. \qquad (15)
\end{aligned}$$

As no term in the summation on the right-hand side of (15) has a phase, we obtain $\omega^{\mathrm{Tr}_{p^m/p}((\boldsymbol{l_1}+\boldsymbol{t_i})\boldsymbol{\gamma}^{\mathrm{T}})} = 1$ for all $\boldsymbol{l_1} \in D_1^{\perp}$ and $i \in \{0, \ldots, s-1\}$. Thus, for $\boldsymbol{l_1} \in D_1^{\perp}$ and $i \in \{0, \ldots, s-1\}$, we obtain $\mathrm{Tr}_{p^m/p}((\boldsymbol{l_1}+\boldsymbol{t_i})\boldsymbol{\gamma}^{\mathrm{T}}) = 0$. As $\boldsymbol{l_1}, \boldsymbol{t_i} \in D_2$, we note that $(\boldsymbol{l_1}+\boldsymbol{t_i}) \in D_2$ and $D_2 = \{\boldsymbol{l_1}+\boldsymbol{t_i} | \boldsymbol{l_1} \in D_1^{\perp}, i \in \{0, 1, \ldots, s-1\}\}$.

Considering $\boldsymbol{\mu} = \boldsymbol{l_1}+\boldsymbol{t_i}$, we obtain that $\mathrm{Tr}_{p^m/p}(\boldsymbol{\mu}\boldsymbol{\gamma}^{\mathrm{T}}) = 0$ $\forall \boldsymbol{\mu} \in D_2$. As $\alpha^y\boldsymbol{\mu} \in D_2$ $\forall$ $y \in \{0, 1, \ldots, m-1\}$, $\mathrm{Tr}_{p^m/p}(\alpha^y\boldsymbol{\mu}\boldsymbol{\gamma}^{\mathrm{T}}) = 0$. From Lemma 1, $\boldsymbol{\mu}\boldsymbol{\gamma}^{\mathrm{T}} = 0$ $\forall \boldsymbol{\mu} \in D_2$. Thus, $\boldsymbol{\gamma}$ can be any element of $D_2^{\perp}$, including $\mathbf{0}$. We note that $D_2^{\perp}$ can be written as a sum of the rows of $H_{d2}, \alpha H_{d2}, \ldots, \alpha^{(m-1)}H_{d2}$.

From (15), equating the quantum states in the superposition, we obtain

$$\begin{aligned}
&|\boldsymbol{l_1}+\boldsymbol{t_i}+\boldsymbol{\beta}\rangle = |\boldsymbol{l_2}+\boldsymbol{t_i}\rangle \Rightarrow \boldsymbol{l_1}+\boldsymbol{t_i}+\boldsymbol{\beta} = \boldsymbol{l_2}+\boldsymbol{t_i} \\
&\Rightarrow \boldsymbol{\beta} = \boldsymbol{l_2}-\boldsymbol{l_1} \Rightarrow \boldsymbol{\beta} \in D_1^{\perp} (\because \boldsymbol{l_1}, \boldsymbol{l_2} \in D_1^{\perp}). \qquad (16)
\end{aligned}$$

We note that $D_1^{\perp}$ can be written as a sum of the rows of $H_{d1}, \alpha H_{d1}, \ldots, \alpha^{(m-1)}H_{d1}$. Also, $\boldsymbol{\beta}$ can be $\mathbf{0}$ as $\mathbf{0} \in D_1^{\perp}$.

As the values of $\boldsymbol{\beta}$ and $\boldsymbol{\gamma}$ are independent of each other, the minimal stabilizer generators are of the form $[\boldsymbol{\beta}|\mathbf{0}]$ and $[\mathbf{0}|\boldsymbol{\gamma}]$, where $\boldsymbol{\beta} \in D_1^{\perp}$ and $\boldsymbol{\gamma} \in D_2^{\perp}$. As the elements of $D_1^{\perp}$ and $D_2^{\perp}$ can be written as a sum of the rows of $H_{d1}, \alpha H_{d1}, \ldots, \alpha^{(m-1)}H_{d1}$, and $H_{d2}, \alpha H_{d2}, \ldots, \alpha^{(m-1)}H_{d2}$, respectively, the result follows. ■

We note that qudit stabilizer codes are analogous to classical additive codes, *not* classical linear codes. In classical additive codes, a codeword scaled by α or its powers need not be another codeword. As $\mathbb{F}_{p^m}$-linear CSS codes over qudits are based on $\mathbb{F}_{p^m}$-linear codes, it is important to consider the matrices $\alpha H_{d_i}, \ldots, \alpha^{m-1}H_{d_i}$ in the check matrix of the $\mathbb{F}_{p^m}$-linear CSS code, for $i = 1, 2$.

Remark 1: We note that the check matrix plays an important role in obtaining the encoding operator as shown in [8]. It is also necessary to design the error correction circuit that contains the syndrome computation circuit that is based on the minimal stabilizer generator or check matrix of the code.

3) ERROR DETECTION AND CORRECTION CAPABILITY OF THE $\mathbb{F}_{p^m}$-LINEAR CSS CODE

We recall that the error detection and correction capability of an asymmetric stabilizer code depends on the distances d_x and d_z. Let d_{cx} and d_{cz} be the X-distance d_x and Z-distance d_z for the $\mathbb{F}_{p^m}$-linear CSS code. Using the proposed check matrix, we next show that d_{cz} and d_{cx} of the $\mathbb{F}_{p^m}$-linear CSS code are at least d_1 and d_2, respectively.

Let $\mathrm{wt}_{\mathrm{X}}(B)$ and $\mathrm{wt}_{\mathrm{Z}}(B)$ be the weight of the $\mathrm{X}^{(p^m)}(\cdot)$ and $\mathrm{Z}^{(p^m)}(\cdot)$ operators in an operator $B \in \mathcal{G}_{p^m}^{\otimes n}$, respectively. An asymmetric stabilizer code is called a *nondegenerate*,[3] code if there does not exist an element B in the stabilizer group S with $\mathrm{wt}_{\mathrm{X}}(B) < d_{cx}$ and $\mathrm{wt}_{\mathrm{Z}}(B) < d_{cz}$; else, it is called a *degenerate* code [2], [6]. A $\mathbb{F}_{p^m}$-linear CSS code can detect $(d_{cx}-1)$ $\mathrm{X}^{(p^m)}(\cdot)$ errors and $(d_{cz}-1)$ $\mathrm{Z}^{(p^m)}(\cdot)$ errors and correct $\lfloor (d_{cx}-1)/2 \rfloor$ $\mathrm{X}^{(p^m)}(\cdot)$ errors and $\lfloor (d_{cz}-1)/2 \rfloor$ $\mathrm{Z}^{(p^m)}(\cdot)$ errors.

Using Lemma 1, we next obtain the minimum distance of the $\mathbb{F}_{p^m}$-linear CSS code over qudits in Theorem 2.

Theorem 2: Let D_1 and D_2 be two classical codes over $\mathbb{F}_{p^m}$ with parity check matrices H_{d1} and H_{d2}, and minimum distances d_1 and d_2, respectively. The X-distance d_{cx} and Z-distance d_{cz} of the $\mathbb{F}_{p^m}$-linear CSS code over qudits based on D_1 and D_2 corresponding to the check matrix $\mathcal{H}_{\mathrm{CSS}}$ satisfy $d_{cz} \geq d_1$ and $d_{cx} \geq d_2$ and saturate the inequalities if and only if the $\mathbb{F}_{p^m}$-linear CSS code is a nondegenerate code.

Proof: The distances d_{cz} and d_{cx} are obtained as the minimum of the weight of the $\mathrm{X}^{(p^m)}(\cdot)$ and $\mathrm{Z}^{(p^m)}(\cdot)$ operators in $\mathcal{N}_S \setminus S$, respectively. We note that the error detection or correction capability of the code for $\mathrm{X}^{(p^m)}(\cdot)$ errors depends on the $\mathrm{Z}^{(p^m)}$ stabilizer generators and for $\mathrm{Z}^{(p^m)}(\cdot)$ errors depends on the $\mathrm{X}^{(p^m)}$ stabilizer generators.

Let $N \equiv [\boldsymbol{h_x}|\boldsymbol{h_z}]$ be an element in $\mathcal{N}_S$, then its symplectic product with each minimal stabilizer generator is 0. Using

[3] In [6], the term "pure codes" are used for nondegenerate codes.

the definition of the symplectic product in (8), we obtain

$$\mathcal{T}\left(\mathcal{H}_{\mathrm{CSS}}\left[\begin{array}{c}\boldsymbol{h_z}^{\mathrm{T}}\\ \hline \boldsymbol{h_x}^{\mathrm{T}}\end{array}\right]\right)=\mathbf{0}$$

$$\Rightarrow \mathcal{T}\left(\left[\begin{array}{c|c} H_{d1} & \\ \alpha H_{d1} & \\ \vdots & \mathbf{0} \\ \alpha^{m-1}H_{d1} & \\ & H_{d2} \\ \mathbf{0} & \alpha H_{d2} \\ & \vdots \\ & \alpha^{m-1}H_{d2}\end{array}\right]\left[\begin{array}{c}\boldsymbol{h_z}^{\mathrm{T}}\\ \hline \boldsymbol{h_x}^{\mathrm{T}}\end{array}\right]\right)=\mathbf{0}$$

$$\Rightarrow \mathcal{T}\left(\left[\begin{array}{c} H_{d1}\boldsymbol{h_z}^{\mathrm{T}} \\ \alpha H_{d1}\boldsymbol{h_z}^{\mathrm{T}} \\ \vdots \\ \alpha^{m-1}H_{d1}\boldsymbol{h_z}^{\mathrm{T}} \\ \hline H_{d2}\boldsymbol{h_x}^{\mathrm{T}} \\ \alpha H_{d2}\boldsymbol{h_x}^{\mathrm{T}} \\ \vdots \\ \alpha^{m-1}H_{d2}\boldsymbol{h_x}^{\mathrm{T}}\end{array}\right]\right)=\mathbf{0}$$

$$\Rightarrow \mathcal{T}(\alpha^y H_{d1}\boldsymbol{h_z}^{\mathrm{T}})=\mathbf{0} \text{ and } \mathcal{T}(\alpha^y H_{d2}\boldsymbol{h_x}^{\mathrm{T}})=\mathbf{0} \tag{17}$$

for all $y \in \{0, 1, \ldots, m-1\}$. From Lemma 1, $H_{d1}\boldsymbol{h_z}^{\mathrm{T}} = \mathbf{0}$ and $H_{d2}\boldsymbol{h_x}^{\mathrm{T}} = \mathbf{0}$. Thus, $\boldsymbol{h_z} \in D_1$ and $\boldsymbol{h_x} \in D_2$.

As the minimum distance of the quantum code is based on the weight of nonidentity operators in $\mathcal{N}_S \setminus S$, let us consider N to be a nonidentity operator. As $\boldsymbol{h_z} \in D_1$ and $\boldsymbol{h_x} \in D_2$, the Hamming weights of $\boldsymbol{h_z}$ and $\boldsymbol{h_x}$ are at least d_1 and d_2, respectively. Based on the definition of the weight of an operator in Section II-B, the weight of $N = [\boldsymbol{h_x}|\boldsymbol{h_z}]$ is greater than or equal to the $\mathrm{wt}(\boldsymbol{h_x})$ and $\mathrm{wt}(\boldsymbol{h_z})$, i.e., $\mathrm{wt}(N) \geq \max(\mathrm{wt}(\boldsymbol{h_x}), \mathrm{wt}(\boldsymbol{h_z}))$.

When N is not the identity operator, either $\boldsymbol{h_x}$ or $\boldsymbol{h_z}$ must be nonzero. If $\boldsymbol{h_x} \neq \mathbf{0}$ and $\boldsymbol{h_z} = \mathbf{0}$, then $\mathrm{wt}(N) = \mathrm{wt}(\boldsymbol{h_x})$ as $N = [\boldsymbol{h_x}|\mathbf{0}] \Rightarrow \mathrm{wt}(N) \geq \max(\mathrm{wt}(\boldsymbol{h_x}), \mathrm{wt}(\mathbf{0})) = \max(\mathrm{wt}(\boldsymbol{h_x}), 0) = \mathrm{wt}(\boldsymbol{h_x})$. Similarly, for $N = [\mathbf{0}|\boldsymbol{h_z}]$, we obtain $\mathrm{wt}(N) \geq \mathrm{wt}(\boldsymbol{h_z})$. For nonzero $\boldsymbol{h_x}$ and $\boldsymbol{h_z}$, as $\boldsymbol{h_z} \in D_1$, $\boldsymbol{h_x} \in D_2$, $\mathrm{wt}(\boldsymbol{h_x}) \geq d_2$, and $\mathrm{wt}(\boldsymbol{h_z}) \geq d_1$, we obtain $\mathrm{wt}(N) \geq \min(d_1, d_2)$, $\mathrm{wt_X}(N) \geq d_2$, and $\mathrm{wt_Z}(N) \geq d_1$, where $N = [\boldsymbol{h_x}|\boldsymbol{h_z}]$.

We next show that there exists an $\mathrm{X}^{(p^m)}(\cdot)$ operator N_x and a $\mathrm{Z}^{(p^m)}(\cdot)$ operator N_z that have weights d_2 and d_1, respectively. When we consider $\boldsymbol{h_x}$ to be the nonzero codeword of D_2 with Hamming weight d_2 and $\boldsymbol{h_z}$ to be zero, the weight of $N_x = [\boldsymbol{h_x}|\mathbf{0}]$ is d_2. Similarly, when we consider $\boldsymbol{h_z}$ to be the nonzero codeword of D_1 with Hamming weight d_1 and $\boldsymbol{h_x}$ to be zero, we obtain the element $N_z = [\mathbf{0}|\boldsymbol{h_z}] \in \mathcal{N}_S$ with weight d_1.

However, the operators N_x and N_z with weights d_2 and d_1 could be stabilizers in $S \subset \mathcal{N}_S$. We recall that the weight of elements of the form $[\boldsymbol{h_x}|0]$ and $[0|\boldsymbol{h_z}]$ in $\mathcal{N}_S$ is greater than or equal to d_2 and d_1, respectively. Thus, as d_{cx} and d_{cz} is obtained from $\mathcal{N}_S \setminus S$, we conclude that $d_{cz} \geq d_1$ and $d_{cx} \geq d_2$.

We next show that the $\mathbb{F}_{p^m}$-linear CSS code is nondegenerate if $d_{cz} = d_1$ and $d_{cx} = d_2$. As $S \subset \mathcal{N}_S$, for every stabilizer $B \in S$, $\mathrm{wt_X}(B) \geq d_2$, and $\mathrm{wt_Z}(B) \geq d_1$. As $d_{cz} = d_1$ and $d_{cx} = d_2$, for each stabilizer B, $\mathrm{wt_X}(B) \geq d_2 = d_{cx}$ and $\mathrm{wt_Z}(B) \geq d_1 = d_{cz}$; hence, the code is a nondegenerate code.

We next show that $d_{cz} = d_1$ and $d_{cx} = d_2$ for a nondegenerate $\mathbb{F}_{p^m}$-linear CSS code over qudits. A nondegenerate code does not contain a stabilizer B with $\mathrm{wt_X}(B) < d_{cx}$ and $\mathrm{wt_Z}(B) < d_{cz}$. Thus, for any stabilizer B, $\mathrm{wt_X}(B) \geq d_{cx}$ and $\mathrm{wt_Z}(B) \geq d_{cz}$. As $d_{cx} \geq d_2$ and $d_{cz} \geq d_1$, $\mathrm{wt_X}(B) \geq d_2$, and $\mathrm{wt_Z}(B) \geq d_1$. Let N be the element in $\mathcal{N}_S$ with $\mathrm{wt_X}(N) = d_2$. N belongs to either S or $\mathcal{N}_S \setminus S$. If $N \in \mathcal{N}_S \setminus S$, then $d_{cx} = d_2$ as $d_{cx} \geq d_2$ and there exists an element of weight d_2 in $\mathcal{N}_S \setminus S$. If $N \in S$, then $\mathrm{wt_X}(N) \geq d_{cx} \Rightarrow d_2 \geq d_{cx}$. As $d_{cx} \geq d_2$, we obtain $d_{cx} = d_2$. Similarly, we obtain $d_{cz} = d_1$. Thus, for a nondegenerate code $d_{cz} = d_1$ and $d_{cx} = d_2$. ■

Similar to Theorem 2, it can be shown that for a symmetric $\mathbb{F}_{p^m}$-linear CSS code, the minimum distance d satisfies $d \geq \min(d_1, d_2)$ and saturates the inequality if and only if the $\mathbb{F}_{p^m}$-linear CSS code is a nondegenerate code.

