Quantum CSS LDPC Codes based on Dyadic Matrices for Belief Propagation-based Decoding

Quantum CSS LDPC Codes based on Dyadic Matrices for Belief Propagation-based Decoding

Alessio Baldelli†, Massimo Battaglioni†, Jonathan Mandelbaum⋆, Sisi Miao⋆, Laurent Schmalen⋆
† *Department of Information Engineering*, Università Politecnica delle Marche, Ancona 60131, Italy
Email: a.baldelli@pm.univpm.it, m.battaglioni@univpm.it
⋆ *Communications Engineering Lab (CEL)*, Karlsruhe Institute of Technology (KIT), 76187 Karlsruhe, Germany
Email: {firstname.lastname}@kit.edu

***Abstract*—Quantum low-density parity-check (QLDPC) codes provide a practical balance between error-correction capability and implementation complexity in quantum error correction (QEC). In this paper, we propose an algebraic construction based on dyadic matrices for designing both classical and quantum LDPC codes. The method first generates classical binary quasi-dyadic LDPC codes whose Tanner graphs have girth 6. It is then extended to the Calderbank–Shor–Steane (CSS) framework, where the two component parity-check matrices are built to satisfy the compatibility condition required by the recently introduced CAMEL-ensemble quaternary belief propagation decoder. This compatibility condition ensures that all unavoidable cycles of length 4 are assembled in a single variable node, allowing the mitigation of their detrimental effects by decimating that variable node.**

***Index Terms*—Quantum error correction, LDPC codes, CSS codes, QLDPC codes, ensemble decoding, quasi-dyadic codes**

I. Introduction

Quantum error correction (QEC) is a fundamental component in the realization of fault-tolerant quantum computation and communication systems. Due to the intrinsic fragility of quantum information, physical qubits are highly susceptible to noise and decoherence, making error control indispensable for reliable operation [1]–[4].

The stabilizer formalism provides a powerful algebraic framework for QEC by embedding k logical qubits into a subspace of the n–qubit Hilbert space stabilized by a set of commuting Pauli operators [5]. Within quantum stabilizer codes (QSCs), the Calderbank–Shor–Steane (CSS) code family [2], [3], [6] is widely used. In this family, the stabilizer structure decomposes into two classical binary codes (C_X, C_Z) with parity-check matrices (PCMs) $\mathbf{H}_X$ and $\mathbf{H}_Z$, respectively, satisfying the well-known *orthogonality condition* $\mathbf{H}_X\mathbf{H}_Z^\top = 0$.

Among CSS-type codes, quantum low-density parity-check (QLDPC) codes, i.e., stabilizer codes represented by a sparse PCM, have emerged as a promising class, which enables scalable and efficient belief propagation (BP) decoding, and a good trade-off between error correction capabilities and the depth of the associated quantum circuit [7]–[9]. However, classical low-density parity-check (LDPC) design principles do not directly translate into the quantum setting, where the orthogonality constraint between $\mathbf{H}_X$ and $\mathbf{H}_Z$ restricts the admissible code ensemble and complicates the elimination of short cycles in the Tanner graph [10].

Recent advances in structured QLDPC code design have focused on preserving sparsity while ensuring algebraic regularity. Notable examples include quasi-cyclic constructions [11] and codes derived from projective geometries [12]. More recently, non-binary codes employing affine permutation matrices have been explored in [13]. In [14], the Cycle Assembling and Mitigating with EnsembLe decoding (CAMEL) framework was introduced. It employs CSS codes in which all short cycles are concentrated around a single variable node, and it incorporates a decoding strategy that exploits this structure to neutralize their impact. The example codes used in [14] are based on circulant permutation matrices and finite geometries.

In this work, we extend the CAMEL design philosophy by introducing a novel construction of QLDPC codes based on dyadic matrices. Compared to the quasi-cyclic codes used in [14], the proposed construction enables the design of new codes with higher rates and good decoding performance. While dual-containing CSS LDPC codes based on dyadic matrices were recently introduced in [15], their Tanner graphs exhibit a large number of length-4 cycles throughout the PCM, which limits their decoding performance. Adapting to the CAMEL framework, the newly proposed construction overcomes this limitation by exploiting affine-row dyadic structures to control the overlap between parity-check blocks, resulting in QLDPC codes suitable for quaternary BP decoding. Moreover, we show that the same principles can be leveraged to design classical quasi-dyadic low-density parity-check (QD-LDPC) codes [16], [17] with a girth of at least 6.

The paper is organized as follows. Section II introduces the notation and background. Section III presents the proposed dyadic-matrix–based classical and quantum LDPC code constructions. Their error rate performance under ensemble BP decoding over depolarizing channels is reported in Sec. IV. Section V concludes the paper.

