Quantum CSS LDPC Codes with Quasi-Dyadic Structure

Quantum CSS LDPC Codes with Quasi-Dyadic Structure

Alessio Baldelli, Massimo Battaglioni, and Paolo Santini
Dipartimento di Ingegneria dell'Informazione, Università Politecnica delle Marche, Ancona, Italy
a.baldelli@pm.univpm.it, {m.battaglioni, p.santini}@univpm.it

***Abstract*—Quantum quasi-cyclic (QC) and quantum low-density parity-check (LDPC) codes have received significant attention due to their algebraic regularity and performance under low-complexity decoding. In this work, we explore a class of structured quantum codes based on reproducible matrices, which generalize known families such as cyclic, QC, and dyadic codes. Focusing on sparse quasi-dyadic (QD) structures, we investigate how their symmetries influence Tanner graph cycles. Moreover, we construct quantum LDPC codes within the Calderbank-Shor-Steane (CSS) framework, analyzing dual-containing configurations, and assess their error rates.**

***Index Terms*—Dyadic codes, CSS codes, LDPC codes, Quasi-Dyadic codes, Quantum codes.**

I. Introduction

The study of quantum error-correcting codes has long been motivated by the search for algebraic and topological structures, which bring advantages in theoretical analysis and implementation. In particular, structured codes simplify the design of encoding circuits, potentially reducing the number of required quantum gates and inter-qubit interactions. This may help limit the introduction of physical noise during decoding, which is a critical concern in current quantum technologies. An example of algebraic structure arises in quantum quasi-cyclic (QC) codes, built from matrices composed of circulant blocks. They allow for compact representations and efficient implementation. When the parity-check or generator matrices representing the code are sparse, quantum quasi-cyclic low-density parity-check (QC-LDPC) codes [1] offer good performance through efficient decoding.

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). The work of Paolo Santini was partially supported by the Italian Ministry of University and Research (MUR) under the PRIN 2022 program with projects "Mathematical Primitives for Post Quantum Digital Signatures" (CUP I53D23006580001) and "Post quantum Identification and eNcryption primiTives: dEsign and Realization (POINTER)" (CUP I53D23003670006), by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan, funded by the European Union - Next Generation EU and by MUR under the Italian Fund for Applied Science (FISA 2022), Call for tender No. 1405 published on 13-09-2022 - project title "Quantum-safe cryptographic tools for the protection of national data and information technology assets" (QSAFEIT) - No. FISA 2022-00618 (CUP I33C24000520001), Grant Assignment Decree no. 15461 adopted on 02.08.2024. The work of Massimo Battaglioni was partially supported by the European Union - Next Generation EU under the Italian National Recovery and Resilience Plan (NRRP), Mission 4, Component 2, Investment 1.3, CUP J33C22002880001, partnership on "Telecommunications of the Future" (PE00000001 - program "RESTART"). The views expressed are those of the authors and do not represent the funding institutions.

As a generalization of this framework, reproducible codes were introduced in [2]. A matrix is said to be reproducible if its full structure can be generated from a small number of rows and a family of linear transformations. This concept encompasses, among others, cyclic, QC, dyadic and quasi-dyadic (QD) codes [3]. Dyadic matrices, in particular, exhibit a rich recursive structure: the entries of the matrix are determined by binary group operations on the indices, and the entire matrix can be reconstructed from a single row, say the first one, called *signature*. Many operations (e.g., inversion and multiplication) can be performed efficiently by looking at signatures and exploiting the special dyadic structure [4].

Dyadic matrices can serve as building blocks for reproducible generator or parity-check matrices. As such, quantum codes based on dyadic structures naturally fall into the category of quantum reproducible codes. Quantum dyadic codes have been introduced in [5], where the authors offer some insights into how structure can be exploited in the design of quantum codes. However, the dyadic condition is quite rigid and it enforces a global structure that may limit the properties of code constructions. For example, [5] focuses on designing stabilizer codes of dimension zero, which do not encode logical qubits. In contrast, QD codes relax this rigidity by introducing block-level dyadic symmetry. In classical coding, this generalization has been fruitful [6]–[8]. Despite their promise, quantum QD codes have not been explored in the literature to date, and we aim to fill this gap.