Remark 2: From the proof of Theorem 2, for an element $N = [\boldsymbol{h_x}|\boldsymbol{h_z}]$, $\boldsymbol{h_x} \in D_2$, and $\boldsymbol{h_z} \in D_1$. We note that if $N \in S$, then $\boldsymbol{h_x}$ is an $\mathbb{F}_p$-linear combination of the rows of the matrices $\alpha^y H_{d1}$s, where $y \in \{0, 1, \ldots, m-1\}$. Thus, $\boldsymbol{h_x} \in D_1^{\perp}$. As d_{cx} is the minimum of the weight of the elements in $\mathcal{N}_S \setminus S$, $d_{cx} = \mathrm{wt_H}(D_2 \setminus D_1^{\perp})$, where $\mathrm{wt_H}(L)$ corresponds to the minimum of the Hamming weight of the elements in the set L. Similarly, $d_{cz} = \mathrm{wt_H}(D_1 \setminus D_2^{\perp})$.

Based on the $\mathbb{F}_{p^m}$-linear CSS code construction over qudits, an $[[n, (k_1 + k_2 - n), d_{cz} \geq d_1/d_{cx} \geq d_2]]_{p^m}$ quantum code is obtained from two classical codes $D_1[n, k_1, d_1]$ and $D_2[n, k_2, d_2]$. We note that the code parameters of this code are same as those of a CSS code over qubits.

We note that the proof of Theorem 2 is based on the proposed check matrix of the $\mathbb{F}_{p^m}$-linear CSS code. In Ketkar *et al.*'s work [10], the result on the minimum distance of the $\mathbb{F}_{p^m}$-linear CSS code does not take into account the degeneracy or nondegeneracy of the code. They provide that the CSS code obtained from codes $C_1[n, k_1, d_1]$ and $C_2[n, k_2, d_2]$ such that $C_2^{\perp} \subset C_1$ is a stabilizer code with minimum distance $d = \min\{\mathrm{wt}(c) | c \in (C_1 \setminus C_2^{\perp}) \cup (C_2 \setminus C_1^{\perp})\}$ with no stabilizers of weight less than $\min(d_1, d_2)$ [10, Lemma 20]. In [6], it has been shown,[4] that the $\mathbb{F}_{p^m}$-linear CSS code is a nondegenerate (pure) code when $d_{cz} = d_1$ and $d_{cx} = d_2$. However, they have not provided the converse, i.e., for every nondegenerate code, $d = \min(d_1, d_2)$, which we establish in this article.

[4] In [6], d_{cz} and d_{cx} are interchanged as they consider $d_{cz} = \mathrm{wt_H}(C_2 \setminus C_1^{\perp})$ and $d_{cx} = \mathrm{wt_H}(C_1 \setminus C_2^{\perp})$. We note that this is equivalent to interchanging the matrices H_{d1} and H_{d2} in the check matrix $\mathcal{H}_{\mathrm{CSS}}$ in Theorem 1.

B. $\mathbb{F}_p$-LINEAR CSS CODES OVER QUDITS

The $\mathbb{F}_p$-linear CSS code over qudits is obtained from the classical codes D_1 and D_2 using the check matrix based approach.

1) CHECK MATRIX BASED CONSTRUCTION OF THE $\mathbb{F}_p$-LINEAR CSS CODE

The $\mathbb{F}_p$-linear CSS code $\mathcal{Q}_{\text{pCSS}}$ is obtained from the classical codes D_1 and D_2 by constructing the check matrix $\mathcal{H}_{\text{pCSS}}$ of the code similar to that of the CSS code over qubits

$$\mathcal{H}_{\text{pCSS}} = \left[\begin{array}{c|c} H_{d1} & \mathbf{0} \\ \mathbf{0} & H_{d2} \end{array}\right]. \tag{18}$$

The rows of the parity check matrices H_{d1} and H_{d2} comprise of the basis of the dual space of D_1 and D_2, respectively. H_{d1} and H_{d2} have ρ_1 and ρ_2 rows, respectively. Thus, the check matrix $\mathcal{H}_{\text{pCSS}}^{(p^m)}$ in (18) corresponds to a stabilizer group S with $(2n-(k_1+k_2))$ minimal stabilizer generators as $\rho = \rho_1 + \rho_2 = (2n-(k_1+k_2))$. Thus, the stabilizer code obtained from the check matrix $\mathcal{H}_{\text{pCSS}}$ in (18) has a dimension of $p^{mn-\rho} = p^{mn-2n+(k_1+k_2)} = p^{(m-2)n+(k_1+k_2)}$.

We note that when $m = 1 \Rightarrow p^m = p$, from Theorem 1 and (18), the check matrices $\mathcal{H}_{\text{pCSS}}$ and $\mathcal{H}_{\text{CSS}}$ are the same. Thus, when $m = 1$, i.e., the dimension of the qudit is prime, the $\mathbb{F}_{p^m}$-linear CSS and the $\mathbb{F}_p$-linear CSS codes are the same.

Remark 3: We note that the minimal stabilizer generators in the check matrix $\mathcal{H}_{\text{pCSS}}$ in (18) are a subset of the minimal stabilizer generators in the check matrix $\mathcal{H}_{\text{CSS}}$ in Theorem 1. Thus, the codewords of the $\mathbb{F}_{p^m}$-linear CSS code over qudits are also stabilized by the minimal stabilizer generators in $\mathcal{H}_{\text{pCSS}}$ in (18). Thus, the $\mathbb{F}_{p^m}$-linear CSS code $\mathcal{Q}_{\text{CSS}}$ corresponding to the check matrix $\mathcal{H}_{\text{CSS}}$ is a subset of the $\mathbb{F}_p$-linear CSS code $\mathcal{Q}_{\text{pCSS}}$ corresponding to the check matrix $\mathcal{H}_{\text{pCSS}}$.

2) ERROR DETECTION AND CORRECTION CAPABILITY OF THE $\mathbb{F}_p$-LINEAR CSS CODE

Let d_{px} and d_{pz} be the X-distance and Z-distance for the $\mathbb{F}_p$-linear CSS code. We provide the relation between the distances d_{px} and d_{pz} and the minimum distances y_1 and y_2 of D_{Hd1} and D_{Hd2}, respectively.

Theorem 3: Let D_1 and D_2 be two classical codes over $\mathbb{F}_{p^m}$ with parity check matrices H_{d1} and H_{d2}, and minimum distances d_1 and d_2, respectively. d_{px} and d_{pz} of the $\mathbb{F}_p$-linear CSS code over qudits based on D_1 and D_2 corresponding to the check matrix $\mathcal{H}_{\text{pCSS}}$ satisfy the following.

1) $d_{px} \geq y_2$ and $d_{pz} \geq y_1$ and saturates the inequality if and only if the $\mathbb{F}_p$-linear CSS code is a nondegenerate code, where y_1 and y_2 are the minimum distances of the D_{Hd1} and D_{Hd2}, respectively.
2) The distances d_{cx} and d_{cz} of the $\mathbb{F}_{p^m}$-linear CSS code are greater than or equal to distances d_{px} and d_{pz} of the $\mathbb{F}_p$-linear CSS code obtained from the classical codes D_1 and D_2.

Proof: d_{px} and d_{pz} are obtained based on the normalizer $\mathcal{N}_S$. Let $[\boldsymbol{h_x}|\boldsymbol{h_z}]$ be an element in $\mathcal{N}_S$, then its symplectic product with each minimal stabilizer generator is 0, i.e.

$$\begin{aligned}
&\mathcal{T}\left(\mathcal{H}_{\text{pCSS}}\left[\begin{array}{c} \boldsymbol{h_z}^{\mathrm{T}} \\ \hline \boldsymbol{h_x}^{\mathrm{T}} \end{array}\right]\right) = \mathbf{0} \\
&\Rightarrow \mathcal{T}\left(\left[\begin{array}{c|c} H_{d1} & \mathbf{0} \\ \mathbf{0} & H_{d2} \end{array}\right]\left[\begin{array}{c} \boldsymbol{h_z}^{\mathrm{T}} \\ \hline \boldsymbol{h_x}^{\mathrm{T}} \end{array}\right]\right) = \mathbf{0} \\
&\Rightarrow \mathcal{T}\left(\left[\begin{array}{c} H_{d1}\boldsymbol{h_z}^{\mathrm{T}} \\ \hline H_{d2}\boldsymbol{h_x}^{\mathrm{T}} \end{array}\right]\right) = \mathbf{0} \\
&\Rightarrow \mathcal{T}(H_{d1}\boldsymbol{h_z}^{\mathrm{T}}) = \mathbf{0} \text{ and } \mathcal{T}(H_{d2}\boldsymbol{h_x}^{\mathrm{T}}) = \mathbf{0}.
\end{aligned} \tag{19}$$

For $\beta \in \mathbb{F}_{p^m}$, we note that $\mathrm{Tr}_{p^m/p}(\beta) = 0$ does not imply that $\beta = 0$. Thus, $\mathcal{T}(H_{d1}\boldsymbol{h_z}^{\mathrm{T}}) = \mathbf{0}$ and $\mathcal{T}(H_{d2}\boldsymbol{h_x}^{\mathrm{T}}) = \mathbf{0}$ does not imply that $\boldsymbol{h_z}$ and $\boldsymbol{h_x}$ belong to D_1 and D_2, respectively, as $H_{d1}\boldsymbol{h_z}^{\mathrm{T}}$ and $H_{d2}\boldsymbol{h_x}^{\mathrm{T}}$ need not be $\mathbf{0}$. Thus, the Hamming weight of $\boldsymbol{h_z}$ and $\boldsymbol{h_x}$ might be lesser than d_1 and d_2, respectively, and is not directly based on the code parameters of D_1 and D_2. We note that $\mathcal{T}(H_{d1}\boldsymbol{h_z}^{\mathrm{T}}) = \mathbf{0}$ and $\mathcal{T}(H_{d2}\boldsymbol{h_x}^{\mathrm{T}}) = \mathbf{0}$ $\Rightarrow \boldsymbol{h_z} \in D_{Hd1}$ and $\boldsymbol{h_x} \in D_{Hd2}$.

Let y_1 and y_2 be the minimum distances of D_{Hd1} and D_{Hd2}, respectively. Then, similar to Theorem 2, d_{px} and d_{pz} of the $\mathbb{F}_p$-linear CSS code over qudits satisfies $d_{px} \geq d_2$ and $d_{pz} \geq d_1$ and saturates the inequalities if and only if the $\mathbb{F}_p$-linear CSS code is a nondegenerate code.

We next show that $d_{cx} \geq d_{px}$ and $d_{cz} \geq d_{pz}$. From Remark 2, we note that $d_{cx} = \mathrm{wt_H}(D_2 \setminus D_1^{\perp})$ and $d_{cz} = \mathrm{wt_H}(D_1 \setminus D_2^{\perp})$. Similar to Remark 2, we obtain $d_{px} = \mathrm{wt_H}(D_{Hd2} \setminus D_{Hd1}^{\perp})$ and $d_{pz} = \mathrm{wt_H}(D_{Hd1} \setminus D_{Hd2}^{\perp})$. As $D_2 \subset D_{Hd2}$ and $D_{Hd1}^{\perp} \subset D_1^{\perp}$, we obtain $D_2 \setminus D_1^{\perp} \subset D_{Hd2} \setminus D_{Hd1}^{\perp}$. Thus, $\mathrm{wt_H}(D_2 \setminus D_1^{\perp}) \geq \mathrm{wt_H}(D_{Hd2} \setminus D_{Hd1}^{\perp})$. Thus, $d_{cx} \geq d_{px}$. Similarly, $d_{cz} \geq d_{pz}$. ■

3) COSET STRUCTURE FOR THE $\mathbb{F}_p$-LINEAR CSS CODE

We next show that the $\mathbb{F}_p$-linear CSS codes are also based on the coset structure, but it is different from the coset structure of the $\mathbb{F}_{p^m}$-linear CSS code over qubits.

D_{Hd2} is the set of all vectors $\boldsymbol{v}$ in $\mathbb{F}_{p^m}^n$ such that $\mathcal{T}(H_{d2}\boldsymbol{v}^{\mathrm{T}}) = \mathbf{0}$. As the dimension of $\mathbb{F}_{p^m}^n$ is mn and $\mathcal{T}(H_{d2}\boldsymbol{v}^{\mathrm{T}}) = \mathbf{0}$ corresponds to ρ_2 constraints, the dimension of D_{Hd2} is $(mn - \rho_2)$. Thus, the size of D_{Hd2} is

$$|D_{Hd2}| = p^{(mn-\rho_2)} = p^{((m-1)n+k_2)}. \tag{20}$$

Let $D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}$ be the set of all vectors $\boldsymbol{w}$ in $\mathbb{F}_{p^m}^n$ that can be obtained as the sum of rows of H_{d1}. We note that each row in $\mathbb{F}_{p^m}^n$ can be added to itself a max of $(p-1)$ times as p is equivalent to 0 in $\mathbb{F}_{p^m}$. If $\boldsymbol{h_1}, \boldsymbol{h_2}, \ldots, \boldsymbol{h_{\rho_1}}$ are the ρ_1 rows of H_{d1}, then the elements in $D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}$ have the

form $a_0\boldsymbol{h_1} + a_1\boldsymbol{h_2} + \cdots + a_{\rho_1}\boldsymbol{h_{\rho_1}}$, where $a_0, a_1, \ldots, a_{\rho_1} \in \mathbb{F}_p$. Thus, $D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}$ contains p^{ρ_1} elements

$$|D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}| = p^{\rho_1}. \tag{21}$$

From (11), as $D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}} \subset D_{Hd2}$, there exist cosets of $D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}$ in D_{Hd2}. From each of these cosets of $D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}$ in D_{Hd2}, we obtain a basis codeword of the $\mathbb{F}_p$-linear CSS code as the normalized superposition of all the elements in that coset. From (20) and (21), the size of D_{Hd2} and $D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}$ are $p^{(m-1)n+k_2}$ and p^{ρ_1}, respectively; hence, there are $p^{((m-2)n+k_1+k_2)}$ cosets of $D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}$ in D_{Hd2} as $(p^{(m-1)n+k_2})/(p^{\rho_1}) = p^{(m-1)n+k_2-(n-k_1)} = p^{(m-2)n+k_1+k_2}$. We note that the number of cosets is equal to the dimension of the $\mathbb{F}_p$-linear CSS code.

Let $\xi_0, \xi_1, \ldots, \xi_{y-1}$ be the y cosets of $D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}$ in D_{Hd2}, where $y = p^{(m-2)n+k_1+k_2}$. Let $\boldsymbol{u_0}, \boldsymbol{u_1}, \ldots, \boldsymbol{u_{y-1}}$ be the coset representatives of $\xi_0, \xi_1, \ldots, \xi_{y-1}$, respectively. The basis codeword of the $\mathbb{F}_p$-linear CSS code corresponding to the coset ξ_i ($i \in \{0, 1, \ldots, y-1\}$) is

$$|\psi_i'\rangle = \frac{1}{p^{(\rho_1/2)}} \sum_{\boldsymbol{l} \in D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}} |\boldsymbol{l} + \boldsymbol{u_i}\rangle. \tag{22}$$

We next show that the quantum state in (22) is stabilized by the minimal stabilizer generators corresponding to $\mathcal{H}_{\mathrm{pCSS}}$ in (18).