The work of Alessio Baldelli was partially supported by Agenzia per la Cybersicurezza Nazionale (ACN) under the programme for promotion of XL cycle PhD research in cybersecurity (CUP I32B24001750005).
This work has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No. 101001899) and the German Federal Ministry of Research, Technology and Space (BMFTR) within the project Open6GHub+ (grant agreement 16KIS2405)

II. Notation and preliminaries

We denote the set of integers between a and b, endpoints included, as $[a, b]$. Let $\mathbb{F}_{2^\ell}$ denote the finite field of order 2^ℓ, with $\ell \in \mathbb{N}$ and $\mathbb{F}_{2^\ell}^{\times} \coloneqq \mathbb{F}_{2^\ell} \setminus \{0\}$. The element-wise XOR of binary vectors is denoted by $\oplus$, and the addition in $\mathbb{F}_{2^\ell}$ is denoted by $+$. Sums and multiplications of matrices are performed over $\mathbb{F}_2$. The field $\mathbb{F}_{2^\ell}$ is constructed as $\mathbb{F}_2[x]/\langle \pi(x) \rangle$, where $\pi(x)$ is a primitive polynomial of degree ℓ, and its root α denotes a primitive element of the field. Each element of the field can be written as

$$\sum_{k=0}^{\ell-1} c_k \alpha^k, \qquad c_k \in \mathbb{F}_2.$$

Matrices are denoted by bold uppercase letters, e.g., $\mathbf{H}$, $\mathbf{P}$; row vectors are denoted by bold lowercase letters, e.g., $\mathbf{a}$. The *Hamming weight* (or *weight*) of a binary vector $\mathbf{a}$ is indicated with $|\mathbf{a}|$, and it corresponds to the number of its non-zero entries. The *support* of the vector $\mathbf{a}$ consists of the set of indices of its non-zero entries. Moreover, scalars in $\mathbb{F}_{2^\ell}$ are denoted by lowercase letters. The $m \times n$ all-zero and all-one matrices are $\mathbf{0}_{m\times n}$ and $\mathbf{1}_{m\times n}$, respectively. The transpose operator is $(\cdot)^\top$.

Given an integer $\ell \geq 1$, we define the *ring of dyadic matrices* $\mathcal{M}_\ell(\mathbb{F}_2)$ as the set of $2^\ell \times 2^\ell$ matrices with entries over $\mathbb{F}_2$, structured as follows

$$\mathbf{M} = \begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B} & \mathbf{A} \end{bmatrix}, \quad \mathbf{A}, \mathbf{B} \in \mathcal{M}_{\ell-1}(\mathbb{F}_2). \tag{1}$$

For $\ell = 0$, $\mathcal{M}_0(\mathbb{F}_2) \coloneqq \mathbb{F}_2$. For any ℓ, when equipped with standard matrix sum and multiplication, $\mathcal{M}_\ell(\mathbb{F}_2)$ forms a commutative ring. It is possible to show that any dyadic matrix is fully represented by its first row, called *signature* [18]. Let $\mathcal{D}_\ell(\mathbb{F}_2) = \{\mathbf{D}^{(0)} \coloneqq \mathbf{I}_{2^\ell \times 2^\ell}, \mathbf{D}^{(1)}, \ldots, \mathbf{D}^{(2^\ell-1)}\} \subseteq \mathcal{M}_\ell(\mathbb{F}_2)$ be the set containing all dyadic matrices whose signatures have weight 1. Then, each $\mathbf{D}^{(i)}$ is called *dyadic permutation matrix (DPM)*. Furthermore, a matrix that is built using only dyadic blocks is called *quasi-dyadic (QD)*. A code defined by a QD generator matrix or by a QD PCM is naturally called QD.

A. Classical and Quantum Codes

An $[n, k, d]$ classical binary linear code $C \subseteq \mathbb{F}_2^n$ has code length n, dimension k, and minimum Hamming distance d. The elements $\mathbf{c}$ of C are the codewords, and $d \coloneqq \min_{\mathbf{c}\in C\setminus\{\mathbf{0}\}} |\mathbf{c}|$. The code rate is defined as $R = k/n$. A code can be represented as the null space of a PCM $\mathbf{H} \in \mathbb{F}_2^{r\times n}$, such that $\mathbf{H}\mathbf{c}^\top = \mathbf{0}$, $\forall\, \mathbf{c} \in C$. The code redundancy is given by $\mathrm{rank}(\mathbf{H})$. If $\mathbf{H}$ is *sparse*, i.e., the majority of its entries are zero, then the associated code is deemed to be an LDPC code. Every PCM can be interpreted as the adjacency matrix of a bipartite Tanner graph [19], characterized by n variable nodes and r check nodes. The edges that link each other such nodes are represented by the non-zero entries in $\mathbf{H}$. A closed path in the Tanner graph is called *cycle*; we define the *girth* g to be the length of the shortest cycle in such a graph.