So, in this work, we study some properties of quantum codes constructed from sparse reproducible matrices with QD structure. Our analysis focuses on how the dyadic and QD symmetries affect the cycles of the associated Tanner graphs [9]. Using these matrices, we propose two constructions of quantum QD-LDPC codes within the Calderbank-Shor-Steane (CSS) framework [10], [11], considering in particular dual-containing configurations. We evaluate the error rate performance of the proposed codes over the depolarizing channel.

The remainder of this paper is organized as follows. Section II introduces notation and background. In Section III, we analyze some properties of dyadic and QD matrices. In Section IV, we propose some constructions of quantum QD-LDPC codes, as dual-containing CSS codes, and assess their logical error rate (LER) in Section V. Section VI concludes the paper.

II. Notation and background

Upper case and lower case bold letters denote matrices and vectors, respectively. We denote the transpose of matrix $\mathbf{M}$ as $\mathbf{M}^T$. The $k \times k$ identity matrix is denoted as $\mathbf{I}_k$, and the size is omitted when clear from the context. The same holds for the all-zero matrix $\mathbf{0}$. Let $\mathbb{F}_2^n$ be the space of binary vectors of length n. The Hamming weight of an element $\mathbf{s}$ corresponds to number of its non-zero entries, and is denoted as $|\mathbf{s}|$.

The tensor product of two matrices or vectors $\mathbf{a}$ and $\mathbf{b}$ is denoted by $\mathbf{a} \otimes \mathbf{b}$. The n-qubit Hilbert space is $(\mathbb{C}^2)^{\otimes n}$, which denotes the tensor product of n copies of the complex two-dimensional space $\mathbb{C}^2$. The Pauli group on n qubits consists of all n-fold tensor products of single-qubit Pauli matrices $\mathbf{I}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}$ with multiplicative factors ± 1 and $\pm i$. A stabilizer group $\mathcal{S}$ is an Abelian subgroup of the Pauli group on n qubits whose elements commute and can be measured simultaneously.

A. Classical linear codes

A linear code $C[n, k, d] \subset \mathbb{F}_2^n$ with length n, dimension k, and minimum Hamming distance d, is a linear subspace of $\mathbb{F}_2^n$. An element in C is a codeword $\mathbf{c} \in C$. A code can be represented with a full-rank parity-check matrix (PCM) $\mathbf{H} \in \mathbb{F}_2^{r \times n}$, where $r \geqslant n - k$, such that the code is the space of all vectors $\mathbf{c} \in \mathbb{F}_2^n$ for which $\mathbf{H}\mathbf{c}^T = \mathbf{0}$ holds. If $\mathbf{H}$ is *sparse*, then the code is an LDPC code. Every PCM can be associated with a Tanner graph [9], which is a bipartite graph consisting of n variable nodes and r check nodes. Each non-zero entry in $\mathbf{H}$ defines an edge in the graph. Tanner graphs are characterized by the presence of *cycles*. The *girth* g is defined as the length of the shortest cycle(s) in the graph. We use the terms girth of a Tanner graph, girth of a code, and girth of a PCM interchangeably.

B. Quantum codes

A quantum stabilizer code $\mathcal{C}[\![n, k, d]\!]$ is a 2^k-dimensional subspace of $(\mathbb{C}^2)^{\otimes n}$, stabilized by all $s \in \mathcal{S}$, i.e., $s\,|\psi\rangle = |\psi\rangle$ for all $|\psi\rangle \in \mathcal{C}$. We are interested in studying CSS codes [10]. A CSS code[1] $\mathcal{C}[\![n, k_1 - k_2, d]\!]$ is constructed starting by two classical codes $C_1[n, k_1, d_1]$ and $C_2[n, k_2, d_2]$, represented by $\mathbf{H}_1$ and $\mathbf{H}_2$, respectively, where $d \geqslant \min\{d_1, d_2\}$, $k_1 > k_2$, and $C_2 \subset C_1$. In particular, the PCM representing $\mathcal{C}$ is

$$\mathbf{H}_{\text{CSS}} = \left(\begin{array}{c|c} \mathbf{H}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{G}_2 \end{array}\right) \tag{1}$$