Let the rth row of H_{d1} be $\boldsymbol{h_r} = [h_{rj}]_{j=1}^n$ ($r \in \{1, 2, \ldots, \rho_1\}$), then the minimal stabilizer generators corresponding to $[\boldsymbol{h_r}|\boldsymbol{0}]$ in $\mathcal{H}_{\mathrm{pCSS}}$ is $S_r = \mathrm{X}^{(p^m)}(h_{r1}) \otimes \cdots \otimes \mathrm{X}^{(p^m)}(h_{rn})$. S_r stabilizes $|\psi_i'\rangle$ in (22) as follows:

$$\begin{aligned} S_r|\psi_i'\rangle &= (\mathrm{X}^{(p^m)}(h_{r1}) \otimes \cdots \otimes \mathrm{X}^{(p^m)}(h_{rn}))|\psi_i'\rangle \\ &= \frac{1}{\sqrt{p^{\rho_1}}} \sum_{\boldsymbol{l} \in D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}} \mathrm{X}^{(p^m)}(h_{r1}) \otimes \cdots \otimes \mathrm{X}^{(p^m)}(h_{rn})|\boldsymbol{l} + \boldsymbol{u_i}\rangle \\ &= \frac{1}{\sqrt{p^{\rho_1}}} \sum_{\boldsymbol{l} \in D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}} |\boldsymbol{l} + \boldsymbol{u_i} + \boldsymbol{h_r}\rangle. \end{aligned} \tag{23}$$

As $\boldsymbol{h_r}$ is a row of H_{d1}, $\boldsymbol{h_r} \in D_1^{\perp} \subset D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}} \Rightarrow \boldsymbol{h_r} \in D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}$. We consider $\boldsymbol{l'} = \boldsymbol{l} + \boldsymbol{h_r}$. As the summation in (23) is over $\boldsymbol{l}$ taking all the vectors in $D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}$, $\boldsymbol{l'}$ also takes all the values in $D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}$ as when $\boldsymbol{l}$ and $\boldsymbol{h_r}$ can be obtained as the sum of rows of H_{d1}, then their sum $\boldsymbol{l'} = \boldsymbol{l} + \boldsymbol{h_r}$ can also be obtained as the sum of rows of H_{d1}. Thus, substituting $\boldsymbol{l'} = \boldsymbol{l} + \boldsymbol{h_r}$ in (23), we obtain

$$S_r|\psi_i'\rangle = \frac{1}{\sqrt{p^{\rho_1}}} \sum_{\boldsymbol{l'} \in D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}} |\boldsymbol{l'} + \boldsymbol{u_i}\rangle = |\psi_i'\rangle. \tag{24}$$

Let $\boldsymbol{z_1}, \boldsymbol{z_2}, \ldots, \boldsymbol{z_{\rho_2}}$ be the rows of H_{d2}. Let $\boldsymbol{z_r} = [z_{rj}]_{j=1}^n$ ($r \in \{1, 2, \ldots, \rho_2\}$), then the minimal stabilizer generators corresponding to $\boldsymbol{z_r}$ in $\mathcal{H}_{\mathrm{pCSS}}$ is $S_{(r+\rho_1)} = \mathrm{Z}^{(p^m)}(z_{r1}) \otimes \cdots \otimes \mathrm{Z}^{(p^m)}(z_{rn})$. $S_{(r+\rho_1)}$ stabilizes $|\psi_i'\rangle$ in (22) as follows:

$$\begin{aligned} &S_{(r+\rho_1)}|\psi_i'\rangle \\ &= (\mathrm{Z}^{(p^m)}(z_{r1}) \otimes \cdots \otimes \mathrm{Z}^{(p^m)}(z_{rn}))|\psi_i'\rangle \\ &= \frac{1}{\sqrt{p^{\rho_2}}} \sum_{\boldsymbol{l} \in D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}} \mathrm{Z}^{(p^m)}(z_{r1}) \otimes \cdots \otimes \mathrm{Z}^{(p^m)}(z_{rn})|\boldsymbol{l} + \boldsymbol{u_i}\rangle \\ &= \frac{1}{\sqrt{p^{\rho_2}}} \sum_{\boldsymbol{l} \in D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}} \omega^{\mathrm{Tr}_{p^m/p}((\boldsymbol{l}+\boldsymbol{u_i})\boldsymbol{z_r}^{\mathrm{T}}))}|\boldsymbol{l}+\boldsymbol{u_i}\rangle. \end{aligned} \tag{25}$$

We note that $\boldsymbol{l} \in D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}} \subset D_{Hd2} \Rightarrow \boldsymbol{l} \in D_{Hd2}$. As $\boldsymbol{u_i} \in D_{Hd2}$ and $\boldsymbol{l} \in D_{Hd2}$, we obtain $\mathcal{T}(H_{d2}\boldsymbol{u_i}^{\mathrm{T}}) = 0$ and $\mathcal{T}(H_{d2}\boldsymbol{l}^{\mathrm{T}}) = 0$. As $\mathcal{T}(\cdot)$ is elementwise field trace operation and the field trace operation $\mathrm{Tr}_{p^m/p}(\cdot)$ is $\mathbb{F}_p$-linear, we obtain $\mathcal{T}(H_{d2}(\boldsymbol{u_i} + \boldsymbol{l})^{\mathrm{T}}) = \mathcal{T}(H_{d2}\boldsymbol{u_i}^{\mathrm{T}}) + \mathcal{T}(H_{d2}\boldsymbol{l}^{\mathrm{T}}) = 0$. Thus, $(\boldsymbol{u_i} + \boldsymbol{l}) \in D_{Hd2}$. As $(\boldsymbol{u_i} + \boldsymbol{l}) \in D_{Hd2}$ and $\boldsymbol{z_r}$ is a row of H_{d2}, $\mathrm{Tr}_{p^m/p}(\boldsymbol{z_r}(\boldsymbol{u_i} + \boldsymbol{l})^{\mathrm{T}}) = 0$. Thus, substituting $\mathrm{Tr}_{p^m/p}((\boldsymbol{u_i} + \boldsymbol{l})\boldsymbol{z_r}^{\mathrm{T}}) = 0$ in (25), we obtain

$$S_{(r+\rho)}|\psi_i'\rangle = \frac{1}{\sqrt{p^{\rho_2}}} \sum_{\boldsymbol{l} \in D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}} |\boldsymbol{l}+\boldsymbol{u_i}\rangle = |\psi_i'\rangle. \tag{26}$$

Thus, from (24) to (26), $\{|\psi_i'\rangle\}_{i=0}^{q-1}$ in (22) are the codewords of the $\mathbb{F}_p$-linear CSS code obtained from $\mathcal{H}_{\mathrm{pCSS}}$.

Remark 4: From Section III-B1 and Theorem 3, we note that the $\mathbb{F}_p$-linear CSS code obtained from D_1 and D_2 is an $((n, p^{((m-2)n+k_1+k_2)}, d_z \geq y_1/d_x \geq y_2))$ quantum code. We note that the $\mathbb{F}_p$-linear CSS code is a special case of the CSS-like codes proposed in [6] by considering $r = p, C_1 = D_{Hd2}$, and $C_2 = D_{Hd1}$ in [6, Th. 3.4]. Thus, the class of $\mathbb{F}_p$-linear CSS codes is a special class of CSS-like codes proposed in [6].

We summarize the code parameters of the $\mathbb{F}_{p^m}$-linear CSS and $\mathbb{F}_p$-linear CSS codes obtained from the codes $D_1[n, k_1, d_1]_{p^m}$ and $D_2[n, k_2, d_2]_{p^m}$ in Table I. As the dimension of the $\mathbb{F}_{p^m}$-linear CSS and $\mathbb{F}_p$-linear CSS codes are $(p^m)^{k_1+k_2-n}$ and $p^{(m-2)n+k_1+k_2}$, their coding rates are $m(k_1 + k_2 - n)/(mn) = (k_1 + k_2 - n)/n$ and $((m-2)n + k_1 + k_2)/mn$, respectively.

From Table I, we note that when $m = 1$, i.e., $q = p$, the check matrices of the $\mathbb{F}_{p^m}$-linear CSS and the $\mathbb{F}_p$-linear CSS codes are the same. Thus, for qudits of prime dimension, the $\mathbb{F}_{p^m}$-linear CSS and the $\mathbb{F}_p$-linear CSS codes are the same codes.

Remark 5: Let us consider two parity check matrices H_{d1} and H_{d2}. The $\mathbb{F}_p$-linear CSS code is based on codes D_{Hd1} and D_{Hd2} obtained as the dual spaces of the H_{d1} and H_{d2} with respect to the trace inner product, that are classical additive

TABLE I. Summary of the Code Parameters of the $\mathbb{F}_{p^m}$-Linear CSS and $\mathbb{F}_p$-Linear CSS Codes Over Qudits Obtained From the Codes $D_1[n, k_1, d_1]_{p^m}$ and $D_2[n, k_2, d_2]_{p^m}$

Code parameters	$\mathbb{F}_{p^m}$-linear CSS code over qudits	$\mathbb{F}_p$-linear CSS code over qudits
Code length	n	n
Coset Structure	Cosets of $D_1^{\perp}$ in D_2	Cosets of $D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}$ in D_{Hd2}
Number of cosets	$(p^m)^{(k_1+k_2-n)}$	$p^{((m-2)n+k_1+k_2)}$
Basis Codewords	Obtained from cosets of $D_1^{\perp}$ in D_2	Obtained from cosets of $D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}}$ in D_{Hd2}
Dimension	$(p^m)^{(k_1+k_2-n)}$	$p^{((m-2)n+k_1+k_2)}$
Rate	$(k_1+k_2-n)/n$	$((m-2)n+k_1+k_2)/mn$
Distance	$d_{cx} \geq d_2$ and $d_{cz} \geq d_1$	$d_{px} \geq y_2$ and $d_{pz} \geq y_1$
Check matrix	$\left[\begin{array}{c\|c} H_{d1} & \\ \alpha H_{d1} & \\ \vdots & \mathbf{0} \\ \alpha^{m-1} H_{d1} & \\ & H_{d2} \\ & \alpha H_{d2} \\ \mathbf{0} & \vdots \\ & \alpha^{m-1} H_{d2} \end{array}\right]$	$\left[\begin{array}{c\|c} H_{d1} & \mathbf{0} \\ \mathbf{0} & H_{d2} \end{array}\right]$

codes. Thus, the $\mathbb{F}_p$-linear CSS code can also be called additive CSS codes. The $\mathbb{F}_{p^m}$-linear CSS code is based on codes D_1 and D_2 obtained as the dual spaces of the H_{d1} and H_{d2} with respect to the Euclidean inner product, that are classical linear codes.

Remark 6: We note that the dimension of a qudit is p^m, while that of a subqudit is p. We note that the dimension of a $\mathbb{F}_p$-linear CSS code is a power of p and need not be a power of p^m; hence, it encodes logical subqudits in physical qudits. The dimension of a $\mathbb{F}_{p^m}$-linear CSS code is a power of p^m; hence, it encodes logical qudits into physical qudits. The $\mathbb{F}_{p^m}$-linear CSS and $\mathbb{F}_p$-linear CSS codes can be encoded using the encoding procedure provided in [8] for the qudit stabilizer codes. Quantum operations can be performed over subqudits by physically performing operations over the qudits containing the subqudits.

Remark 7: The error correction procedures for $\mathbb{F}_{p^m}$-linear CSS and $\mathbb{F}_p$-linear CSS codes use the eigenvalue-based syndrome with respect to the minimal stabilizer generators to deduce and correct the errors, similar to the error correction procedure for stabilizer codes. As the power s_i of ω in $S_iE = \omega^{s_i} ES_i$ that is used to obtain the syndrome belongs to $\{0, 1, \ldots, p-1\}$ and a subqudit has a dimension of p, a subqudit is enough to store its value. Thus, for ρ minimal stabilizer generators, the number of syndrome subqudits needed during error correction is ρ. During error correction, the $\mathbb{F}_{p^m}$-linear CSS code requires $m(2n-k_1-k_2)$ syndrome subqudits, i.e., $(2n-k_1-k_2)$ syndrome qudits, while the $\mathbb{F}_p$-linear CSS code requires only $(2n-k_1-k_2)$ syndrome subqudits that are implemented as a part of $\lfloor (2n-k_1-k_2)/m \rfloor$ syndrome qudits. Thus, the complexity of the error correction circuit and the number of ancillary syndrome qudits needed is much lesser for a $\mathbb{F}_p$-linear CSS code when compared to the corresponding $\mathbb{F}_{p^m}$-linear CSS code. We note that when $(2n-k_1-k_2)$ is not a multiple of m, the operators on the syndrome subqudits are performed by performing operations on the qudits, which contain the subqudits.

TABLE II. Elements of $\mathbb{F}_9$ With Primitive Element α and Primitive Polynomial $p(x) = x^2 + x + 2$

Element	Expansion	Field trace
0	0	0
1	1	2
α	α	2
α^2	$2\alpha+1$	0
α^3	$2\alpha+2$	2
α^4	2	1
α^5	2α	1
α^6	$\alpha+2$	0
α^7	$\alpha+1$	1

C. EXAMPLES

Using a few examples, we demonstrate the tradeoff between the error detection and correction capability and the coding rate of the $\mathbb{F}_{p^m}$-linear CSS and the $\mathbb{F}_p$-linear CSS code and exhibit a few caveats.

Example 1: In this example, we consider a classical code $C_1[5, 3, 3]$ over $\mathbb{F}_9$ with parity check matrix H_{d1} as follows:

$$H_{d1} = \begin{bmatrix} 1 & 1 & 1 & \alpha & \alpha^3 \\ \alpha & \alpha^2 & \alpha^5 & 1 & \alpha \end{bmatrix} \tag{27}$$

where α is the primitive element of $\mathbb{F}_9$.

C_1 is a dual containing code ($C_1^{\perp} \subset C_1$) as $H_{d1}H_{d1}^{\mathrm{T}} = 0$; hence, we consider the code C_2 to be equal to C_1. Thus, $H_{d2} = H_{d1}$.

In Table II , we provide the elements of $\mathbb{F}_9$ along with their field trace and expansion in terms of $\{1, \alpha\}$.

From Section III-A and Theorem 1, the $\mathbb{F}_{p^m}$-linear CSS code based on C_1 is obtained from the following check matrix:

$$\mathcal{H}_S = \left[\begin{array}{ccccc|ccccc} 1 & 1 & 1 & \alpha & \alpha^3 & & & & & \\ \alpha & \alpha^2 & \alpha^5 & 1 & \alpha & & & & & \\ \alpha & \alpha & \alpha & \alpha^2 & \alpha^4 & & & \mathbf{0} & & \\ \alpha^2 & \alpha^3 & \alpha^6 & \alpha & \alpha^2 & & & & & \\ & & & & & 1 & 1 & 1 & \alpha & \alpha^3 \\ & & \mathbf{0} & & & \alpha & \alpha^2 & \alpha^5 & 1 & \alpha \\ & & & & & \alpha & \alpha & \alpha & \alpha^2 & \alpha^4 \\ & & & & & \alpha^2 & \alpha^3 & \alpha^6 & \alpha & \alpha^2 \end{array}\right]. \tag{28}$$

The dimension of the $\mathbb{F}_{p^m}$-linear CSS code obtained from C_1 is 9 as $(p^m)^{k_1+k_2-n} = 9^{3+3-5} = 9$. From Theorem 2, the minimum distance $d \geq \min(d_1, d_2) = \min(3, 3) = 3$. From the quantum Singleton bound, for a code of dimension $(p^m)^l$, we have $2(d-1) \leq n-l \Rightarrow 2(d-1) \leq 5-1 = 4 \Rightarrow d \leq 3$. Thus, as $3 \leq d \leq 3$, we obtain $d = 3$. We note that the code is a nondegenerate code as there is no stabilizer of weight less than or equal to $(d-1) = 2$ as $d_1 = d_2 = 3$.

Thus, from Theorem 2, $d_{cx} = d_{cz} = 3$. Thus, the $\mathbb{F}_{p^m}$-linear CSS code obtained from C_1 is a $[[5, 1, 3/3]]_9$-quantum code.