QSCs [4] are the quantum equivalent of classical binary linear codes. An $[\![n, k, d]\!]$ QSC $\mathcal{C} \subseteq (\mathbb{C}^2)^{\otimes n}$ is called a stabilizer code because it is stabilized by all stabilizer generators $s \in \mathcal{S}$ of the code[1]. An $[\![n, k_1 - k_2, d]\!]$ CSS code $\mathcal{C}$ is a special case of a QSC [2], [3], [6], which can be constructed as follows. Let us consider two binary classical codes C_1 and C_2 with parameters $[n, k_1, d_1]$ and $[n, k_2, d_2]$, respectively, and such that $C_2 \subseteq C_1$. Given $\mathbf{H}_X \in \mathbb{F}_2^{(n-k_1)\times n}$, and $\mathbf{H}_Z \in \mathbb{F}_2^{k_2\times n}$, which are the PCMs of C_1 and $C_2^\perp$, respectively, that satisfy the *symplectic product* (also called *orthogonality*) *condition*

$$\mathbf{H}_X\mathbf{H}_Z^\top = \mathbf{0} \quad (\text{or } \mathbf{H}_Z\mathbf{H}_X^\top = \mathbf{0}),$$

then, by using $\mathbb{F}_4 = \{0, 1, \omega \coloneqq \alpha, \bar{\omega} = \alpha^2\}$, the associated CSS code $\mathcal{C}$ is represented by the quaternary PCM

$$\begin{bmatrix} \omega\mathbf{H}_X \\ \bar{\omega}\mathbf{H}_Z \end{bmatrix}. \tag{2}$$

The minimum distance d is lower-bounded by $\min\{d_1, d_2\}$, and the rate of $\mathcal{C}$ is $R_Q = (k_1 - k_2)/n$.

B. CAMEL

Up to this day, several constructions for the binary PCMs $\mathbf{H}_X$ and $\mathbf{H}_Z$ of a CSS code guarantee a girth of at least 6 for each of the respective associated Tanner graphs [11], [13], [20]. However, when considering quaternary BP decoding, which is favorable compared to binary BP decoding because it takes correlation between X and Z errors into account, the performance may be degraded by inevitable 4-cycles in the Tanner graph of the quaternary PCM $\mathbf{H}$ [14]. The CAMEL framework introduced in [14] jointly designs the code and quaternary BP-based decoder to alleviate the harmful effect of these short cycles.

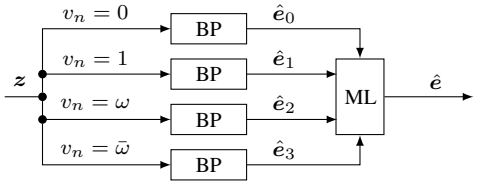

Fig. 1. Block diagram of the CAMEL decoder according to [14].

Definition 1 A CAMEL decoder and code pair consists of the ensemble decoder depicted in Fig. 1 together with a CSS code represented by binary PCMs

$$\mathbf{H}_X = \begin{pmatrix} \mathbf{H}'_X & \mathbf{1}_{r\times 1} \end{pmatrix}, \quad \mathbf{H}_Z = \begin{pmatrix} \mathbf{H}'_Z & \mathbf{1}_{r\times 1} \end{pmatrix}, \tag{3}$$

where $\mathbf{H}'_X, \mathbf{H}'_Z \in \mathbb{F}_2^{r\times n}$ and the submatrices satisfy the *CAMEL condition*

$$\mathbf{H}'_X(\mathbf{H}'_Z)^\top = \mathbf{1}_{r\times r}. \tag{4}$$

In [14], two construction methods are presented that ensure a girth of at least 6 for the Tanner graphs associated with $\mathbf{H}'_X$ and $\mathbf{H}'_Z$, respectively. In this case, all (unavoidable) cycles of length 4 in the Tanner graph associated with $\mathbf{H}$ are assembled

[1] To distinguish between classical codes and QSC, we denote the latter by the symbol $\mathcal{C}$ and the double-bracket notation $[\![\cdot]\!]$.

in the last column. By guessing all distinct values of the last variable node, as done in each path of the ensemble decoder in Fig. 1, the influence of the cycles of length 4 is effectively suppressed. The final estimate is obtained by choosing the error estimate with the lowest weight satisfying the syndrome among all decoding paths.

C. PCMs based on DPMs

We represent each QD matrix based on DPMs by a special *exponent matrix* $\mathbf{P} \in \mathbb{F}_{2^\ell}^{w\times N}$, where each entry $p_{i,j} \in \mathbb{F}_{2^\ell}$ selects one DPM from the set $\mathcal{D}_\ell(\mathbb{F}_2)$ through a fixed bijection $\psi : \mathbb{F}_{2^\ell} \to [0, 2^\ell-1]$, defined as

$$\psi\left(\sum_{k=0}^{\ell-1} c_k\alpha^k\right) = \sum_{k=0}^{\ell-1} c_k 2^k,$$

and we will denote by $\lambda_j \coloneqq \psi^{-1}(j) \in \mathbb{F}_{2^\ell}$ the field element corresponding to integer j. Specifically, the DPM in position (i, j) is given by $\mathbf{D}^{(\psi(p_{i,j}))}$, where each $\mathbf{D}^{(l)} \in \mathcal{D}_\ell(\mathbb{F}_2)$ has a single 1 in the l-th position of its first row, with counting starting from 0. The operation of substituting the entries of $\mathbf{P}$ with such DPMs to obtain the PCM $\mathbf{H}$ is called *lifting*. The binary representation $\rho_{i,j} \in \mathbb{F}_2^\ell$ of $p_{i,j} \in \mathbb{F}_{2^\ell}$ is obtained via the fixed vector space isomorphism $\varphi : \mathbb{F}_{2^\ell} \to \mathbb{F}_2^\ell$ with

$$\varphi\left(\sum_{k=0}^{\ell-1} c_k\alpha^k\right) \coloneqq (c_{\ell-1}, \ldots, c_0),$$

so that

$$\varphi(p_{i,j} + p_{i',j'}) = \varphi(p_{i,j}) \oplus \varphi(p_{i',j'}) = \rho_{i,j} \oplus \rho_{i',j'}.$$

We refer to a *block-row* (*column-row*) as any row (column) of $\mathbf{H}$ composed exclusively of dyadic blocks.