and that both $\mathbf{H}_1\mathbf{G}_2^T$ and $\mathbf{G}_2\mathbf{H}_1^T$ are zero matrices, where $\mathbf{H}_1 \in \mathbb{F}_2^{(n-k_1)\times n}$ and $\mathbf{G}_2 \in \mathbb{F}_2^{k_2 \times n}$. In other words, one can consider $\mathbf{G}_2$ as the PCM of $C_2^\perp$. If we use only one code C_1, such that its dual is contained within itself, i.e., $C_1^\perp \subset C_1$, instead of two distinct codes to construct the quantum CSS code, we obtain a special subclass known as *dual-containing* CSS codes. In this case, the classical codes involved are $C_1[n, k_1, d]$ and its dual $C_1^\perp[n, n - k_1, d^\perp]$, and the associated parity-check matrix satisfies $\mathbf{H}_1\mathbf{H}_1^T = \mathbf{0}$. The resulting quantum code is denoted by $\mathcal{C}_{\text{dc}}[\![n, 2k_1 - n, d_{\text{dc}}]\!]$.

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

C. Dyadic and quasi-dyadic codes

A class of reproducible matrices is that of *dyadic* matrices.

Definition 1 (Ring of dyadics). *For $\ell \geqslant 1$ an integer, we define $\mathcal{M}_\ell(\mathbb{F}_2)$ as the set of $2^\ell \times 2^\ell$ matrices with entries over $\mathbb{F}_2$ and structured as follows:*

$$\mathbf{M} = \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B} & \mathbf{A} \end{pmatrix}, \quad \mathbf{A}, \mathbf{B} \in \mathcal{M}_{\ell-1}(\mathbb{F}_2). \tag{2}$$

For $\ell = 0$, $\mathcal{M}_0(\mathbb{F}_2) \coloneqq \mathbb{F}_2$. For any ℓ, when equipped with standard matrix sum and multiplication, then $\mathcal{M}_\ell(\mathbb{F}_2)$ forms a commutative ring.

It is easy to see that a dyadic matrix can be fully described using only its first row $(m_{0,0}, m_{0,1}, \cdots, m_{0,2^\ell-1})$, which is sometimes called *signature* $\mathbf{s}$. Indeed, for any i, j, we have $m_{i,j} = m_{0,i\oplus j}$,where $i \oplus j$ denotes the integer corresponding to the XOR between the binary representations of i and j.[2] By weight of a dyadic matrix, we refer to the Hamming weight of its signature, $|\mathbf{s}|$. Let $\mathcal{P}_\ell(\mathbb{F}_2) = \{\mathbf{P}^{(0)} \coloneqq \mathbf{I}_{2^\ell}, \mathbf{P}^{(1)}, \cdots, \mathbf{P}^{(2^\ell-1)}\} \subseteq \mathcal{M}_\ell(\mathbb{F}_2)$ be the set containing all dyadics with weight 1, so that $\mathbf{P}^{(i)}$ is the dyadic whose signature has a 1 in position i. Then, each $\mathbf{P}^{(i)}$ is called dyadic permutation matrix (DPM). In the following, given $\mathbf{P}^{(i)}$, we denote the binary representation of position i as $\boldsymbol{\rho} \in \mathbb{F}_2^\ell$. Each DPM has multiplicative order 2, since

$$\left(\mathbf{P}^{(i)}\right)^2 = \mathbf{P}^{(i)} \cdot (\mathbf{P}^{(i)})^T = \mathbf{P}^{(i)} \cdot (\mathbf{P}^{(i)})^{-1} = \mathbf{I}_{2^\ell}, \quad \forall\, i.$$

It is easy to see that each dyadic can be uniquely expressed as a linear combination of DPMs:

$$\exists!(\alpha_0, \cdots, \alpha_{2^\ell-1}) \in \mathbb{F}_2^{2^\ell} : \mathbf{M} = \sum_{i=0}^{2^\ell-1} \alpha_i \mathbf{P}^{(i)}, \ \ \forall\, \mathbf{M} \in \mathcal{M}_\ell(\mathbb{F}_2),$$

where $(\alpha_0, \cdots, \alpha_{2^\ell-1})$ is the signature. Furthermore, it is straightforward to note that, for any two DPMs $\mathbf{P}^{(i)}$ and $\mathbf{P}^{(j)}$, it holds that $\mathbf{P}^{(i)} \cdot \mathbf{P}^{(j)} = \mathbf{P}^{(i\oplus j)}$.

Lemma 1. *Let $\ell \geqslant 1$ be an integer and $\mathbf{M} \in \mathcal{M}_\ell(\mathbb{F}_2)$ with signature $\mathbf{s}$. Then:*

$$\mathbf{M}^2 = \begin{cases} \mathbf{0}, & \text{if } |\mathbf{s}| \text{ is even,} \\ \mathbf{I}_{2^\ell}, & \text{if } |\mathbf{s}| \text{ is odd.} \end{cases}$$

Hence, $\mathbf{M}$ is non singular if and only if its signature has odd weight and $\mathbf{M}^{-1} = \mathbf{M}$.