We next obtain the $\mathbb{F}_p$-linear CSS code from C_1 by considering $C_2 = C_1$. From Section III-B and (18), the $\mathbb{F}_p$-linear CSS code based on C_1 is obtained from the following check matrix:

$$\mathcal{H}_S = \left[\begin{array}{c|c} \begin{matrix} 1 & 1 & 1 & \alpha & \alpha^3 \\ \alpha & \alpha^2 & \alpha^5 & 1 & \alpha \end{matrix} & \mathbf{0} \\ \mathbf{0} & \begin{matrix} 1 & 1 & 1 & \alpha & \alpha^3 \\ \alpha & \alpha^2 & \alpha^5 & 1 & \alpha \end{matrix} \end{array}\right]. \tag{29}$$

The dimension of the $\mathbb{F}_p$-linear CSS code obtained is 9^3 as $p^{(m-2)n+k_1+k_2} = 3^{(2-2)5+3+3} = 3^6 = 9^3$. From Theorem 3, d_{px} and d_{px} of the $\mathbb{F}_p$-linear CSS code are less than d_{cx} and d_{cx} of the $\mathbb{F}_{p^m}$-linear CSS code, i.e., $d_{px} \leq d_{cx} = 3$ and $d_{pz} \leq d_{cz} = 3$.

We consider the operator $O \equiv [0\ 0\ 0\ 0\ 0|\alpha^5\ 1\ 0\ 0\ 0]$ of weight 2. By considering $\boldsymbol{h_x} = [0\ 0\ 0\ 0\ 0]$ and $\boldsymbol{h_z} = [\alpha^5\ 1\ 0\ 0\ 0]$, we obtain $\mathcal{T}(H_{d2}\boldsymbol{h_x}^{\mathrm{T}}) = \mathcal{T}(H_{d1}\mathbf{0}) = \mathbf{0}$ and

$$\begin{aligned} H_{d1}\boldsymbol{h_z}^{\mathrm{T}} &= H_{d1}[\alpha^5\ 1\ 0\ 0\ 0]^{\mathrm{T}} \\ &= \begin{bmatrix} 1 & 1 & 1 & \alpha & \alpha^3 \\ \alpha & \alpha^2 & \alpha^5 & 1 & \alpha \end{bmatrix} \begin{bmatrix} \alpha^5 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} \alpha^5 + 1 \\ \alpha^6 + \alpha^2 \end{bmatrix} = \begin{bmatrix} \alpha^2 \\ 0 \end{bmatrix} \\ \Rightarrow \mathcal{T}(H_{d1}\boldsymbol{h_z}^{\mathrm{T}}) &= \begin{bmatrix} \mathrm{Tr}_{p^m/p}(\alpha^2) \\ \mathrm{Tr}_{p^m/p}(0) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} = \mathbf{0}. \end{aligned} \tag{30}$$

Thus, as $\mathcal{T}(H_{d2}\boldsymbol{h_x}^{\mathrm{T}}) = \mathcal{T}(H_{d1}\boldsymbol{h_z}^{\mathrm{T}}) = \mathbf{0}$, from (19), O commutes with all the minimal stabilizer generators in $\mathcal{H}_S$ in (29); hence, O belongs to the normalizer $\mathcal{N}_S$. Similarly, $O' = [\alpha^5\ 1\ 0\ 0\ 0|0\ 0\ 0\ 0\ 0] \in \mathcal{N}_S$.

As $C_1^{\perp} \subset C_1$ and the minimum distance of C_1 is 3, the weight of the elements in $C_1^{\perp}$ is at least 3. As the stabilizers are based on the elements in $C_1^{\perp}$, the weight of the stabilizers is at least 3. Thus, as the weights of O and O' are 2 each, O and O' do not belong to S. Hence, $O, O' \in \mathcal{N}_S \setminus S$. We note that there does not exist an element of weight 1 in the normalizer $\mathcal{N}_S$. Thus, the minimum distance of the $\mathbb{F}_p$-linear CSS code is 2, $d_{px} = d_{pz} = 2$. Thus, the $\mathbb{F}_p$-linear CSS code obtained from C_1 is a $[[5, 3, 2/2]]_9$-quantum code.

We note that the codes D_{Hd1} and D_{Hd2} obtained from H_{d1} and H_{d2} have a minimum distance of 2. Thus, $y_1 = y_2 = 2$. As $d_{px} = y_2$ and $d_{pz} = y_1$, the code is a nondegenerate code.

Based on the $\mathbb{F}_{p^m}$-linear CSS and the $\mathbb{F}_p$-linear CSS code obtained in this example, we can see the tradeoff between the error-correction capability and the coding rate. The $\mathbb{F}_p$-linear CSS code has a coding rate of 3/5 that is more compared to the coding rate 1/5 of the $\mathbb{F}_{p^m}$-linear CSS code. However, the $\mathbb{F}_p$-linear CSS code can only detect a single qudit error as $d_{px} = d_{pz} = 2$, while the $\mathbb{F}_{p^m}$-linear CSS code can correct any single qudit error as $d_{cx} = d_{cz} = 3$.

Example 2: In this example, we consider two classical codes $C_1[3, 1, 3]$ and $C_2[3, 1, 2]$ over $\mathbb{F}_9$ with parity check matrix H_{d1} and H_{d2} as follows:

$$H_{d1} = \begin{bmatrix} 1 & 1 & 1 \\ \alpha^2 & \alpha^3 & \alpha^6 \end{bmatrix} \quad H_{d2} = \begin{bmatrix} \alpha^2 & \alpha^3 & \alpha^5 \\ \alpha^7 & 1 & \alpha^2 \end{bmatrix} \tag{31}$$

where α is the primitive element of $\mathbb{F}_9$. The elements of $\mathbb{F}_9$ are provided in Table II. Based on Table II, we note that $H_{d1}H_{d2}^{\mathrm{T}} = 0$ and $C_2^{\perp} \subset C_1$.

From Section III-A and Theorem 1, the $\mathbb{F}_{p^m}$-linear CSS code based on C_1 and C_2 is obtained from the following check matrix:

$$\mathcal{H}_S = \left[\begin{array}{c|c} \begin{matrix} 1 & 1 & 1 \\ \alpha^2 & \alpha^3 & \alpha^6 \\ \alpha & \alpha & \alpha \\ \alpha^3 & \alpha^4 & \alpha^7 \end{matrix} & \mathbf{0} \\ \mathbf{0} & \begin{matrix} \alpha^2 & \alpha^3 & \alpha^5 \\ \alpha^7 & 1 & \alpha^2 \\ \alpha^3 & \alpha^4 & \alpha^6 \\ 1 & \alpha & \alpha^3 \end{matrix} \end{array}\right]. \tag{32}$$

The dimension of the $\mathbb{F}_{p^m}$-linear CSS code will be 9^{-1} as $(p^m)^{k_1+k_2-n} = 9^{1+1-3} = 9^{-1}$, which is not possible as the dimension is always a positive integer. Thus, we cannot construct a $\mathbb{F}_{p^m}$-linear CSS code based on C_1 and C_2. We note that this is also due to the fact that eight minimal stabilizer generators cannot stabilize a three-qudit state with each qudit of dimension $q = 9$ as each minimal stabilizer generators reduces the dimension of the codespace by a factor of 3 and the dimension of three-qudit state is only $9^3 = 3^6 < 3^8$.

Nevertheless, we can obtain an $\mathbb{F}_p$-linear CSS code from C_1 and C_2 whose check matrix is as follows:

$$\mathcal{H}_S = \left[\begin{array}{c|c} \begin{matrix} 1 & 1 & 1 \\ \alpha^2 & \alpha^3 & \alpha^6 \end{matrix} & \mathbf{0} \\ \mathbf{0} & \begin{matrix} \alpha^2 & \alpha^3 & \alpha^5 \\ \alpha^7 & 1 & \alpha^2 \end{matrix} \end{array}\right]. \tag{33}$$

The dimension of the $\mathbb{F}_p$-linear CSS code obtained is 9 as $p^{((m-2)n+k_1+k_2)} = 3^{(2-2)5+1+1} = 3^2 = 9$.

To compute the minimum distance d_p, we consider the operator $O \equiv [0\ 0\ 0|\alpha^5\ 1\ 0]$ of weight 2. By considering $\boldsymbol{h_x} = [0\ 0\ 0]$ and $\boldsymbol{h_z} = [\alpha^5\ 1\ 0]$, we obtain $\mathcal{T}(H_{d2}\boldsymbol{h_x}^{\mathrm{T}}) = \mathcal{T}(H_{d2}\mathbf{0}) = \mathbf{0}$ and

$$\begin{aligned} H_{d1}\boldsymbol{h_z}^{\mathrm{T}} &= H_{d1}[\alpha^5\ 1\ 0]^{\mathrm{T}} = \begin{bmatrix} 1 & 1 & 1 \\ \alpha^2 & \alpha^3 & \alpha^6 \end{bmatrix} \begin{bmatrix} \alpha^5 \\ 1 \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} \alpha^5 + 1 \\ \alpha^7 + \alpha^3 \end{bmatrix} = \begin{bmatrix} \alpha^2 \\ 0 \end{bmatrix} \end{aligned}$$

TABLE III. Elements of $\mathbb{F}_8$ With Primitive Element α and Primitive Polynomial $p(x) = x^3 + x + 1$

Element	Expansion	Field trace
0	0	0
1	1	1
α	α	0
α^2	α^2	0
α^3	$\alpha+1$	1
α^4	$\alpha^2+\alpha$	0
α^5	$\alpha^2+\alpha+1$	1
α^6	α^2+1	1

$$\Rightarrow \mathcal{T}(H_{d1}\boldsymbol{h_z}^{\mathrm{T}}) = \begin{bmatrix} \mathrm{Tr}_{p^m/p}(\alpha^2) \\ \mathrm{Tr}_{p^m/p}(0) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} = \mathbf{0}. \tag{34}$$

Thus, as $\mathcal{T}(H_{d2}\boldsymbol{h_x}^{\mathrm{T}}) = \mathcal{T}(H_{d1}\boldsymbol{h_z}^{\mathrm{T}}) = \mathbf{0}$, from (19), O commutes with all the minimal stabilizer generators in $\mathcal{H}_S$ in (33); hence, O belongs to the normalizer $\mathcal{N}_S$. Similarly, $O' = [\alpha\ 1\ 0|0\ 0\ 0] \in \mathcal{N}_S$.

As $C_2^{\perp} \subset C_1$ and the minimum distance of C_1 is 3, the weight of the elements in $C_2^{\perp}$ is at least 3. As the stabilizers of form $[\mathbf{0}|\boldsymbol{u}]$ are based on the H_{d2}, namely the elements in $C_2^{\perp}$, the weight of the stabilizers is at least 3. Thus, as the weight of O is 2, O does not belong to S. Hence, $O \in \mathcal{N}_S \setminus S$. We note that a stabilizer of form $[\boldsymbol{v}|\mathbf{0}]$ is based on H_{d1} and generated by the rows of H_{d1}. As $[\alpha\ 1\ 0]$ cannot be generated by the rows of H_{d1}, O' does not belong to S; hence, $O' \in \mathcal{N}_S \setminus S$. We note that there does not exist an element of weight 1 in the normalizer $\mathcal{N}_S$. Thus, the minimum distance of the $\mathbb{F}_p$-linear CSS code is $d_p = 2$, $d_{px} = d_{pz} = 2$. Thus, the $\mathbb{F}_p$-linear CSS code obtained from C_1 and C_2 is a $[[3, 1, 2/2]]_9$-quantum code.

We note that the minimum distances y_1 and y_2 of the codes D_{Hd1} and D_{Hd2} obtained from H_{d1} and H_{d2} are both equal to 2 as $[\alpha^5\ 1\ 0] \in D_{Hd1}$ and $[\alpha\ 1\ 0] \in D_{Hd2}$. As $d_{px} = d_{pz} = 2$, the code is a nondegenerate code.

Through this example, we demonstrated the caveat that from two classical codes C_1 and C_2 satisfying the dual containing criteria it might not always be possible to obtain a $\mathbb{F}_{p^m}$-linear CSS code; however, we could obtain $\mathbb{F}_p$-linear CSS codes from these codes.

Example 3: In this example, we consider the classical Reed–Solomon (RS) code $C_1[7, 5, 3]$ over $\mathbb{F}_8$ with parity check matrix H_{d1} as follows:

$$H_{d1} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \end{bmatrix} \tag{35}$$

where α is the primitive element of $\mathbb{F}_8$.

In Table III , we provide the elements of $\mathbb{F}_8$ along with their field trace and expansion in terms of $\{1, \alpha, \alpha^2\}$. We consider the code C_2 to be equal to C_1 as C_1 is a dual containing code ($C_1^{\perp} \subset C_1$) as $H_{d1}H_{d1}^{\mathrm{T}} = 0$ based on Table III. Thus, $H_{d2} = H_{d1}$.

From Section III-A and Theorem 1, as $H_{d1} = H_{d2}$, the $\mathbb{F}_{p^m}$-linear CSS code based on C_1 is obtained from the following check matrix:

$$\mathcal{H}_S = \left[\begin{array}{c|c} \begin{matrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & 1 \\ \alpha & \alpha^3 & \alpha^5 & 1 & \alpha^2 & \alpha^4 & \alpha^6 \end{matrix} & \mathbf{0} \\ \mathbf{0} & \begin{matrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & 1 \\ \alpha & \alpha^3 & \alpha^5 & 1 & \alpha^2 & \alpha^4 & \alpha^6 \end{matrix} \end{array}\right]. \tag{36}$$

The dimension of the $\mathbb{F}_{p^m}$-linear CSS code obtained from C_1 is 8^3 as $(p^m)^{k_1+k_2-n} = 8^{5+5-7} = 8^3$. From Theorem 2, $d \geq \min(d_1, d_2) = d_1 = \min(3, 3) = 3$. We note that the operator $O \equiv [1\ 1\ 0\ 1\ 0\ 0\ 0|0\ 0\ 0\ 0\ 0\ 0\ 0]$ commutes with all the minimal stabilizer generators in $\mathcal{H}_S$ and belongs to $\mathcal{N}_S$ as $H_{d1}\boldsymbol{h_z}^{\mathrm{T}} = \mathbf{0}$ and $H_{d2}\boldsymbol{h_x}^{\mathrm{T}} = \mathbf{0}$, where $\boldsymbol{h_x} = [1\ 1\ 0\ 1\ 0\ 0\ 0]$ and $\boldsymbol{h_z} = [0\ 0\ 0\ 0\ 0\ 0\ 0]$, as follows:

$$\begin{aligned} H_{d1}\boldsymbol{h_z}^{\mathrm{T}} &= H_{d1}[0\ 0\ 0\ 0\ 0\ 0\ 0]^{\mathrm{T}} = \mathbf{0} \\ H_{d2}\boldsymbol{h_x}^{\mathrm{T}} &= H_{d2}[1\ 1\ 0\ 1\ 0\ 0\ 0]^{\mathrm{T}} \\ &= \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} 1+\alpha+\alpha^3 \\ 1+\alpha^2+\alpha^6 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} = \mathbf{0}. \end{aligned} \tag{37}$$

Similarly, $O' \equiv [0\ 0\ 0\ 0\ 0\ 0\ 0|1\ 1\ 0\ 1\ 0\ 0\ 0]$ commutes with all stabilizers.

We note that O and O' do not belong to S as it cannot be obtained based on the minimal stabilizer generators in H_S in (36). Thus, $O, O' \in \mathcal{N}_S \setminus S$ and $d = 3$, $d_{cx} = d_{cz} = 3$ as the weight of O and O' are bot 3, $d \geq 3$, $d_{cx} \geq d_2 = 3$, and $d_{cz} \geq d_1 = 3$. We also note that the code is a nondegenerate code as there is no stabilizer of weight less than or equal to $(d-1) = 2$.

Thus, the $\mathbb{F}_{p^m}$-linear CSS code obtained from C_1 is a $[[7, 3, 3/3]]_8$-quantum code.