III. Code design

In the following, we introduce our code construction both for classical and quantum codes.

A. Classical QD-LDPC Codes Design with Girth 6

Let us consider classical QD-LDPC codes with $N = L \coloneqq 2^\ell$, $3 \le w \le 2^\ell$. Our goal is to design an exponent matrix $\mathbf{P}$ corresponding to a QD-LDPC code with girth 6. To this end, we propose to obtain each row of $\mathbf{P}$ as an affine permutation of the field elements of $\mathbb{F}_{2^\ell}$, i.e.,

$$p_{u,j} \coloneqq a_u\lambda_j + b_u, \tag{5}$$

where $u \in [0,\, w-1], j \in [0, 2^\ell-1]$, and $\lambda_j = \psi^{-1}(j) \in \mathbb{F}_{2^\ell}$. Then, the set of $a_u \in \mathbb{F}_{2^\ell}^\times$ are called *multipliers* which are all distinct. Additionally, $b_u \in \mathbb{F}_{2^\ell}$. Each distinct multiplier a_u defines a unique affine permutation of $\mathbb{F}_{2^\ell}$. We will show that this rule yields LDPC matrices with Tanner graphs of girth 6, if the multipliers within the same exponent matrix are distinct.

Lemma 1 [15, Theorem 3] Let $\mathbf{P} \in \mathbb{F}_{2^\ell}^{w\times N}$ be the exponent matrix of a QD-LDPC code. By applying the lifting procedure on $\mathbf{P}$ using the associated DPMs of size $2^\ell \times 2^\ell$, we obtain the Tanner graph of the corresponding binary PCM $\mathbf{H}$ which contains at least ℓ cycles of length 4 if

$$\rho_{i_1,j_1} \oplus \rho_{i_2,j_1} \;=\; \rho_{i_2,j_2} \oplus \rho_{i_1,j_2}, \tag{6}$$

with $i_1 \neq i_2$ and $j_1 \neq j_2$.

Theorem 1 Let $\mathbf{P} \in \mathbb{F}_{2^\ell}^{w\times N}$ be an exponent matrix generated according to (5) with distinct (non-zero) multipliers $a_1, \ldots, a_w$. Then, for every pair of distinct rows $u, v \in [0, w-1]$, the mapping

$$j \mapsto p_{u,j} + p_{v,j} = (a_u + a_v)\lambda_j + (b_u + b_v), \quad j \in [0, 2^\ell - 1], \tag{7}$$

with $\lambda_j = \psi^{-1}(j)$, yields a distinct permutation of $\mathbb{F}_{2^\ell}$. Consequently, the Tanner graph of $\mathbf{H}$ obtained by lifting $\mathbf{P}$ has girth 6.

Proof: Since $a_u \neq a_v$, we have $a_u + a_v \in \mathbb{F}_{2^\ell}^\times$. Hence, the coefficient $(a_u + a_v)$ has a multiplicative inverse. Thus, using the same argument as below, it is easy to show that the map $j \mapsto (a_u + a_v)\lambda_j + (b_u + b_v)$ is bijective over $\mathbb{F}_{2^\ell}$, implying that all values $p_{u,j} + p_{v,j}$ are distinct for $j \in [0, 2^\ell - 1]$.

Let again $\rho_{u,j}$ denote the ℓ-bit binary representation of $p_{u,j}$ through φ. Assume two columns with indices $j_1 \neq j_2$ satisfy

$$\rho_{u,j_1} \oplus \rho_{v,j_1} = \rho_{u,j_2} \oplus \rho_{v,j_2}.$$

Then, applying φ^{-1} yields

$$p_{u,j_1} + p_{v,j_1} = p_{u,j_2} + p_{v,j_2}.$$

Substituting the affine form (5) gives

$$(a_u + a_v)(\lambda_{j_1} - \lambda_{j_2}) = 0.$$

Since $(a_u + a_v) \neq 0$, we must have $\lambda_{j_1} = \lambda_{j_2}$ resulting in a contradiction. Hence, all $\rho_{u,j_1} \oplus \rho_{v,j_1}$ are distinct for any pair of rows, and no 4-cycles exist according to Lemma 1. ∎

B. Quantum LDPC Code Design

In this section, we propose the construction of QD CSS codes satisfying the CAMEL condition (4). To this end, we define two QD matrices $\mathbf{H}'_X$ and $\mathbf{H}'_Z$ with corresponding exponent matrices $\mathbf{P}'_X$ and $\mathbf{P}'_Z$.