A matrix is called *quasi-dyadic* if it is formed by dyadic blocks, and a linear code is called QD if it admits a generator matrix (equivalently, a PCM) which is QD.

[2]This is an abuse of notation, as i and j are not binary vectors. If ϕ denotes a bijection between integers $\{0, \ldots, 2^\ell - 1\}$ and binary vectors in $\mathbb{F}_2^\ell$, then we should write $\phi^{-1}(\phi(i) \oplus \phi(j))$, but this would be unnecessarily cumbersome. Each index is represented using ℓ digits, with the LSB on the left.

III. Properties of dyadic and QD matrices

In this section we study some properties of QD codes.

Theorem 1. *Let $u \geqslant 2$ be an integer and $\mathbf{H} \in \mathbb{F}_2^{2^\ell \times u2^\ell}$ be a QD matrix with the following structure*

$$\mathbf{H} = (\mathbf{H}_0, \ldots, \mathbf{H}_{u-1}), \quad \mathbf{H}_i \in \mathcal{M}_\ell(\mathbb{F}_2), \quad \forall\, i \in \{0, \ldots, u-1\}, \tag{3}$$

where each $\mathbf{H}_i$ is dyadic, with side 2^ℓ and odd weight v. Let $C \subseteq \mathbb{F}_2^{u2^\ell}$ be the classical code whose PCM is $\mathbf{H}$. Then:

1) *$\mathbf{H}$ has full rank and, consequently, C has redundancy 2^ℓ and dimension $2^\ell(u-1)$;*
2) *if all blocks $\mathbf{H}_i$ are distinct, C contains at least $\binom{u}{2}2^{1+\ell}$ codewords of weight $2v$;*
3) *if u is even, then the code is dual-containing.*

Proof: From Lemma 1, a dyadic with odd weight is non singular: hence, by hypothesis, the rows of $\mathbf{H}$ are linearly independent, which proves the first claim. To prove thesis 2), we consider a pair of indices $0 \leqslant i < j \leqslant u-1$, which we use to define a QD matrix $\mathbf{C} = (\mathbf{C}_0, \cdots, \mathbf{C}_{u-1})$, as follows:

$$\mathbf{C}_z = \begin{cases} \mathbf{H}_j & \text{if } z = i, \\ \mathbf{H}_i & \text{if } z = j, \\ \mathbf{0} & \text{otherwise.} \end{cases}$$

For instance, if $u = 3$, $i = 0$ and $j = 2$, then $\mathbf{C} = (\mathbf{H}_2, \mathbf{0}, \mathbf{H}_0)$. We have $\mathbf{C}\mathbf{H}^T = \mathbf{0}$, since

$$\mathbf{C}\mathbf{H}^T = \mathbf{C}_i\mathbf{H}_i^T + \mathbf{C}_j\mathbf{H}_j^T = \mathbf{H}_j\mathbf{H}_i + \mathbf{H}_j\mathbf{H}_i = \mathbf{0}.$$

Thus, each row of $\mathbf{C}$ is a codeword of weight v. Since $\mathbf{C}$ has full rank, each choice for $\mathbf{C}$ identifies 2^ℓ codewords of weight $2v$. Note that each choice for $\mathbf{C}$ is determined by a specific pair (i, j): we have $\binom{u}{2}$ such choices, yielding an overall number of $\binom{u}{2}2^\ell$ such codewords. This number can be doubled by observing that, for each pair (i, j), we can define another QD matrix $\mathbf{C}' \in \mathbb{F}_2^{2^\ell \times u2^\ell}$ such that $\mathbf{C}'\mathbf{H}^T = \mathbf{0}$. Indeed, it is enough to swap the blocks $\mathbf{C}'_i$ and $\mathbf{C}'_j$, i.e., $\mathbf{C}'_i = \mathbf{H}_i$, $\mathbf{C}'_j = \mathbf{H}_j$ while all the other blocks are null. This yields another family of $\binom{u}{2}2^\ell$ codewords of weight $2v$. Finally, we prove thesis 3). To this end, it suffices to observe that $\mathbf{H}\mathbf{H}^T = \mathbf{H}_0^2 + \ldots + \mathbf{H}_{u-1}^2 = u \cdot \mathbf{I}_{2^\ell}$. Since u is even, the previous sum is null. ∎

From Theorem 1, we find that the minimum distance of codes with PCM as in (3) is upper-bounded by $2v$.