We next obtain the $\mathbb{F}_p$-linear CSS code from C_1 by considering $C_2 = C_1$. From Section III-B and (18), the $\mathbb{F}_p$-linear CSS code based on C_1 is obtained from the following check matrix:

$$\mathcal{H}_S = \left[\begin{array}{c|c} \begin{matrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \end{matrix} & \mathbf{0} \\ \mathbf{0} & \begin{matrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \end{matrix} \end{array}\right]. \tag{38}$$

The dimension of the $\mathbb{F}_p$-linear CSS code obtained is 2^{17} as $p^{(m-2)n+k_1+k_2} = 2^{(3-2)7+5+5} = 2^{17}$. From Theorem 3, we note that $d_{px} \leq d_{cx} = 3$ and $d_{pz} \leq d_{cz} = 3$. We note that the weight of any stabilizer of the $\mathbb{F}_p$-linear CSS code is at least 3 as they are obtained from H_{d1}, that are based on $C_1^{\perp} \subset C_1$, and minimum distance of C_1 is 3. The operator $O = [0\ 1\ 0\ 0\ 0\ 0\ 0|0\ 0\ 0\ 0\ 0\ 0\ 0]$ is an element of the normalizer $\mathcal{N}_S$ as it commutes with all stabilizers as $\mathcal{T}(H_{d1}\boldsymbol{h_z}^{\mathrm{T}}) = \mathbf{0}$ and $\mathcal{T}(H_{d2}\boldsymbol{h_x}^{\mathrm{T}}) = \mathbf{0}$, where $\boldsymbol{h_x} = [0\ 1\ 0\ 0\ 0\ 0\ 0]$ and $\boldsymbol{h_z} = [0\ 0\ 0\ 0\ 0\ 0\ 0]$, as follows:

$$\begin{aligned}
\mathcal{T}(H_{d1}\boldsymbol{h_z}^{\mathrm{T}}) &= \mathcal{T}(H_{d1}\mathbf{0}^{\mathrm{T}})\mathbf{0} \\
H_{d2}\boldsymbol{h_x}^{\mathrm{T}} &= H_{d1}\boldsymbol{h_x}^{\mathrm{T}} \\
&= \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \\
&= \begin{bmatrix} \alpha \\ \alpha^2 \end{bmatrix} \\
\Rightarrow \mathcal{T}(H_{d2}\boldsymbol{h_x}^{\mathrm{T}}) &= \begin{bmatrix} \mathrm{Tr}_{p^m/p}(\alpha) \\ \mathrm{Tr}_{p^m/p}(\alpha^2) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} = \mathbf{0}. \qquad (39)
\end{aligned}$$

As weight of O is 1, it does not belong to S. Thus, $O \in \mathcal{N}_S \setminus S$, $d_p = 1$, and $d_{px} = 1$. Similarly, $O' = [0\ 0\ 0\ 0\ 0\ 0\ 0|0\ 1\ 0\ 0\ 0\ 0\ 0] \in \mathcal{N}_S \setminus S$ and $d_{pz} = 1$.

Thus, the $\mathbb{F}_p$-linear CSS code obtained from C_1 is a $((7, 2^{17}, 1/1))_8$-quantum code. Thus, the code can neither detect nor correct any errors. Thus, this code is not a useful code.

Through this example, we illustrated the caveat that the $\mathbb{F}_p$-linear CSS code obtained from the dual containing classical code might not always be a useful code enough, although the $\mathbb{F}_{p^m}$-linear CSS code obtained is a useful code.

IV. QUANTUM CODES FROM DUAL CONTAINING CLASSICAL CODES OVER $\mathbb{F}_{p^m}$

In this section, we discuss two classes of qudit stabilizer codes obtained from the parity check matrices H_{d1} and H_{d2} of the codes D_1 and D_2. We further discuss the tradeoff for designing codes with better error detection and correction capability or higher coding rate within each class.

A. $\mathbb{F}_{p^l}$-LINEAR CSS-LIKE CODES

We first discuss a special subclass of the $\mathbb{F}_{p^l}$-linear CSS-like codes [6] obtained from H_{d1} and H_{d2}, where l divides m.

Let l be a positive integer that divides m. Then, $\mathbb{F}_{p^l}$ is a subfield of $\mathbb{F}_{p^m}$. As α is the primitive element of $\mathbb{F}_{p^m}$, $\zeta = \alpha^z$ is the primitive element of $\mathbb{F}_{p^l}$, where $z = (p^m - 1)/(p^l - 1)$. For $i = 1, 2$, let $D_{p^l i}$ be the code obtained as a set of all vectors $\boldsymbol{v} \in \mathbb{F}_{p^m}^n$ such that $\mathcal{T}_{p^m/p^l}(H_{di}\boldsymbol{v}^{\mathrm{T}}) = 0$, where $\mathcal{T}_{p^m/p^l}(A) = [\mathrm{Tr}_{p^m/p^l}(a_{ij})]$ for a matrix $A = [a_{ij}]$ over $\mathbb{F}_{p^m}$. For $i = 1, 2$, we note that $D_{Hdi} = D_{pi}$ and $D_i = D_{p^m i}$.

Let $\mathcal{Q}_{p^l}$ be the qudit stabilizer code with the following check matrix:

$$\mathcal{H}_{p^l} = \left[\begin{array}{c|c} H_{d1} & \\ \zeta H_{d1} & \\ \vdots & \mathbf{0} \\ \zeta^{l-1} H_{d1} & \\ & H_{d2} \\ & \zeta H_{d2} \\ \mathbf{0} & \vdots \\ & \zeta^{l-1} H_{d2} \end{array}\right]. \qquad (40)$$

Let $d_{p^l x}$ and $d_{p^l z}$ be the X-distance and Z-distance of the quantum code $\mathcal{Q}_{p^l}$. As the number of minimal stabilizer generators in the check matrix $\mathcal{H}_{\mathrm{p^l}}$ is $l(2n - k_1 - k_2)$, $\mathcal{Q}_{p^l}$ is a $((n, p^{(m-2\,l)n+l(k_1+k_2)}, d_{p^l z}/d_{p^l x}))_{p^m}$-stabilizer code.

We first provide a result in Lemma 2 that we will be using to obtain $d_{p^l x}$ and $d_{p^l z}$ of the code $\mathcal{Q}_{p^l}$ in Theorem 4.

Lemma 2: For $\beta \in \mathbb{F}_{p^m}$, $\mathrm{Tr}_{p^m/p}(\zeta^i \beta) = 0$ $\forall i \in \{0, 1, \ldots, l-1\}$ if and only if $\mathrm{Tr}_{p^m/p^l}(\beta) = 0$, where l divides m and ζ is the primitive element of $\mathbb{F}_{p^l}$.

The proof of Lemma 2 is provided in the Appendix. We discuss the distances $d_{p^l x}$ and $d_{p^l z}$ of the code and other properties in Theorem 4.

Theorem 4: Let D_1 and D_2 be two classical codes over $\mathbb{F}_{p^m}$ of length n with parity check matrices H_{d1} and H_{d2}. Let $D_{p^l i} = \{\boldsymbol{v} \in \mathbb{F}_{p^m}^n | \mathcal{T}_{p^m/p^l}(H_{di}\boldsymbol{v}^{\mathrm{T}}) = \mathbf{0}\}$, then, the following conditions hold.

1) $d_{p^l x}$ and $d_{p^l z}$ of $\mathcal{Q}_{p^{l_1}}$ corresponding to the check matrix $\mathcal{H}_{\mathrm{p^l}}$ satisfy $d_{p^l x} \geq f_2$ and $d_{p^l z} \geq f_1$ and saturate the inequalities if and only if the code $\mathcal{Q}_{p^{l_1}}$ is a nondegenerate code, where f_1 and f_2 are the minimum distances of $D_{p^l 1}$ and $D_{p^l 2}$, respectively.
2) Let l_1 and l_2 divide m and l_1 divide l_2. Then, $\mathcal{Q}_{p^m} \subset \mathcal{Q}_{p^{l_2}} \subset \mathcal{Q}_{p^{l_1}} \subset \mathcal{Q}_p$, $d_{px} \leq d_{p^{l_1} x} \leq d_{p^{l_2} x} \leq d_{p^m x}$, and $d_{pz} \leq d_{p^{l_1} z} \leq d_{p^{l_2} z} \leq d_{p^m z}$.

Proof: Let us consider an element $[\boldsymbol{h_x}|\boldsymbol{h_z}]$ from $\mathcal{N}_S$. Then, the symplectic product of $[\boldsymbol{h_x}|\boldsymbol{h_z}]$ with each minimal stabilizer generator is 0, i.e.,

$$\mathcal{T}\left(\mathcal{H}_{p^l}\left[\begin{array}{c} \boldsymbol{h_z}^{\mathrm{T}} \\ \hline \boldsymbol{h_x}^{\mathrm{T}} \end{array}\right]\right) = \mathbf{0}$$

$$\Rightarrow \mathcal{T}\left(\left[\begin{array}{c|c} H_{d1} & \\ \zeta H_{d1} & \\ \vdots & \mathbf{0} \\ \zeta^{l-1}H_{d1} & \\ & H_{d2} \\ \mathbf{0} & \zeta H_{d2} \\ & \vdots \\ & \zeta^{l-1}H_{d2} \end{array}\right]\left[\begin{array}{c} \boldsymbol{h_z}^{\mathrm{T}} \\ \hline \boldsymbol{h_x}^{\mathrm{T}} \end{array}\right]\right) = \mathbf{0}$$

$$\Rightarrow \mathcal{T}\left(\left[\begin{array}{c} H_{d1}\boldsymbol{h_z}^{\mathrm{T}} \\ \zeta H_{d1}\boldsymbol{h_z}^{\mathrm{T}} \\ \vdots \\ \zeta^{l-1}H_{d1}\boldsymbol{h_z}^{\mathrm{T}} \\ \hline H_{d2}\boldsymbol{h_x}^{\mathrm{T}} \\ \zeta H_{d2}\boldsymbol{h_x}^{\mathrm{T}} \\ \vdots \\ \zeta^{l-1}H_{d2}\boldsymbol{h_x}^{\mathrm{T}} \end{array}\right]\right) = \mathbf{0}$$

$$\Rightarrow \mathcal{T}(\zeta^y H_{d1}\boldsymbol{h_z}^{\mathrm{T}}) = \mathbf{0} \text{ and } \mathcal{T}(\zeta^y H_{d2}\boldsymbol{h_x}^{\mathrm{T}}) = \mathbf{0} \tag{41}$$

for all $y \in \{0, 1, \ldots, l-1\}$. Thus, from Lemma 2, we obtain $\mathcal{T}_{p^m/p^l}(H_{d1}\boldsymbol{h_z}^{\mathrm{T}}) = \mathbf{0}$ and $\mathcal{T}_{p^m/p^l}(H_{d2}\boldsymbol{h_x}^{\mathrm{T}}) = \mathbf{0}$. Thus, $\boldsymbol{h_z} \in D_{p^l1}$ and $\boldsymbol{h_x} \in D_{p^l2}$. Let f_1 and f_2 be the minimum distances of D_{p^l1} and D_{p^l2}, respectively. Similar to the proofs of Theorems 2 and 3, it can be proved that d_{p^lx} and d_{p^lz} satisfy $d_{p^lx} \geq f_2$ and $d_{p^lz} \geq f_1$ and saturate the inequality if and only if the code $\mathcal{Q}_{p^l1}$ is a nondegenerate code.

Let l_1 and l_2 divide m and l_1 divide l_2. Thus, $\mathbb{F}_p \subset \mathbb{F}_{p^{l_1}} \subset \mathbb{F}_{p^{l_2}} \subset \mathbb{F}_{p^m}$ We next show that $\mathcal{Q}_{p^m} \subset \mathcal{Q}_{p^{l_2}} \subset \mathcal{Q}_{p^{l_1}} \subset \mathcal{Q}_p$, $d_{px} \leq d_{p^{l_1}x} \leq d_{p^{l_2}x} \leq d_{p^mx}$, and $d_{pz} \leq d_{p^{l_1}z} \leq d_{p^{l_2}z} \leq d_{p^mz}$. As $\mathbb{F}_p \subset \mathbb{F}_{p^{l_1}} \subset \mathbb{F}_{p^{l_2}} \subset \mathbb{F}_{p^m}$, the minimal stabilizer generators in $\mathcal{H}_p$ is a subset of those in $\mathcal{H}_{p^{l_1}}$, which is a subset of those in $\mathcal{H}_{p^{l_2}}$, which is a subset of those in $\mathcal{H}_{p^m}$. As each minimal stabilizer generator is a constraint on the codespace, all the codewords of $\mathcal{Q}_{p^{l_2}}$ are also codewords of $\mathcal{Q}_{p^m}$. Thus, $\mathcal{Q}_{p^m} \subset \mathcal{Q}_{p^{l_2}}$, $d_{p^{l_2}x} \leq d_{p^mx}$, and $d_{p^{l_2}z} \leq d_{p^mz}$. Similarly, we obtain $\mathcal{Q}_{p^m} \subset \mathcal{Q}_{p^{l_2}} \subset \mathcal{Q}_{p^{l_1}} \subset \mathcal{Q}_p$, $d_{px} \leq d_{p^{l_1}x} \leq d_{p^{l_2}x} \leq d_{p^mx}$, and $d_{pz} \leq d_{p^{l_1}z} \leq d_{p^{l_2}z} \leq d_{p^mz}$. ■

Similar to the $\mathbb{F}_p$-linear CSS code, the stabilizer code based on check matrix $\mathcal{H}_{\mathrm{p^l}}$ in (40) is obtained from the cosets of $(D_{p^l1})^{\perp_{\mathrm{Tr}_{p^m/p^l}}}$ in D_{p^l2}. Similar to Remark 2, $d_{p^lx} = \mathrm{wt_H}(D_{p^l2} \setminus (D_{p^l1})^{\perp})$ and $d_{p^lz} = \mathrm{wt_H}(D_{p^l1} \setminus (D_{p^l2})^{\perp})$.

In Theorem 4, as $\mathcal{Q}_{p^m} \subset \mathcal{Q}_{p^{l_2}} \subset \mathcal{Q}_{p^{l_1}} \subset \mathcal{Q}_p$, we obtain $\mathrm{rate}(\mathcal{Q}_{p^m}) \leq \mathrm{rate}(\mathcal{Q}_{p^{l_2}}) \leq \mathrm{rate}(\mathcal{Q}_{p^{l_1}}) \leq \mathrm{rate}(\mathcal{Q}_p)$. We note that d_{p^lx} and d_{p^lz} determine the error detection and correction capability of the code $\mathcal{Q}_{p^l}$ and $d_{px} \leq d_{p^{l_1}x} \leq d_{p^{l_2}x} \leq d_{p^mx}$, and $d_{pz} \leq d_{p^{l_1}z} \leq d_{p^{l_2}z} \leq d_{p^mz}$. Thus, there is a tradeoff between better error detection and correction capability and higher coding rate.

Remark 8: We note that the code $\mathcal{Q}_{p^l}$ can be constructed by using $r = p^l$, $C_1 = D_{p^l2}$, and $C_2 = D_{p^l1}$, in [6, Th. 3.4]. Thus, the class of codes $\mathcal{Q}_{p^l}$ obtained from ls that divide m are a special class of CSS-like codes. As $\mathbb{F}_{p^l}$-linear CSS-like codes are obtained from codes D_{p^l1} and D_{p^l2}, which are subfield-linear (linear over $\mathbb{F}_{p^l}$), they can also be called subfield-linear CSS-like codes.

When $l = 1$, the CSS-like code is the $\mathbb{F}_p$-linear CSS code discussed in Section III-B. When $l = m$, the CSS-like code is the $\mathbb{F}_{p^m}$-linear CSS codes discussed in Section III-A.