Remark 1 Let $\mathbf{r}_X$ be a binary row of $\mathbf{H}'_X$ and $\mathbf{r}_Z$ be a binary row of $\mathbf{H}'_Z$. The inner product $\mathbf{r}_X \cdot \mathbf{r}_Z^\top$ is taken over $\mathbb{F}_2$. Hence, it equals the *parity* of the number of positions where both rows have a 1. Therefore, stating that $\mathbf{H}'_X \left(\mathbf{H}'_Z\right)^\top$ has all entries equal to 1 over $\mathbb{F}_2$ means that for *every* pair of rows—one from $\mathbf{H}'_X$ and one from $\mathbf{H}'_Z$—the number of positions where both entries are 1 is odd.

As in Sec. III-A, each row of $\mathbf{P}'_X$ and $\mathbf{P}'_Z$ is generated through an affine transformation in $\mathbb{F}_{2^\ell}$, that is,

$$p_{u,j}^{(M)} = a_u^{(M)}\lambda_j + b_u^{(M)} \tag{8}$$

where $a_u^{(M)} \in \mathbb{F}_{2^\ell}^\times$, $b_u^{(M)} \in \mathbb{F}_{2^\ell}$, $j \in [0, 2^\ell - 1]$, $\lambda_j = \psi^{-1}(j)$, and $M \in \{X, Z\}$. Also, $N = L = 2^\ell$ ensures a bijection between the blocks forming the PCMs and the $\mathbb{F}_{2^\ell}$ elements.

Lemma 2 Let two exponent matrices, which we denote as $\mathbf{P}'_X, \mathbf{P}'_Z \in \mathbb{F}_{2^\ell}^{w\times N}$, have affine rows as per (8), with $a_u^{(X)} \neq a_v^{(Z)}, \forall\, u, v$. We form $\mathbf{H}'_X, \mathbf{H}'_Z$ by lifting $\mathbf{P}'_X$ and $\mathbf{P}'_Z$ with the corresponding DPMs. Then, *every* pair consisting of one row from the uth block-row of $\mathbf{H}'_X$ and one row from the vth block-row of $\mathbf{H}'_Z$ has exactly one overlapping non-zero position.

Proof: It is convenient to label the 2^ℓ lifted rows within the uth block-row of $\mathbf{H}'_X$ by $r \in [0, 2^\ell - 1]$ and within the vth block-row of $\mathbf{H}'_Z$ by $s \in [0, 2^\ell - 1]$. We also label the columns within each block-column with elements of $[0, 2^\ell - 1]$. By the definition of the DPM, in block-column j, row r has its unique 1 at column

$$\psi\left(\varphi^{-1}(\varphi(p_{u,j}^{(X)}) \oplus \varphi(\lambda_r))\right) = \psi\left(p_{u,j}^{(X)} + \lambda_r\right),$$

whereas row s has its unique 1 at column

$$\psi\left(\varphi^{-1}(\varphi(p_{v,j}^{(Z)}) \oplus \varphi(\lambda_s))\right) = \psi\left(p_{v,j}^{(Z)} + \lambda_s\right).$$

Therefore, in block-column j, the two lifted rows overlap iff[2]

$$\lambda_r + p_{u,j}^{(X)} = \lambda_s + p_{v,j}^{(Z)} \iff p_{u,j}^{(X)} - p_{v,j}^{(Z)} = \lambda_s - \lambda_r.$$

Define the difference map

$$\Delta(j) \coloneqq p_{u,j}^{(X)} - p_{v,j}^{(Z)} = \left(a_u^{(X)} - a_v^{(Z)}\right)\lambda_j + \left(b_u^{(X)} - b_v^{(Z)}\right).$$

Since $a_u^{(X)} \neq a_v^{(Z)}$, the coefficient of λ_j is nonzero, and so $\Delta : \mathbb{F}_{2^\ell} \to \mathbb{F}_{2^\ell}$ is an affine bijection. Given the pair of lifted-row indices (r, s), set $\delta \coloneqq \psi(\lambda_s - \lambda_r)$. By bijectivity, there exists a unique block index $j^\star$ such that $\Delta(j^\star) = \lambda_\delta$, i.e.,

$$p_{u,j^\star}^{(X)} - p_{v,j^\star}^{(Z)} = \lambda_s - \lambda_r.$$

Hence the two rows overlap *only* in block $j^\star$. Inside that block, each of the two rows has a single 1, and the equality above forces these to occur in the same column, yielding exactly one common 1 overall. No other block can satisfy the equality because $j^\star$ is unique. Thus, any such pair of lifted rows has exactly one overlap. ∎

Theorem 2 Let $\mathbf{P}'_X, \mathbf{P}'_Z \in \mathbb{F}_{2^\ell}^{w\times N}$ be defined as in (8). Assume all non-zero multipliers $a_u^{(M)}$ are distinct both within and across the two matrices, i.e.,

$$a_u^{(X)} \neq a_{u'}^{(X)}, \quad \text{for all } u \neq u',$$

$$a_v^{(Z)} \neq a_{v'}^{(Z)}, \quad \text{for all } v \neq v',$$

$$a_u^{(X)} \neq a_v^{(Z)}, \quad \text{for all } u, v.$$

Then, the CAMEL condition (4) is satisfied regardless of the choice of b_u.