Remark 1. *The code described in Theorem 1 can be described by a sparse generator matrix. Indeed, we know that the code has dimension $k = 2^\ell(u-1)$ and contains $\binom{u}{2}2^{\ell+1} \geqslant k$ codewords with weight $2v$. Hence, these codewords can be used to obtain a generator matrix with row weight $2v$. This would lead to an encoding process with cost $O(kv)$. We observe that even the systematic generator matrix is somewhat sparse. Indeed, it is in the form:*

$$\mathbf{G} = \left(\mathbf{I}_{2^\ell(u-1)} \middle| \begin{matrix} \mathbf{H}_u\mathbf{H}_1 \\ \vdots \\ \mathbf{H}_u\mathbf{H}_{u-1} \end{matrix} \right).$$

The row weight of this matrix is at most $1 + v^2$ and, therefore, systematic encoding can be done with cost $O(kv^2)$.

A. Cycle properties of QD codes

QD matrices constructed from dyadic blocks with a signature row of weight greater than one have girth 4, as shown in [5], [8], since their constituent dyadic matrices already exhibit cycles of length 4. Therefore, we focus on QD matrices built from DPMs. This construction is particularly appealing for iterative decoding, as DPMs can potentially yield codes with girth greater than 4. Next, two theoretical results are reported from [5], [8] on 2×2 arrays of n-adic matrices. They easily generalize to the dyadic case.

Lemma 2. *If $\mathbf{P} = \begin{pmatrix} \mathbf{P}_{0,0} & \mathbf{P}_{0,1} \\ \mathbf{P}_{1,0} & \mathbf{P}_{1,1} \end{pmatrix}$ where $\mathbf{P}_{i,j}$ is an n-adic matrix of weight 1 with the non-zero signature row entry in position $\boldsymbol{\rho}_{i,j} \in \mathbb{F}_n^\ell$, then each cycle in the Tanner graph corresponding to $\mathbf{P}$ has the same length.*

Theorem 2. *If $\mathbf{P} = \begin{pmatrix} \mathbf{P}_{0,0} & \mathbf{P}_{0,1} \\ \mathbf{P}_{1,0} & \mathbf{P}_{1,1} \end{pmatrix}$ where $\mathbf{P}_{i,j}$ is an n-adic matrix of weight 1 with the non-zero signature row entry in position $\boldsymbol{\rho}_{i,j} \in \mathbb{F}_n^\ell$, then the girth of the Tanner graph corresponding to $\mathbf{P}$ is*

$$g = 4(\#\langle \boldsymbol{\alpha} \rangle), \tag{4}$$

where $\boldsymbol{\alpha} = \boldsymbol{\rho}_{0,0} \oplus \boldsymbol{\rho}_{1,1} - (\boldsymbol{\rho}_{0,1} \oplus \boldsymbol{\rho}_{1,0})$, the positions $\boldsymbol{\rho}_{i,j}$ are written in binary notation, and $\#\langle \boldsymbol{\alpha} \rangle$ is the order of $\boldsymbol{\alpha}$.

Remark 2. *From Lemma 2 and Theorem 2, it is clear that for any 2×2 matrix built using dyadic blocks, each cycle has length 8 in the best case or 4, in the worst. So, the girth of a QD 2×2 matrix built using 4 DPMs is always 4 or 8.*

Corollary 1. *Let*

$$\mathbf{P} = \begin{pmatrix} \mathbf{P}_{0,0} & \mathbf{P}_{0,1} & \cdots & \mathbf{P}_{0,u-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{P}_{w-1,0} & \mathbf{P}_{w-1,1} & \cdots & \mathbf{P}_{w-1,u-1} \end{pmatrix}, \tag{5}$$

be a QD matrix, being $\mathbf{P}_{i,j} \in \mathcal{P}_\ell(\mathbb{F}_2)$. If every possible 2×2 sub-matrix of $\mathbf{P}$, i.e.,

$$\mathbf{P}' = \begin{pmatrix} \mathbf{P}_{i,j} & \mathbf{P}_{i,j'} \\ \mathbf{P}_{i',j} & \mathbf{P}_{i',j'} \end{pmatrix}, \tag{6}$$

with $i \neq i'$ and $j \neq j'$ has girth equal to 8, then the girth of the code associated to $\mathbf{P}$ is either 6 or 8.