B. NORMAL BASIS BASED CSS-LIKE CODES

We next discuss the class of qudit stabilizer codes obtained by varying the number of scaled versions of H_{d1} and H_{d2} in the check matrix, where the coefficients in the scaled versions are from the normal basis $\{1, \alpha, \ldots, \alpha^{m-1}\}$ of the extension field $\mathbb{F}_{p^m}$ over the primitive field $\mathbb{F}_p$. Let $\mathcal{Q}^{(v)}$ be the qudit stabilizer code with the following check matrix:

$$\mathcal{H}^{(v)} = \left[\begin{array}{c|c} H_{d1} & \\ \alpha H_{d1} & \\ \vdots & \mathbf{0} \\ \alpha^{v-1}H_{d1} & \\ & H_{d2} \\ \mathbf{0} & \alpha H_{d2} \\ & \vdots \\ & \alpha^{v-1}H_{d2} \end{array}\right]. \tag{42}$$

As each row of $\mathcal{H}^{(v)}$ is also a row of the check matrix $\mathcal{H}_{\mathrm{CSS}}$, the stabilizer group corresponding to $\mathcal{H}^{(v)}$ is a subgroup of the stabilizer group of the corresponding $\mathbb{F}_{p^m}$-linear code.

Let $d_x^{(v)}$ and $d_z^{(v)}$ be the X-distance and Z-distance of the quantum code $\mathcal{Q}^{(v)}$. As the number of minimal stabilizer generators in the check matrix $\mathcal{H}^{(v)}$ is $v(2n - k_1 - k_2)$, $\mathcal{Q}^{(v)}$ is a $((n, p^{(m-2v)n+v(k_1+k_2)}, d_z^{(v)}/d_x^{(v)}))_{p^m}$-stabilizer code.

We discuss the distances $d_z^{(v)}$ and $d_x^{(v)}$ of the code and other properties in Theorem 5. For $i = \{1, 2\}$, let $D_i^{(v)}$ be the $\mathbb{F}_p$-linear space that contains all vectors $\boldsymbol{b} \in \mathbb{F}_{p^m}^n$ that satisfies $\mathcal{T}(\alpha^y H_{di}\boldsymbol{b}^{\mathrm{T}}) = 0$ for all $y \in \{0, 1, \ldots, v-1\}$.

Theorem 5: Let D_1 and D_2 be two classical codes over $\mathbb{F}_{p^m}$ of length n with parity check matrices H_{d1} and H_{d2}. Then, the following conditions hold.

1) $d_x^{(v)}$ and $d_z^{(v)}$ of $\mathcal{Q}^{(v)}$ corresponding to the check matrix $\mathcal{H}_v$ satisfies $d_z^{(v)} \geq o_1$ and $d_x^{(v)} \geq o_2$ and saturates both the inequalities simultaneously if and only if the code is a nondegenerate code, where o_1 and o_2 are the minimum distances of the $D_1^{(v)}$ and $D_2^{(v)}$, respectively.
2) $\mathcal{Q}^{(m)} \subset \mathcal{Q}^{(m-1)} \subset \cdots \subset \mathcal{Q}_1$, $d_x^{(1)} \leq d_x^{(2)} \leq \cdots \leq d_x^{(m)}$, and $d_z^{(1)} \leq d_z^{(2)} \leq \cdots \leq d_z^{(m)}$.

Proof: Let us consider an element $[\boldsymbol{h_x}|\boldsymbol{h_z}]$ from $\mathcal{N}_S$. Then, the symplectic product of $[\boldsymbol{h_x}|\boldsymbol{h_z}]$ with each minimal stabilizer generator is 0, i.e.,

$$\mathcal{T}\left(\mathcal{H}^{(v)}\begin{bmatrix}\boldsymbol{h_z}^{\mathrm{T}}\\ \hline \boldsymbol{h_x}^{\mathrm{T}}\end{bmatrix}\right)=\mathbf{0}$$

$$\Rightarrow \mathcal{T}\left(\left[\begin{array}{c|c} H_{d1} & \\ \alpha H_{d1} & \\ \vdots & \mathbf{0} \\ \alpha^{v-1}H_{d1} & \\ & H_{d2} \\ & \alpha H_{d2} \\ \mathbf{0} & \vdots \\ & \alpha^{v-1}H_{d2}\end{array}\right]\begin{bmatrix}\boldsymbol{h_z}^{\mathrm{T}}\\ \hline \boldsymbol{h_x}^{\mathrm{T}}\end{bmatrix}\right)=\mathbf{0}$$

$$\Rightarrow \mathcal{T}\left(\left[\begin{array}{c} H_{d1}\boldsymbol{h_z}^{\mathrm{T}} \\ \alpha H_{d1}\boldsymbol{h_z}^{\mathrm{T}} \\ \vdots \\ \alpha^{v-1}H_{d1}\boldsymbol{h_z}^{\mathrm{T}} \\ \hline H_{d2}\boldsymbol{h_x}^{\mathrm{T}} \\ \alpha H_{d2}\boldsymbol{h_x}^{\mathrm{T}} \\ \vdots \\ \alpha^{v-1}H_{d2}\boldsymbol{h_x}^{\mathrm{T}}\end{array}\right]\right)=\mathbf{0}$$

$$\Rightarrow \mathcal{T}(\alpha^y H_{d1}\boldsymbol{h_z}^{\mathrm{T}})=\mathbf{0} \text{ and } \mathcal{T}(\alpha^y H_{d2}\boldsymbol{h_x}^{\mathrm{T}})=\mathbf{0} \tag{43}$$

for all $y \in \{0, 1, \ldots, v-1\}$. Thus, $\boldsymbol{h_z} \in D_1^{(v)}$ and $\boldsymbol{h_x} \in D_2^{(v)}$. Let o_1 and o_2 be the minimum distances of $D_1^{(v)}$ and $D_2^{(v)}$, respectively. Similar to the proofs of Theorems 2 and 3, it can be proved that $d_x^{(v)}$ and $d_z^{(v)}$ of $\mathcal{Q}^{(v)}$ corresponding to the check matrix $\mathcal{H}^{(v)}$ satisfy $d_z^{(v)} \geq o_1$ and $d_x^{(v)} \geq o_2$ and saturate both the inequalities simultaneously if and only if the code is a nondegenerate code.

Similar to proof of Theorem 4, it can be proved that $\mathcal{Q}^{(m)} \subset \mathcal{Q}^{(m-1)} \subset \cdots \subset \mathcal{Q}_1$, $d_x^{(1)} \leq d_x^{(2)} \leq \cdots \leq d_x^{(m)}$, and $d_z^{(1)} \leq d_z^{(2)} \leq \cdots \leq d_z^{(m)}$. ■

In Theorem 5, as $\mathcal{Q}^{(m)} \subset \mathcal{Q}^{(m-1)} \subset \cdots \subset \mathcal{Q}^{(1)}$, we obtain $\text{rate}(\mathcal{Q}^{(m)}) \leq \text{rate}(\mathcal{Q}^{(m-1)}) \leq \cdots \leq \text{rate}(\mathcal{Q}^{(1)})$. As $d_x^{(v)}$ and $d_z^{(v)}$ determine the error detection and correction capability of the code $\mathcal{Q}^{(v)}$, $d_x^{(1)} \leq d_x^{(2)} \leq \cdots \leq d_x^{(m)}$, and $d_z^{(1)} \leq d_z^{(2)} \leq \cdots \leq d_z^{(m)}$, there is a tradeoff between better error detection and correction capability and higher coding rate.

Remark 9: We note that the code $\mathcal{Q}^{(v)}$ can be constructed by using $r = p$, $C_1 = D_2^{(v)}$, and $C_2 = D_1^{(v)}$, in [6, Th. 3.4]. Thus, the class of codes $\mathcal{Q}^{(v)}$ obtained are a special class of CSS-like codes.

When $v = 1$, the code is the $\mathbb{F}_p$-linear CSS code discussed in Section III-B. When $v = m$, the CSS-like code is the $\mathbb{F}_{p^m}$-linear CSS codes discussed in Section III-A.

TABLE IV. Elements of $\mathbb{F}_{16}$ With Primitive Element α and Primitive Polynomial $p(x) = x^4 + x + 1$

Element	Expansion	$\mathrm{Tr}_{16/2}$	$\mathrm{Tr}_{16/4}$
0	0	0	0
1	1	0	0
α	α	0	1
α^2	α^2	0	1
α^3	α^3	1	3
α^4	$1+\alpha$	0	1
α^5	$\alpha+\alpha^2$	0	0
α^6	$\alpha^2+\alpha^3$	1	2
α^7	$1+\alpha+\alpha^3$	1	2
α^8	$1+\alpha^2$	0	1
α^9	$\alpha+\alpha^3$	1	2
α^{10}	$1+\alpha+\alpha^2$	0	0
α^{11}	$\alpha+\alpha^2+\alpha^3$	1	3
α^{12}	$1+\alpha+\alpha^2+\alpha^3$	1	3
α^{13}	$1+\alpha^2+\alpha^3$	1	2
α^{14}	$1+\alpha^3$	1	3

C. EXAMPLE

In this section, through an example, we demonstrate that the codes proposed in this section are useful as it might not be possible to construct useful $\mathbb{F}_{p^m}$-linear CSS codes and $\mathbb{F}_p$-linear codes as they might have zero rate and poor error detection and correction capability, respectively.

Example 4: In this example, we consider two classical codes $D_1[5, 2, 4]$ and $D_2[5, 3, 3]$ over $\mathbb{F}_{16}$ with parity check matrices H_{d1} and H_{d2} as follows:

$$H_{d1}=\begin{bmatrix}\alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10}\\ \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3\\ \alpha^{12} & \alpha & \alpha^5 & \alpha^9 & \alpha^{13}\end{bmatrix} \tag{44}$$

$$H_{d2}=\begin{bmatrix}\alpha^{13} & \alpha^{14} & \alpha^4 & \alpha^6 & 1\\ \alpha^2 & \alpha^2 & \alpha^9 & \alpha^{13} & \alpha^6\end{bmatrix} \tag{45}$$

where α is the primitive element of $\mathbb{F}_{16}$. We note that D_1 is an RS code. The elements of $\mathbb{F}_{16}$ are provided in Table IV . Based on Table IV, we note that $H_{d1}H_{d2}^{\mathrm{T}} = 0$ and $D_1^{\perp} \subset D_2$.

As $p = 2$ and $m = 4$, we note that only $l = 2$ divides m. We obtain $z = (p^m - 1)/(p^l - 1) = 15/3 = 5$ and $\zeta = \alpha^z = \alpha^5$. Thus, the primitive element of the subfield $\mathbb{F}_4$ is $\zeta = \alpha^5$ and $\mathbb{F}_4 = \{0, 1, \zeta, \zeta^2\}$.

Using H_{d1} and H_{d2}, we construct the following quantum codes.

1) The $\mathbb{F}_{p^m}$-linear CSS code $\mathcal{Q}_{\text{CSS}}$ with check matrix $\mathcal{H}_{\text{CSS}}$ from (14): $\mathcal{Q}_{\text{CSS}}$ is a $[[5, 0, 4/3]]$ code with rate 0. As the rate is 0, the code is not useful as it consists of only one basis codeword and the distances d_{cx} and d_{cz} do not matter. We note that $\mathcal{Q}_{\text{CSS}} = \mathcal{Q}_{p^4} = \mathcal{Q}^{(4)}$.
2) The $\mathbb{F}_p$-linear CSS code $\mathcal{Q}_{\text{pCSS}}$ with check matrix $\mathcal{H}_{\text{pCSS}}$ from (18): $\mathcal{Q}_{\text{pCSS}}$ is a $((5, 2^{15}, 1/1))$ code with rate $1/2^5$. As $d_{px} = d_{pz} = 1$, the code is not useful as it cannot detect or correct any error. We note that $\mathcal{Q}_{\text{pCSS}} = \mathcal{Q}_p = \mathcal{Q}^{(1)}$.
3) The CSS-like code $\mathcal{Q}_{p^2}$ with check matrix $\mathcal{H}_{p^2}$ from (40): $\mathcal{Q}_{p^2}$ is a $((5, 2^{10}, 2/2))$ with rate $1/2^{10}$. As

TABLE V. CSS-Like Codes From D_1 and D_2

Code	Rate	$\mathrm{EDC_x}$	$\mathrm{EDC_z}$	$\mathrm{ECC_x}$	$\mathrm{ECC_z}$
$\mathcal{Q}_{p^4}$	0	-	-	-	-
$\mathcal{Q}_{p^2}$	$1/2^{10}$	1	1	0	0
$\mathcal{Q}_p$	$1/2^5$	0	0	0	0

TABLE VI. Quantum Codes $\mathcal{Q}^{(v)}$ Obtained From D_1 and D_2

Code	Rate	$\mathrm{EDC_x}$	$\mathrm{EDC_z}$	$\mathrm{ECC_x}$	$\mathrm{ECC_z}$
$\mathcal{Q}^{(4)}$	0	-	-	-	-
$\mathcal{Q}^{(3)}$	$1/2^{15}$	1	2	0	1
$\mathcal{Q}^{(2)}$	$1/2^{10}$	0	1	0	0
$\mathcal{Q}^{(1)}$	$1/2^5$	0	0	0	0

$d_{p^2x} = d_{p^2z} = 2$, the code can detect one qudit error but cannot correct any error.

4) The code $\mathcal{Q}^{(2)}$ with check matrix $\mathcal{H}^{(2)}$ from (42) with $v = 2$: $\mathcal{Q}^{(2)}$ is a $((5, 2^{10}, 2/1))$ code with rate $1/2^{10}$. As the $d_x^{(2)} = 1$ and $d_z^{(2)} = 2$, the code can detect one qudit $\mathrm{Z}^{(p^m)}(\cdot)$ errors but cannot detect any $\mathrm{X}^{(p^m)}(\cdot)$ error or correct any error.
5) The code $\mathcal{Q}^{(3)}$ with check matrix $\mathcal{H}^{(3)}$ from (42) with $v = 3$: $\mathcal{Q}^{(3)}$ is a $((5, 2^5, 3/2))$ code with rate $1/2^{15}$. As the $d_x^{(3)} = 2$ and $d_z^{(3)} = 3$, the code can detect any error E with $\mathrm{wt_X}(E) \leq 1$ and $\mathrm{wt_Z}(E) \leq 2$ and can correct one qudit $\mathrm{Z}^{(p^m)}(\cdot)$ errors, but cannot correct $\mathrm{X}^{(p^m)}(\cdot)$ errors.

From Theorems 3–5, we note that, the codes $\mathcal{Q}_{\mathrm{pCSS}}$, $\mathcal{Q}_{p^2}$, $\mathcal{Q}^{(2)}$, and $\mathcal{Q}^{(3)}$ are all nondegenerate codes. Let $\mathrm{EDC_x}$, $\mathrm{EDC_z}$, $\mathrm{ECC_x}$, and $\mathrm{ECC_z}$ be the error detection and correction capabilities of the quantum code for $\mathrm{X}^{(p^m)}(\cdot)$ and $\mathrm{Z}^{(p^m)}(\cdot)$ errors, respectively. In Tables V and VI , we list the error detection and correction capabilities and the coding rates of the quantum codes obtained from D_1 and D_2 using the constructions in Sections IV-A and IV-B, respectively.

From Tables V and VI, we note that the rate of the code increases and the error detection and correction capability decreases as the value of l in p^l and the value of v decreases. Thus, there is a tradeoff between the coding rate and the error detection and correction capability of the code. The code design and geometry can depend on the application based on the generic framework discussed in this Section. In this article, we constructed the quantum codes using RS codes, which are efficient codes, and a few codes of short length. The design of longer length codes with larger minimum distances for particular applications could be obtained using computational searches using computer algebra systems, that is beyond the scope of this article.

D. LOWER BOUND ON THE DISTANCES OF $\mathbb{F}_{p^l}$-LINEAR CSS-LIKE CODES AND NORMAL BASIS BASED CSS-LIKE CODES

We next provide a lower bound on the minimum distance of $\mathbb{F}_{p^l}$-linear CSS-like codes and normal basis based CSS-like codes provided in Sections IV-A and IV-B.

We note that quantum codes $\mathcal{Q}_p$ and $\mathcal{Q}^{(1)}$ are both equal to the $\mathbb{F}_p$-linear CSS code $\mathcal{Q}_{\mathrm{pCSS}}$. Thus, the X-distance $d_x^{(1)}$ and Z-distance $d_z^{(1)}$ of $\mathcal{Q}^{(1)}$ are equal to the X-distance d_{px} and Z-distance d_{pz} of the $\mathbb{F}_p$-linear CSS codes, respectively.