Proof: Fix any u in $\mathbf{P}'_X$ and any v in $\mathbf{P}'_Z$. By the across-matrix distinctness, we have that $a_u^{(X)} \neq a_v^{(Z)}$. Let us form $\mathbf{H}'_X, \mathbf{H}'_Z$ by lifting $\mathbf{P}'_X$ and $\mathbf{P}'_Z$ with the corresponding DPMs. By considering Lemma 2, for every choice of row indices $r, s \in [0, 2^\ell - 1]$, the rth binary row in the uth block-row of $\mathbf{H}'_X$ and the sth binary row in the vth block-row of $\mathbf{H}'_Z$ overlap in *exactly one* position (and in no other). Equivalently, their Hamming inner product over $\mathbb{F}_2$ equals 1. Since u and v, but also r and s, are arbitrary, every cross inner product between a row of $\mathbf{H}'_X$ and a row of $\mathbf{H}'_Z$ equals 1, which means all entries of $\mathbf{H}'_X \left(\mathbf{H}'_Z\right)^\top$ are 1 in $\mathbb{F}_2$. Therefore $\mathbf{H}'_X \left(\mathbf{H}'_Z\right)^\top = \mathbf{1}_{(n-k_1)\times k_2}$, i.e., satisfying (4). ∎

Finally, $\mathbf{H}_X$ and $\mathbf{H}_Z$ are obtained from $\mathbf{H}'_X$ and $\mathbf{H}'_Z$ as in (3). Next, we provide an example.

Example 1 Let $w = 3$ and $\ell = 3$. Following (8), we choose the affine coefficients over the finite field $\mathbb{F}_{2^\ell} = \mathbb{F}_8 = \mathbb{F}_2[x]/\langle x^3 + x + 1\rangle$. The coefficients $a_u^{(M)}$ are selected from the multiplicative group $\mathbb{F}_8^\times$, while $b_u^{(M)} \in \mathbb{F}_8$. Namely,

$$\begin{aligned}
&(a_0^{(X)}, b_0^{(X)}) = (\alpha, 1), && (a_0^{(Z)}, b_0^{(Z)}) = (1, \alpha),\\
&(a_1^{(X)}, b_1^{(X)}) = (\alpha^2, \alpha^2), && (a_1^{(Z)}, b_1^{(Z)}) = (\alpha^3, \alpha^6),\\
&(a_2^{(X)}, b_2^{(X)}) = (\alpha^4, \alpha^4), && (a_2^{(Z)}, b_2^{(Z)}) = (\alpha^6, 1).
\end{aligned}$$

The corresponding exponent matrices are

$$\mathbf{P}'_X = \begin{bmatrix} 1 & \alpha^3 & \alpha^6 & \alpha^5 & \alpha & 0 & \alpha^4 & \alpha^2 \\ \alpha^2 & 0 & \alpha^5 & \alpha^3 & \alpha & \alpha^4 & 1 & \alpha^6 \\ \alpha^4 & 0 & 1 & \alpha^5 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha \end{bmatrix},$$

$$\mathbf{P}'_Z = \begin{bmatrix} \alpha & \alpha^3 & 0 & 1 & \alpha^4 & \alpha^5 & \alpha^2 & \alpha^6 \\ \alpha^6 & \alpha^4 & \alpha^3 & 0 & \alpha & 1 & \alpha^2 & \alpha^5 \\ 1 & \alpha^2 & 0 & \alpha^6 & \alpha^3 & \alpha^4 & \alpha & \alpha^5 \end{bmatrix}.$$

By applying the standard lifting procedure with DPMs to the exponent matrices above, we obtain $\mathbf{H}'_X$ and $\mathbf{H}'_Z$, and append horizontally to both of them an all-one column yielding the PCMs $\mathbf{H}_X$ and $\mathbf{H}_Z$ for the CSS framework.

IV. Numerical results

We assess the performance of quantum QD-LDPC codes in terms of logical error rate (LER) through Monte Carlo simulations over the depolarizing channel, with a depolarizing probability p. We employ the CAMEL decoder described in Fig. 1, which runs for at most 15 iterations, and the simulation continues with the same p until 100 logical errors are detected.

Based on Theorem 2, we construct QLDPC codes considering different underlying fields, i.e., we use $\ell \in \{4, 5\}$, resulting in fields $\mathbb{F}_{16}$ and $\mathbb{F}_{32}$, respectively. To construct QD-QLDPC codes, we simply use the largest allowed set of multipliers a that are distinct and non-zero, and allow $\mathbf{H}_X$ and $\mathbf{H}_Z$ to have the same size. Therefore, one element of $\mathbb{F}_{2^\ell}^\times$ is randomly discarded, leaving an even number $2^\ell - 2$ of field elements, which form the set of multipliers. We have observed through extensive numerical simulations that, as expected, the choice of the discarded element does not affect the decoding performance. Therefore, with α being a primitive element of the underlying field, we can use, without loss of generality, $\mathcal{A}_X \coloneqq \{1, \alpha, \alpha^2, \ldots, \alpha^{2^{\ell-1}-2}\}$ and $\mathcal{A}_Z \coloneqq \{\alpha^{2^{\ell-1}-1}, \alpha^{2^{\ell-1}}, \ldots, \alpha^{2^\ell-2}\}$ as the set of

[2] All operations are over $\mathbb{F}_{2^\ell}$. Since the field has characteristic 2. The minus sign is retained only for the sake of readability.