Let us provide a general result on the existence of cycles, whose simple proof is omitted for the sake of conciseness.

Theorem 3. *Consider a $\lambda/2 \times \lambda/2$ block matrix $\mathbf{P}$ of the form*

$$\mathbf{P} = \begin{bmatrix} \mathbf{P}_{0,0} & \mathbf{0} & \mathbf{0} & \ldots & \mathbf{P}_{0,\lambda/2-1} \\ \mathbf{P}_{1,0} & \mathbf{P}_{1,1} & \mathbf{0} & \ldots & \mathbf{0} \\ \mathbf{0} & \ddots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \ldots & \mathbf{0} & \mathbf{P}_{\lambda/2-1,\lambda/2-2} & \mathbf{P}_{\lambda/2-1,\lambda/2-1} \end{bmatrix}, \tag{7}$$

where each $\mathbf{P}_{i,j} \in \mathcal{P}_\ell(\mathbb{F}_2)$. *Let*

$$\boldsymbol{\alpha} = \bigoplus_{\substack{(i,j) \\ \mathbf{P}_{i,j} \neq \mathbf{0}}} \boldsymbol{\rho}_{i,j},$$

where $\boldsymbol{\rho}_{i,j} \in \mathbb{F}_2^\ell$ *is the position of the non-zero element in the first row of* $\mathbf{P}_{i,j}$. *A cycle of length* λ *exists in* $\mathbf{P}$ *iff* $\boldsymbol{\alpha} = \mathbf{0}$.

The above results allow us to write a condition on the existence of cycles in a generic $r_0 \times n_0$ array $\mathbf{P}$ of (non-zero) DPMs, as done in [12] for arrays of non-zero circulant matrices. Let $\boldsymbol{\Delta}_{j_k,j_{k+1}}(l) = \boldsymbol{\rho}_{j_k,l} \oplus \boldsymbol{\rho}_{j_{k+1},l}$. $\mathbf{P}$ contains a cycle of length λ iff

$$\bigoplus_{k=0}^{\lambda/2-1} \boldsymbol{\Delta}_{j_k,j_{k+1}}(l_k) = \mathbf{0}, \tag{8}$$

with $j_0 = j_\lambda$, $j_k \neq j_{k+1}$, and $l_k \neq l_{k+1}$.

Proposition 1. *Let* $\mathbf{P} = \begin{pmatrix} \mathbf{P}_{i,j} & \mathbf{P}_{i,j'} \\ \mathbf{P}_{i',j} & \mathbf{P}_{i',j'} \end{pmatrix}$ *be a QD matrix, built using DPMs. Let us assume that* $\mathbf{P}_{i,j}\mathbf{P}_{i',j} = \mathbf{P}_{i,j'}\mathbf{P}_{i',j'}$. *Then, the Tanner graph associated to* $\mathbf{P}$ *has girth 4.*

Proof: Since $\mathbf{P}_{i,j}\mathbf{P}_{i',j} = \mathbf{P}_{i,j'}\mathbf{P}_{i',j'}$, then $\boldsymbol{\rho}_{i,j} \oplus \boldsymbol{\rho}_{i',j} = \boldsymbol{\rho}_{i,j'} \oplus \boldsymbol{\rho}_{i',j'}$, that is, $\boldsymbol{\rho}_{i,j} \oplus \boldsymbol{\rho}_{i',j'} = \boldsymbol{\rho}_{i,j'} \oplus \boldsymbol{\rho}_{i',j}$, and, according to (8), the code associated to $\mathbf{P}$ has girth 4. ∎

IV. Quantum QD-LDPC codes

In this section, we present two constructions of the PCM of classical QD codes as $w \times u$ arrays of dyadic matrices. We then show how to use these PCMs to the design quantum dual-containing CSS QD-LDPC codes.