Let y_1 and y_2 be the minimum distances of D_{Hd1} and D_{Hd2}, respectively. From Theorems 4 and 5, the X-distance d_{px} and Z-distance d_{pz} are lower bounds on the X-distances and Z-distances of $\mathbb{F}_{p^l}$-linear CSS-like codes $\mathcal{Q}_{p^l}$ and normal basis based CSS-like codes $\mathcal{Q}^{(v)}$, respectively. Thus, from Theorem 3, y_1 and y_2 are lower bounds on the X-distances and Z-distances of $\mathbb{F}_{p^l}$-linear CSS-like codes $\mathcal{Q}_{p^l}$ and normal basis based CSS-like codes $\mathcal{Q}^{(v)}$, respectively.

We next provide a technique to compute y_1 and y_2 from the matrices H_{d1} and H_{d2}. For $i \in \{1, 2\}$, as y_i is the minimum distance of D_{Hdi}, it corresponds to the minimum weight of the vectors $\boldsymbol{v} \in \mathbb{F}_{p^m}^n$ that satisfy $\mathcal{T}(H_{di}\boldsymbol{v}^{\mathrm{T}}) = \boldsymbol{0}$. As H_{di} has $\rho_i = n - k_i$ rows, $\mathcal{T}(H_{di}\boldsymbol{v}^{\mathrm{T}}) = \boldsymbol{0}$ corresponds to ρ_i $\mathbb{F}_p$-linear constraints (as $\mathcal{T}$ is based on $\mathrm{Tr}_{p^m/p}$, which is $\mathbb{F}_p$-linear).

Let $\boldsymbol{g}$ be a row of H_{di}. Let $\boldsymbol{v} = [v_j]_{j=1}^n$ and $\boldsymbol{g} = [g_j]_{j=1}^n$. Let the expansion of g_j in the normal basis $\{1, \alpha, \ldots, \alpha^{m-1}\}$ be $g_j = \sum_{t=0}^{m-1} g_{jt}\alpha^t$, where $g_{jt} \in \mathbb{F}_p$. We note that

$$\begin{aligned}\mathrm{Tr}_{p^m/p}(\boldsymbol{g}\boldsymbol{v}^{\mathrm{T}}) &= \mathrm{Tr}_{p^m/p}\left(\sum_{j=1}^{n} v_j g_j\right)\\ &= \mathrm{Tr}_{p^m/p}\left(\sum_{j=1}^{n}\sum_{t=0}^{m-1} g_{jt} v_j \alpha^t\right)\\ &= \sum_{j=1}^{n}\sum_{t=0}^{m-1} g_{jt}\mathrm{Tr}_{p^m/p}(v_j\alpha^t). \qquad (46)\end{aligned}$$

Thus, the trace inner product $\mathrm{Tr}_{p^m/p}(\boldsymbol{g}\boldsymbol{v}^{\mathrm{T}})$ of $\boldsymbol{g}$ and $\boldsymbol{v}$ is equal to the Euclidean inner product between the vector $[g_{jt}]_{(j,t)=(1,0)}^{(n,m-1)}$ and the vector $[\mathrm{Tr}_{p^m/p}(v_j\alpha^t)]_{(j,t)=(1,0)}^{(n,m-1)}$.

We note that the vector $[g_{jt}]_{(j,t)=(1,0)}^{(n,m-1)}$ is obtained by replacing each element g_j in $\boldsymbol{g}$ by its normal basis based isomorphic equivalent $[g_{jt}]_{t=0}^{m-1}$. We note that the vector $[\mathrm{Tr}_{p^m/p}(v_j\alpha^t)]_{(j,t)=(1,0)}^{(n,m-1)}$ is obtained by replacing each element v_j in $\boldsymbol{v}$ by its trace based isomorphic equivalent $[\mathrm{Tr}_{p^m/p}(v_j)\alpha^t)]_{t=0}^{m-1}$. It has been shown in [22] that v_j has a one-to-one and onto relation with $[\mathrm{Tr}_{p^m/p}(v_j\alpha^t)]_{t=0}^{m-1}$. Thus, we note that the constraints $\mathcal{T}(H_{di}\boldsymbol{v}^{\mathrm{T}}) = \boldsymbol{0}$ correspond to ρ_i constraints on the $\mathbb{F}_p^{mn}$.

Let the number of nonzero elements of the least weight vector $\boldsymbol{v}$ satisfying $\mathcal{T}(H_{di}\boldsymbol{v}^{\mathrm{T}}) = \boldsymbol{0}$ be z. Let $r_1, r_2, \ldots, r_z$ be the indices of the nonzero elements of $\boldsymbol{v}$. Let H_{zdi} and $\boldsymbol{v_z}$ be the matrix and the vector obtained from H_{di} and $\boldsymbol{v}$ by considering the columns with indices $r_1, r_2, \ldots, r_z$. Then, $\boldsymbol{v_z}$ satisfies $\mathcal{T}(H_{zdi}\boldsymbol{v_z}^{\mathrm{T}}) = \boldsymbol{0}$.

We note that $\mathcal{T}(H_{zdi}\boldsymbol{v_z}^{\mathrm{T}}) = \boldsymbol{0}$ corresponds to at most ρ_i constraints on $\mathbb{F}_p^{mn}$. If these ρ_i constraints are $\mathbb{F}_p$-linearly independent, then the number of possible solutions for

TABLE VII. Representation of Elements of $\mathbb{F}_4$ Over $\mathbb{F}_2$

β	$b_1\alpha + b_0$	$[b_1\ b_0]$	$[\mathrm{Tr}_{4/2}(\alpha\beta)\ \mathrm{Tr}_{4/2}(\beta)]$
0	0	[0 0]	[0 0]
1	1	[0 1]	[1 0]
α	α	[1 0]	[1 1]
α^2	$\alpha+1$	[1 1]	[0 1]

$\mathcal{T}(H_{zdi}\boldsymbol{v_z}^{\mathrm{T}}) = \mathbf{0}$ is $p^{mz-\rho_i}$ [21], [22]. If these ρ_i constraints are not $\mathbb{F}_p$-linearly independent, then the number of possible solutions for $\mathcal{T}(H_{zdi}\boldsymbol{v_z}^{\mathrm{T}}) = \mathbf{0}$ is $p^{mz-\mathrm{rank}_p(H_{zdi})}$, where $\mathrm{rank}_p(\cdot)$ corresponds to the rank of the matrix over $\mathbb{F}_p$ [21], [22].

We note that $\boldsymbol{v_z} = \mathbf{0}$ is a trivial solution for $\mathcal{T}(H_{zdi}\boldsymbol{v_z}^{\mathrm{T}}) = \mathbf{0}$. If $mz - \mathrm{rank}_p(H_{zdi}) \leq 0$, then there are no nontrivial solutions for $\mathcal{T}(H_{zdi}\boldsymbol{v_z}^{\mathrm{T}}) = \mathbf{0}$. Thus, $mz - \mathrm{rank}_p(H_{zdi})$ should be greater than 0 for a nonzero vector $\boldsymbol{v}$ of weight z to exist such that $\mathcal{T}(H_{di}\boldsymbol{v}^{\mathrm{T}}) = \mathbf{0}$. Thus, a nonzero vector $\boldsymbol{v}$ of weight z exists in D_{Hdi} if and only if there exists a submatrix of H_{di} with z columns (containing all rows of the columns) that satisfy $mz - \mathrm{rank}_p(H_{\mathrm{zdi}}) > 0$. Thus, the minimum distance y_i is obtained as the number of columns z of the smallest submatrix of H_{di} containing all ρ_i rows and that satisfies $\mathrm{rank}_p(H_{\mathrm{zdi}}) < mz$. The distances of the $\mathbb{F}_{p^l}$-linear CSS-like codes and normal basis based CSS-like codes are greater than or equal to the respective y_is. We will use this result to next construct $\mathbb{F}_p$-linear CSS codes over qudits of dimension $\mathbb{F}_{p^m}$ from classical codes over $\mathbb{F}_p$ with good distances.

E. CONSTRUCTION OF QUANTUM CODES OVER EXTENSION FIELD FROM CLASSICAL CODES OVER PRIMITIVE FIELD

We next provide a procedure to construct $\mathbb{F}_p$-linear CSS codes over an extension field $\mathbb{F}_{p^m}$ from classical codes over the primitive field $\mathbb{F}_p$ that satisfy the dual-containing criteria.

Let us consider two classical codes $C_1[mn, k_{1p}, d_{1p}]$ and $C_2[mn, k_{2p}, d_{2p}]$ over $\mathbb{F}_p$ with parity check matrices P_1 and P_2. We provide a procedure to construct $\mathbb{F}_p$-linear CSS codes, $\mathbb{F}_{p^l}$-linear CSS codes (l divides m), $\mathbb{F}_{p^m}$-linear CSS codes, and normal basis based CSS-like codes. We show that a lower bound on the Z-distances and X-distances of all these codes are $\lfloor (d_{1p}-1)/m \rfloor + 1$ and $\lfloor (d_{2p}-1)/m \rfloor + 1$, respectively.

The idea of the construction procedure is as follows: As $C_1^{\perp} \subset C_2$, we obtain $P_1 P_2^{\mathrm{T}} = \mathbf{0}$. We recall from Section IV-D that the inner product between two vector $\boldsymbol{g}$ and $\boldsymbol{v}$ over $\mathbb{F}_{p^m}^n$ is equal to the inner product between two vectors $[g_{jt}]_{(j,t)=(1,0)}^{(n,m-1)}$ and the vector $[\mathrm{Tr}_{p^m/p}(v_j\alpha^t)]_{(j,t)=(1,0)}^{(n,m-1)}$. The vectors $[g_{jt}]_{(j,t)=(1,0)}^{(n,m-1)}$ and $[\mathrm{Tr}_{p^m/p}(v_j\alpha^t)]_{(j,t)=(1,0)}^{(n,m-1)}$ belong to $\mathbb{F}_p^{mn}$ and were obtained by replacing the element in $\boldsymbol{g}$ and $\boldsymbol{v}$ by their corresponding isomorphic equivalents over $\mathbb{F}_p$. In Table VII, we provide the two isomorphic equivalents for elements of $\mathbb{F}_4$ over $\mathbb{F}_2$.

Considering the equivalence between the trace inner product over $\mathbb{F}_4$ and the Euclidean inner product over $\mathbb{F}_2$, we obtain the matrices H_{d1} and H_{d2} by replacing m length vectors in P_1 and P_2 by their normal basis based isomorphic equivalent and trace based isomorphic equivalent along the rows, respectively. For example, if we consider

$$P_1 = P_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{47}$$

then, H_{d1} and H_{d2} are obtained as

$$H_{d1} = \begin{bmatrix} \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 \\ 1 & 1 & 1 & 1 \\ 0 & \alpha^2 & 0 & \alpha^2 \\ 0 & 1 & 0 & 1 \end{bmatrix} \text{ and } H_{d2} = \begin{bmatrix} \alpha & \alpha & \alpha & \alpha \\ \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 \\ 0 & \alpha & 0 & \alpha \\ 0 & \alpha^2 & 0 & \alpha^2 \end{bmatrix}. \tag{48}$$

As $P_1 P_2^{\mathrm{T}} = \mathbf{0}$ and due to the equivalence between the trace inner product over $\mathbb{F}_4$ and Euclidean inner product over $\mathbb{F}_2$, we obtain $\mathcal{T}(H_{d1}H_{d2}^{\mathrm{T}}) = \mathbf{0}$. Thus, the codes D_{Hd1} and D_{Hd2} obtained from H_{d1} and H_{d2} satisfy $D_{Hd1}^{\perp_{\mathrm{Tr}_{p^m/p}}} \subset D_{Hd2}$ and an $\mathbb{F}_p$-linear CSS code can be obtained. Thus, from H_{d1} and H_{d2}, an $\mathbb{F}_{p^l}$-linear CSS cods, an $\mathbb{F}_{p^m}$-linear CSS code, and a normal basis based CSS-like code can also be obtained.

For $i \in \{1, 2\}$, as the minimum distance of C_i is d_{ip}, any $(d_{ip}-1)$ columns of P_i are linearly independent. We note that z columns of H_{di} is equivalent to mz columns of P_i. As any $(d_{ip}-1)$ columns of P_i are linearly independent, any submatrix H_{zdi} containing $z \leq \lfloor (d_{ip}-1)/m \rfloor$ columns of H_{di} (with all rows) has mz $\mathbb{F}_p$-linearly independent rows. Thus, when $z \leq \lfloor (d_{ip}-1)/m \rfloor$, $\mathrm{rank}_p(H_{zdi}) = mz$, which is not less than mz. Thus, the minimum distance y_i is greater than $\lfloor (d_{ip}-1)/m \rfloor$; hence, $y_i \geq \lfloor (d_{ip}-1)/m \rfloor + 1$. Thus, from a classical binary code over $\mathbb{F}_p$ of length mn, we obtain an $\mathbb{F}_p$-linear CSS code over $\mathbb{F}_{p^m}$ of length n with Z-distance and X-distance satisfying $d_{pz} \geq \lfloor (d_{1p}-1)/m \rfloor + 1$ and $d_{px} \geq \lfloor (d_{2p}-1)/m \rfloor + 1$. From Theorems 4 and 5, the Z-distances and X-distances of $\mathbb{F}_{p^l}$-linear CSS-like codes $\mathcal{Q}_{p^l}$ and normal basis based CSS-like codes $\mathcal{Q}^{(v)}$ are at least $\lfloor (d_{1p}-1)/m \rfloor + 1$ and $\lfloor (d_{2p}-1)/m \rfloor + 1$, respectively.

We summarize the procedure to obtain the $\mathbb{F}_p$-linear CSS code from classical code over $\mathbb{F}_p$ in Algorithm 1.

Remark 10: We note that the procedure provided in Algorithm 1 can be used to construct quantum codes over qudits of dimension $\mathbb{F}_{p^m}$ from classical codes over $\mathbb{F}_{p^l}$ similarly.

Remark 11: We note that the matrices H_{d1} and H_{d2} obtained from P_1 and P_2 are full rank matrices with respect to $\mathbb{F}_p$ when P_1 and P_2 have full rank. However, H_{d1} and H_{d2} may not be full rank matrices with respect to $\mathbb{F}_{p^m}$. For example, from (47) to (48), $\mathrm{rank}_2(P_1) = \mathrm{rank}_2(P_2) = \mathrm{rank}_2(H_{d1}) = \mathrm{rank}_2(H_{d2}) = 4$. However, $\mathrm{rank}_4(H_{d1}) = \mathrm{rank}_4(H_{d2}) = 2$. We note that, in such cases, the $\mathbb{F}_p$-linear CSS code could be equal to the $\mathbb{F}_{p^l}$-linear CSS-like codes or the normal basis based CSS-like codes.

We use the procedure provided in Algorithm 1 with the Reed–Muller (RM) codes $\mathrm{RM}_2(3, 6)$ and $\mathrm{RM}_2(4, 7)$, which are both dual-containing codes [16, Ch. 4]. The RM codes $\mathrm{RM}_2(3, 6)$ and $\mathrm{RM}_2(4, 7)$ are [64,42,8] and [128, 99, 8]

Algorithm 1: Procedure to Obtain $\mathbb{F}_p$-Linear CSS Code Over $\mathbb{F}_{p^m}$ From Classical Codes Over $\mathbb{F}_p$.