TABLE I
QD QLDPC CODES CONSTRUCTED USING THEOREM 2.

Code	n	k	R_Q	ℓ
D1	257	121	0.47	4
D2	1025	583	0.57	5

TABLE II
PARAMETERS OF THE QUASI-CYCLIC (QC) CODES C1 AND C2 CONSTRUCTED ACCORDING TO [14], THE EUCLIDEAN GEOMETRY CODE E5 FROM [14], AND THE BICYCLE CODE B1.

Code	n	k	R_Q
C1	290	128	0.44
C2	962	540	0.56
E5	1057	571	0.54
B1	800	400	0.5

multipliers a for $\mathbf{H}_X$ and $\mathbf{H}_Z$, respectively. Here, $|\mathcal{A}_X| = |\mathcal{A}_Z| = 2^{\ell-1} - 1$. We always set $b = 0$, and apply the dyadic lifting, obtaining $\mathbf{H}'_X, \mathbf{H}'_Z \in \mathbb{F}_2^{2^\ell(2^{\ell-1}-1)\times 2^{2\ell}}$. Appending an all-one column as in (3) results in $\mathbf{H}_X, \mathbf{H}_Z \in \mathbb{F}_2^{2^\ell(2^{\ell-1}-1)\times(2^{2\ell}+1)}$. The parameters of the resulting codes D1 and D2 are summarized in Table I.

In Figs. 2 and 3, we report the post-decoding LER of the constructed codes over a depolarizing channel where the three Pauli errors occur with equal probability $p/3$. All BP decoders employ sum-product BP decoding with a flooding-schedule. We consider three decoding strategies: plain quaternary BP decoding; a genie-aided quaternary BP decoder, in which the correct error value of the last qubit is provided to the decoder; and the proposed 4-path CAMEL decoding algorithm.

As a benchmark, we include codes designed through the QC construction from [14, Sec. IV] (C1 and C2), where we choose the number of block-rows to match the code rate of D1 and D2, respectively. We additionally report results for the Euclidean geometry code (E5) from [14]. As a further reference, we show the performance of the $[\![800, 400]\!]$ bicycle code (B1) decoded using the modified non-binary decoder with

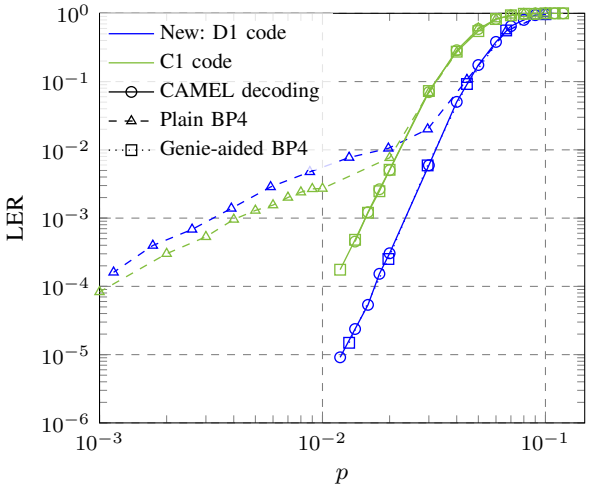

Fig. 2. LER of QLDPC codes as a function of the depolarizing probability p.

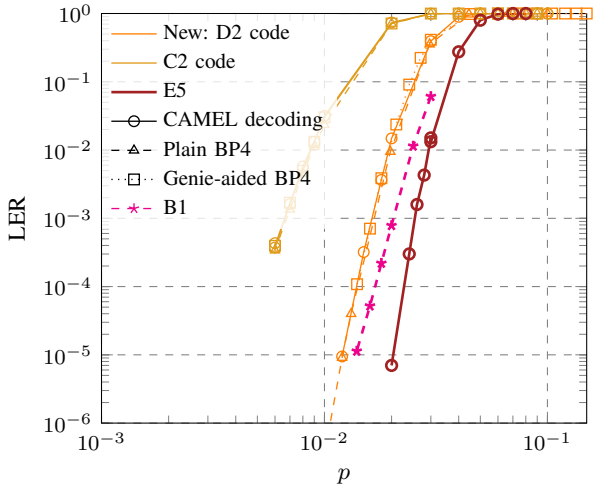

Fig. 3. LER of QLDPC codes as a function of the depolarizing probability p.

enhanced feedback [10], [21], which has higher complexity than the CAMEL decoding scheme. The parameters of the reference codes are summarized in Table II.