Construction A. The parameter u must be even in order to preserve the dual-containing structure, and $w < u$. The dimension and the rate of the classical code C we construct are $(u-w)2^\ell$, and $1-w/u$, respectively. So, the dimension of the associated quantum CSS dual-containing code is $2k_1 - n = 2(u-w)2^\ell - u2^\ell = (u-2w)2^\ell$. Therefore, since we aim to obtain a quantum code with dimension greater than 0, it holds that $w < u/2$. The procedure for building the PCM, given $w \leqslant 4$, is as follows:

- Select $u/2+1$ DPMs. From this set, choose one matrix $\mathbf{P}^{(z_0)} \in \mathcal{P}_\ell(\mathbb{F}_2)$ to serve as *anchor matrix*, denoted by $\mathbf{Q} = \mathbf{P}^{(z_0)}$. The first block row (indexed by 0) of the PCM is constructed by alternating the anchor matrix with the remaining $u/2$ matrices, as follows:

$$(\mathbf{Q} \quad \mathbf{P}^{(z_1)} \quad \mathbf{Q} \quad \mathbf{P}^{(z_2)} \quad \dots \quad \mathbf{Q} \quad \mathbf{P}^{(z_{u/2})}).$$

- The block row indexed by 1 is obtained by performing a blockwise-cyclic shift of the 0-th block row to the right by one position.
- The block row indexed by 2 is generated using a technique we refer to as the *left-hand conveyor belt*: we rewrite the matrix pairs of the row indexed by 0 in reverse order, alternating from right to left. The result is:

$$(\mathbf{Q} \quad \mathbf{P}^{(z_{u/2})} \quad \mathbf{Q} \quad \mathbf{P}^{(z_{u/2-1})} \quad \dots \quad \mathbf{Q} \quad \mathbf{P}^{(z_1)}).$$

$$\begin{pmatrix} \mathbf{Q} & \mathbf{P}^{(z_1)} & \mathbf{Q} & \mathbf{P}^{(z_2)} & \dots & \mathbf{Q} & \mathbf{P}^{(z_{u/2})} \\ \mathbf{P}^{(z_{u/2})} & \mathbf{Q} & \mathbf{P}^{(z_1)} & \mathbf{Q} & \dots & \mathbf{P}^{(z_{u/2-1})} & \mathbf{Q} \\ \mathbf{Q} & \mathbf{P}^{(z_{u/2})} & \mathbf{Q} & \mathbf{P}^{(z_{u/2-1})} & \dots & \mathbf{Q} & \mathbf{P}^{(z_1)} \\ \mathbf{P}^{(z_1)} & \mathbf{Q} & \mathbf{P}^{(z_{u/2})} & \mathbf{Q} & \dots & \mathbf{P}^{(z_2)} & \mathbf{Q} \end{pmatrix}$$

Figure 1: PCM built using *Construction A*, with $w = 4$.

Table I: Parameters for Constructions A and B

Const.	Classical Code			CSS dual-containing Code		
	k	n	R	k_Q	n_Q	R_Q
A	$2^\ell(u-w)$	$2^\ell u$	$\frac{u-w}{u}$	$2^\ell(u-2w)$	$2^\ell u$	$\frac{u-2w}{u}$
B	$2^\ell(u-1)$	$2^\ell u$	$\frac{u-1}{u}$	$2^\ell(u-2)$	$2^\ell u$	$\frac{u-2}{u}$

- Finally, the last block row, indexed by 3, is constructed by applying a block-wise right cyclic shift to the block row above it.

In this construction, by the pigeonhole principle, it is possible to use at most $u/2+1$ distinct DPMs, as long as $u/2+1 \leqslant 2^\ell$. The construction is illustrated in Fig. 1.

Construction B. This construction refers to Theorem 1. The parameter u must be even in order to preserve the dual-containing structure, $w = 1$, and we set the signature row weight $|\mathbf{s}|$ to be the same for all the constituent dyadic matrices. As a result, we obtain a regular code in the column weight. The dimension and the rate of the classical code C we obtain are $(u-1)2^\ell$, and $1-1/u$, respectively. So, the dimension of the associated quantum CSS dual-containing code is $2k_1 - n = 2(u-1)2^\ell - u2^\ell = (u-2)2^\ell$. By the pigeonhole principle, it is possible to use at most u distinct dyadic matrices in the construction, as long as $u \leqslant \binom{2^\ell}{|\mathbf{s}|}$.

The design parameters of the classical and quantum CSS codes obtainable through the two above constructions are summarized in Table I, as a function of u and w. The next theorem follows naturally.

Theorem 4. *Given a PCM* $\mathbf{H}$ *built using Construction A and Construction B, it holds that* $\mathbf{H}\mathbf{H}^T = \mathbf{0}$.