Input: Check matrices P_1 and P_2 of classical codes $C_1[mn, k_{1p}, d_{1p}]$ and $C_2[mn, k_{2p}, d_{2p}]$ that satisfy $C_1^{\perp} \subset C_2$.
Output: $\mathbb{F}_p$-linear CSS code $\mathcal{Q}_{\text{pCSS}}$
Procedure:
Step 1: Replace each m length vector in the rows of P_1 by their normal basis based isomorphic equivalent to obtain H_{d1}. Replace each m length vector in the rows of P_2 by their trace based isomorphic equivalent to obtain H_{d2}.
Step 2: Construct the $\mathbb{F}_p$-linear CSS code using the matrices H_{d1} and H_{d2} using the construction provided in Section III-B. The Z-distance and X-distance of $\mathbb{F}_p$-linear CSS code satisfy $d_{pz} \geq \lfloor (d_{1p} - 1)/m \rfloor + 1$ and $d_{px} \geq \lfloor (d_{2p} - 1)/m \rfloor + 1$.

classical binary codes, respectively. Using the procedure in Algorithm 1 with the parity check matrix[5] of $\text{RM}_2(3, 6)$, we obtain an $[[32, 10, d_{pz} \geq 4/d_{px} \geq 4]]$ quantum code. Using the procedure in Algorithm 1 with the parity check matrix of $\text{RM}_2(4, 7)$, we obtain an $[[64, 35, d_{pz} \geq 4/d_{px} \geq 4]]$ quantum code.

Similar quantum codes of larger distances can be obtained from classical RM codes. Binary classical RM codes $\text{RM}_2(r, m)$ are $[2^m, \sum_{i=0}^{r}\binom{m}{i}, 2^{m-r}]$ codes. When $r \geq (m-1)/2$, the RM codes are dual-containing codes. The distances of $\mathbb{F}_{p^l}$-linear CSS-like codes $\mathcal{Q}_{p^l}$ and normal basis based CSS-like codes $\mathcal{Q}^{(v)}$ obtained from these dual-containing classical RM codes are at least $\lfloor (2^{m-r} - 1)/m \rfloor + 1$.

V. CONCLUSION

We developed a theory towards the construction of quantum codes from dual containing codes over $\mathbb{F}_{p^m}$. We showed that the generalization of the CSS coding framework over qubits to qudits yielded two different classes of quantum codes, and we studied their properties. We proposed the check matrix of the $\mathbb{F}_{p^m}$-linear CSS codes and studied the distance properties. We further proposed two classes of quantum codes based on the classical codes that satisfy the dual-containing criterion and studied the tradeoff between higher coding rate and better error detection and correction capability within each class, useful for applications requiring the same.

We also provided a method to compute a lower bound of the distances of the proposed codes. We finally provided a method to construct quantum codes over an extension field from classical codes over primitive field and provided a lower bound on the distances of the proposed quantum code based on the minimum distances of the classical codes. We view the study of $\mathbb{F}_p$-linear and $\mathbb{F}_{p^m}$-linear CSS codes based on qudit toric codes [23] as a future direction of research, useful for topological error correction.

[5]The parity matrix $H_{\text{RM}}(r, m)$ of the $\text{RM}_2(r, m)$ code is obtained as the generator matrix $G_{\text{RM}}(m-r-1, m)$ of the $\text{RM}_2(m-r-1, m)$ code as $\text{RM}_2^{\perp}(r, m) = \text{RM}_2(m-r-1, m)$. The generator matrix $G_{\text{RM}}(r, m)$ of the $\text{RM}_2(r, m)$ code consists of those rows of $G_{(2^m, 2^m)} = G_{(2,2)}^{\otimes m}$ with weight greater than or equal to 2^{m-r} [16].

APPENDIX

Lemma 1: For $\beta \in \mathbb{F}_{p^m}$, $\text{Tr}_{p^m/p}(\alpha^i \beta) = 0 \quad \forall i \in \{0, 1, \ldots, m-1\}$ if and only if $\beta = 0$ [20].

Proof: When $\beta = 0$, for $i \in \{0, 1, \ldots, m-1\}$, we obtain $\text{Tr}_{p^m/p}(\alpha^i \beta) = \text{Tr}_{p^m/p}(0) = 0$.

We next prove the converse. For some $\beta \in \mathbb{F}_{p^m}$, let $\text{Tr}_{p^m/p}(\alpha^i \beta) = 0 \quad \forall i \in \{0, 1, \ldots, m-1\}$. As each element $\gamma \in \mathbb{F}_{p^m}$ can be expressed in terms of the set $\{1, \alpha, \ldots, \alpha^{m-1}\}$ [16], there exists $\gamma_0, \ldots, \gamma_{m-1} \in \mathbb{F}_p$ such that $\gamma = \sum_{i=0}^{m-1} \gamma_i \alpha^i$. Thus

$$\text{Tr}_{p^m/p}(\gamma\beta) = \text{Tr}\left(\sum_{i=0}^{m-1} \gamma_i \alpha^i \beta\right) = \sum_{i=0}^{m-1} \gamma_i \text{Tr}_{p^m/p}(\alpha^i \beta) = 0. \tag{49}$$

As β is nonzero, by the closure property of $\mathbb{F}_{p^m}$, the set $\{\gamma\beta\}_{\gamma \in \mathbb{F}_{p^m}}$ contains all the field elements. From (49), $\text{Tr}_{p^m/p}(\gamma\beta) = 0$ for every $\gamma \in \mathbb{F}_{p^m}$. As the trace of all elements of $\mathbb{F}_{p^m}$ cannot be 0, we obtain $\beta = 0$. ■

Lemma 2: For $\beta \in \mathbb{F}_{p^m}$, $\text{Tr}_{p^m/p}(\zeta^i \beta) = 0 \quad \forall i \in \{0, 1, \ldots, l-1\}$ if and only if $\text{Tr}_{p^m/p^l}(\beta) = 0$, where l divides m and ζ is the primitive element of $\mathbb{F}_{p^l}$.

Proof: For $i \in \{0, 1, \ldots, l-1\}$, we obtain

$$\text{Tr}_{p^m/p}(\zeta^i \beta) = \sum_{f=0}^{m-1} (\zeta^i \beta)^{p^f} = \sum_{f=0}^{m-1} \zeta^{ip^f} \beta^{p^f}. \tag{50}$$

As m divides l, we split the summation $\sum_{f=0}^{m-1}$ into m/l summations, i.e., $\sum_{f=0}^{m-1} = \sum_{a=0}^{(m/l)-1} \sum_{b=al}^{(a+1)l-1}$, where f is replaced by b in the summand. Replacing the summation $\sum_{f=0}^{m-1}$ in (50) with $\sum_{a=0}^{(m/l)-1} \sum_{b=al}^{(a+1)l-1}$, we obtain

$$\begin{aligned}
&\text{Tr}_{p^m/p}(\zeta^i \beta) \\
&= \sum_{a=0}^{(m/l)-1} \sum_{b=al}^{(a+1)l-1} \zeta^{ip^b} \beta^{p^b} \\
&= \sum_{a=0}^{(m/l)-1} \sum_{c=0}^{l-1} \zeta^{ip^{c+al}} \beta^{p^{c+al}}, \text{ where } c = b - al \\
&= \sum_{a=0}^{(m/l)-1} \sum_{c=0}^{l-1} \zeta^{ip^c p^{al}} \beta^{p^{c+al}} = \sum_{a=0}^{(m/l)-1} \sum_{c=0}^{l-1} (\zeta^{p^{al}})^{ip^c} \beta^{p^{c+al}} \\
&= \sum_{a=0}^{(m/l)-1} \sum_{c=0}^{l-1} \zeta^{ip^c} \beta^{p^{c+al}} = \sum_{c=0}^{l-1} \zeta^{ip^c} \sum_{a=0}^{(m/l)-1} \beta^{p^{c+al}}
\end{aligned} \tag{51}$$

for all $i \in \{0, 1, \ldots, l-1\}$, as $\zeta^l = \zeta$.

Let $\mathrm{Tr}_{p^m/p}(\zeta^i\beta) = 0$ for all $i \in \{0, 1, \ldots, l-1\}$. Then, from (51), we obtain

$$\underbrace{\begin{bmatrix} 1 & 1 & \ldots & 1 \\ \zeta & \zeta^p & \ldots & \zeta^{p^{(l-1)}} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta^{(l-1)} & \zeta^{p(l-1)} & \ldots & \zeta^{(l-1)p^{(l-1)}} \end{bmatrix}}_{A} \begin{bmatrix} \sum_{a=0}^{(m/l)-1} \beta^{p^{al}} \\ \sum_{a=0}^{(m/l)-1} \beta^{p^{1+al}} \\ \vdots \\ \sum_{a=0}^{(m/l)-1} \beta^{p^{(l-1)+al}} \end{bmatrix} = \mathbf{0}. \tag{52}$$

The matrix A is a transpose of a Vandermonde matrix; hence, A has full rank. Thus, the only vector in the null space of A is the zero vector. Thus, $\sum_{a=0}^{(m/l)-1} \beta^{p^{c+al}} = 0$ for all $c \in \{1, \ldots, l-1\}$. Thus, $\mathrm{Tr}_{p^m/p^l}(\beta) = \sum_{a=0}^{(m/l)-1} \beta^{p^{al}} = 0$.

We next prove the converse. When $\mathrm{Tr}_{p^m/p^l}(\beta) = 0$, we obtain $\sum_{a=0}^{(m/l)-1} \beta^{(p^l)^a} = 0 \Rightarrow \sum_{a=0}^{(m/l)-1} \beta^{p^{c+al}} = \beta^{p^c} \sum_{a=0}^{(m/l)-1} \beta^{(p^l)^a} = 0$, for $c \in \{0, \ldots, l-1\}$. From (51), we obtain $\mathrm{Tr}_{p^m/p}(\zeta^i\beta) = 0 \;\; \forall \;\; i \in \{0, 1, \ldots, l-1\}$ when $\mathrm{Tr}_{p^m/p^l}(\beta) = 0$. ■

REFERENCES

[1] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. dissertation, Div. Phys., Math. and Astron., California Inst. Technol., Pasadena, CA, USA, 1997.

[2] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998, doi: 10.1109/18.681315.

[3] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, no. 2, pp. 1098–1105, Aug. 1996, doi: 10.1103/PhysRevA.54.1098.

[4] A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.*, vol. 77, no. 5, pp. 793–797, Jul. 1996, doi: 10.1103/PhysRevLett.77.793.

[5] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th ed. New York, NY, USA: Cambridge Univ. Press, 2011.

[6] M. F. Ezerman, S. Jitman, S. Ling, and D. V. Pasechnik, "CSS-Like constructions of asymmetric quantum codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 10, pp. 6732–6754, Oct. 2013, doi: 10.1109/TIT.2013.2272575.

[7] P. J. Nadkarni and S. S. Garani, "Quantum error correction architecture for qudit stabilizer codes", *Phys. Rev. A*, vol. 103, no. 4, pp. 1–20, Apr. 2021, Art. no. 042420, doi: 10.1103/PhysRevA.103.042420.

[8] P. J. Nadkarni and S. S. Garani, "Encoding of nonbinary entanglement-unassisted and assisted stabilizer codes," *IEEE Trans. Quantum Eng.*, vol. 2, pp. 1–22, Jan. 2021, Art. no 2100322, doi: 10.1109/TQE.2021.3050848.

[9] P. J. Nadkarni, A. Raina, and S. S. Garani, "Modified graph-state codes for single-node recovery in quantum distributed storage,"*Phys. Rev. A*, vol. 102, pp. 1–12, Dec. 2020, Art. no. 062430, doi: 10.1103/PhysRevA.102.062430.

[10] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 4892–4914, Nov. 2006, doi: 10.1109/TIT.2006.883612.

[11] M. Grassl, L. Kong, Z. Wei, Z. Yin, and B. Zeng, "Quantum error-correcting codes for qudit amplitude damping," *IEEE Trans. Inf. Theory*, vol. 64, no. 6, pp. 4674–4685, Jun. 2018, doi: 10.1109/TIT.2018.2790423.

[12] J. Shao, L. Zhou, and Y. Sun, "Entanglement-assisted nonbinary quantum LDPC codes with finite field method," in *Proc. 13th IEEE Conf. Ind. Electron. Appl.*, Wuhan, China, Jun. 2018, pp. 99–103, doi: 10.1109/ICIEA.2018.8397697.

[13] G. G. La Guardia, R. Palazzo, and C. Lavor, "Nonbinary Quantum Reed-Solomon codes," *Int. J. Pure Appl. Math.*, vol. 65, no. 1, pp. 55–64, Jan. 2010.

[14] P. J. Nadkarni and S. S. Garani, "Coding analog of superadditivity using entanglement-assisted quantum tensor product codes over $\mathbb{F}_{p^k}$," *IEEE Trans. Quantum Eng.*, vol. 1, 2020, Art. no. 2101417, doi: 10.1109/TQE.2020.3027035.

[15] P. J. Nadkarni and S. S. Garani, "Entanglement-assisted reed-solomon codes over qudits: Theory and architecture," *Quantum Inf. Proc.*, vol. 20, no. 4, pp. 1–68, Apr. 2021, Art. no. 129, doi: 10.1007/s11128-021-03028-w.

[16] S. Lin and D. J. Costello, *Error Control Coding: Fundamentals and Applications*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1983.

[17] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 3065–3072, Nov. 2001, doi: 10.1109/18.959288.

[18] D. Lidar and T. A. Brun, *Quantum Error Correction*, Cambridge, U.K.: Cambridge Univ. Press, 2013.

[19] P. J. Nadkarni and S. S. Garani, "Encoding of quantum stabilizer codes over qudits with $d = p^m$," in *Proc. IEEE Globecom Workshops*, Abu Dhabi, Dec. 2018, pp. 1–6, doi: 10.1103/PhysRevA.103.042420.

[20] P. J. Nadkarni and S. S. Garani, "Entanglement-assisted quantum reed-solomon codes," in *Proc. IEEE Inf. Theory Appl. Workshop.*, 2019, pp. 1–10.

[21] G. Strang, *Linear Algebra and Its Applications*, 4th ed. Boston, MA, USA: Cengage, 2006.

[22] P. J. Nadkarni and S. S. Garani, "Non-binary entanglement-assisted stabilizer codes," submitted for publication.

[23] F. H. E. Watson, H. Anwar, and D. E. Browne, "Fast fault-tolerant decoder for qubit and qudit surface codes," *Phys. Rev. A*, vol. 92, no. 3, pp. 1–12, Sep. 2015, Art. no. 032309, doi: 10.1103/PhysRevA.92.032309.

Priya J. Nadkarni (Member, IEEE) received the B.E. degree in electronics and communication engineering from the B.M.S. College of Engineering, Bengaluru, India, in 2014, and the Ph.D. degree in engineering sciences from the Indian Institute of Science, Bengaluru, India.

She is currently working with Xanadu Quantum Technologies Inc., Toronto, ON, Canada, as a quantum error correction researcher (independent contractor). Her research interests include quantum error correction codes, fault-tolerant quantum computation, quantum circuit architectures, quantum algorithms, and quantum communication.

Shayan Srinivasa Garani (Senior Member, IEEE) received the B.E. degree in electronics and communication engineering from Mysore University, Mysore, India, in 1997, the M.S. degree in electrical engineering from the University of Florida, Gainesville, FL, USA, in 2001, and the Ph.D. degree in electrical and computer engineering (with a minor in mathematics) from the Georgia Institute of Technology, Atlanta, GA, USA, in 2006.

He is currently a Faculty Member with the Department of Electronic Systems Engineering, Indian Institute of Science, Bengaluru, India, where he is also the Director of the Physical Nano-Memories, Signal, and Information Processing Laboratory. He was managing the Advanced Read Channels Division, Western Digital, San Jose, CA, USA, where he was involved in advanced research and development efforts on disruptive technologies that went into products, and directing several external university research programs. He was the Chairman for the Coding and Signal Processing Group within IDEMA-ASTC and the Co-Chair for the overall technological committee. He holds 14 U.S. patents and many other patents pending in the area of physical data storage. His current research interests include the broad areas of quantum information processing, physical data storage, artificial intelligence, and music signal processing.

Dr. Garani was the Chair for the IEEE Data Storage Technical Committee from 2018 to 2020. He was a Lead Guest Editor for the 2016 IEEE Journal on Selected Areas in Communications special issue on Channel Modeling, Coding, and Signal Processing for Novel Physical Memory Devices and Systems. In 2018, he received the Prof. Satish Dhawan Award, citing outstanding contributions in the field of engineering sciences.