In [14], an error floor attributed to the presence of numerous length-4 cycles in the Tanner graph was observed for all considered codes. In contrast, we observe from Fig. 3 that, for code D2, plain quaternary BP decoding exhibits no observable error floor and shows a significant waterfall behavior. In this case, CAMEL decoding does not provide additional gains. Nevertheless, D2 achieves an error-rate performance comparable to that of the reference codes E5 and B1, despite both having lower code rates; moreover, E5 possesses a larger block length, and B1 requires higher decoding complexity.

However, for codes such as D1 and C1, where plain quaternary BP decoding suffers from a pronounced error floor due to length-4 cycles, the CAMEL ensemble decoding effectively suppresses the error floor, as shown in Fig. 2. Consistent with the observations in [14], its performance closely matches that of genie-aided decoding, yielding a substantial improvement over plain quaternary BP decoding. Furthermore, when using CAMEL decoding, the QD code D1 proposed in this work outperforms the reference code C1, despite operating at a higher rate and with a smaller block length.

Overall, the results indicate that the proposed constructions achieve high rates and competitive performance relative to state-of-the-art codes, while being paired with an effective decoding strategy capable of mitigating potential error floors.

V. CONCLUSIONS

We presented an algebraic construction of classical and quantum QD LDPC codes. The resulting CSS codes extend the family of CAMEL codes and thereby offer increased flexibility in both block length and code rate. In terms of LER, when stand-alone quaternary BP decoding is limited by error-floor effects, CAMEL ensemble decoding provides a clear performance advantage over conventional iterative decoders and achieves competitive performance to that of state-of-the-art code constructions.

REFERENCES

[1] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Physical Review A*, vol. 52, no. 4, pp. R2493–R2496, 1995.

[2] A. M. Steane, "Error correcting codes in quantum theory," *Physical Review Letters*, vol. 77, no. 5, pp. 793–797, 1996.

[3] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Physical Review A*, vol. 54, no. 2, pp. 1098–1105, 1996.

[4] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. dissertation, California Institute of Technology, 1997. [Online]. Available: https://arxiv.org/abs/quant-ph/9705052

[5] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, UK: 10th Anniversary Edition, Cambridge University Press, 2010.

[6] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Transactions on Information Theory*, vol. 44, no. 4, 1998.

[7] R. G. Gallager, "Low-density parity-check codes," *IRE Trans. Inf. Theory*, vol. IT-8, no. 1, pp. 21–28, 1962.

[8] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inf. Theory*, vol. 45, pp. 399–432, 1999.

[9] D. Poulin and Y. Chung, "On the iterative decoding of sparse quantum codes," *Quantum Information and Computation*, vol. 8, no. 10, pp. 987–1000, 2008.

[10] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "Fifteen years of quantum LDPC coding and improved decoding strategies," *IEEE Access*, vol. 3, pp. 2492–2519, 2015.

[11] M. Hagiwara and H. Imai, "Quantum quasi-cyclic LDPC codes," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, 2007, pp. 806–810.

[12] C. Tang, C. Bai, and Y. Feng, "New quantum LDPC codes based on projective geometry," *Scientific Reports*, vol. 14, no. 1, p. 17014, 2024. [Online]. Available: https://doi.org/10.1038/s41598-024-67786-0

[13] K. Kasai, "Quantum error correction with girth-16 non-binary LDPC codes via affine permutation construction," in *Proc. International Symposium on Topics in Coding (ISTC)*, 2025, pp. 1–5.

[14] S. Miao, J. Mandelbaum, H. Jäkel, and L. Schmalen, "A joint code and belief propagation decoder design for quantum LDPC codes," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, 2024, pp. 2263–2268.

[15] A. Baldelli, M. Battaglioni, and P. Santini, "Quantum CSS LDPC codes with quasi-dyadic structure," in *Proc. International Symposium on Topics in Coding (ISTC)*, 2025, pp. 1–5.

[16] M. Martinez and C. A. Kelley, "Minimum distance and other properties of quasi-dyadic parity check codes," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, 2022, pp. 2118–2123.

[17] M. Martinez, T. Pllaha, and C. A. Kelley, "Codes based on dyadic matrices and their generalizations," *Advances in Mathematics of Communications*, vol. 19, no. 5, pp. 1277–1300, 2025.

[18] P. Santini, E. Persichetti, and M. Baldi, "Reproducible families of codes and cryptographic applications," *Journal of Mathematical Cryptology*, vol. 16, no. 1, pp. 20–48, 2022.

[19] M. R. Tanner, "A recursive approach to low complexity codes," *IEEE Transactions on Information Theory*, vol. 27, no. 5, pp. 533–547, Sep. 1981.

[20] M. Pacenti, D. Chytas, and B. Vasic, "Construction and decoding of quantum Margulis codes," 2025. [Online]. Available: https://arxiv.org/abs/2503.03936

[21] Y.-J. Wang, B. C. Sanders, B.-M. Bai, and X.-M. Wang, "Enhanced feedback iterative decoding of sparse quantum codes," *IEEE Transactions on Information Theory*, vol. 58, no. 2, 2012.