The following result follows from Proposition 1.

Corollary 2. *Let*

$$\mathbf{H} = \begin{pmatrix} \mathbf{H}_{0,0} & \mathbf{H}_{0,1} & \cdots & \mathbf{H}_{0,u-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{H}_{w-1,0} & \mathbf{H}_{w-1,1} & \cdots & \mathbf{H}_{w-1,u-1} \end{pmatrix}, \tag{9}$$

be a quasi-dyadic matrix built up using wu *DPMs* $\mathbf{H}_{i,j} \in \mathcal{P}_\ell(\mathbb{F}_2)$. *Assume that* $\mathbf{H}$ *is the PCM of a dual-containing code, so* $\mathbf{H}\mathbf{H}^T = \mathbf{0}$. *Then, the associated Tanner graph has girth 4.*

Although the presence of cycles of length 4 is a common challenge in the design of quantum LDPC codes, methods to avoid such cycles exist (see [1], [13, Section III-A]). In addition, many improved decoding strategies have been proposed to mitigate their effect on error rate performance.

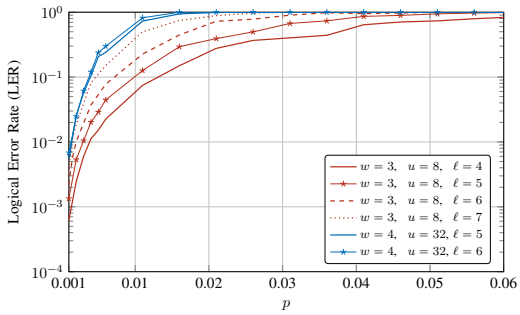

Figure 2: LER of CSS codes designed by Construction A, as a function of the depolarizing probability p.

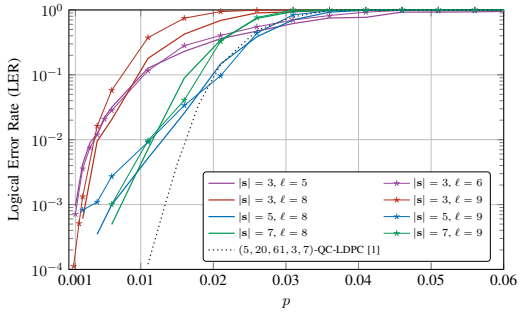

Figure 3: LER of CSS codes designed by Construction B, as a function of the depolarizing probability p.

V. Numerical results

In this section, we assess the LER (i.e., word error rate) of some codes designed with Constructions A and B, through Monte Carlo simulations over the depolarizing channel with depolarizing probability p. We employ a Belief Propagation (BP) decoder in its Min-Sum (MS) variant [14]. The decoder runs at most 100 iterations, and the simulation continues with the same depolarizing probability until 100 logical errors are detected. Only one of the two PCMs was decoded, since they are identical in a dual-containing CSS code.

In Fig. 2 we report the performance of several quantum CSS dual-containing codes obtained by Construction A, considering $w \in \{3, 4\}$. We note that the best curves are associated to classical codes built using a relatively small number of columns, say $u = 8$, and low values of ℓ. In particular, we note that if we build a 48×128 PCM with $w = 3$, $u = 8$ and $\ell = 4$ (solid red) instead of $w = 3$, $u = 8$ and $\ell \in \{5, 6, 7\}$ (other red curves), we get better performance. Similarly, if we build a 128×1024 PCM with $w = 4$, $u = 32$, $\ell = 5$ (blue), instead of $w = 4$, $u = 32$, $\ell = 6$ (blue, starred), we get again better performance. This might be due to the increasing number of short cycles in the latter codes. For $w = 3$ and $u = 8$, we get classical rate $R = 5/8$, from which $R_Q = 1/4$. Instead, for $w = 4$ and $u = 32$, we obtain worst performance, but larger rates, namely $R = 7/8$ and $R_Q = 3/4$.

Instead, in Fig.3 we consider only classical codes with $R = 3/4$, from which $R_Q = 1/2$. We use dyadic matrices with $\ell \in \{5, 6, 8, 9\}$ and $|\mathbf{s}| \in \{3, 5, 7\}$, and consider $u = 4$. We note that the performance is better for large values of odd signature weights, i.e., 5, 7.

The black curve in Fig. 3 corresponds to a QC-LDPC code $C[2044, 1515]$ with rate $R = 3/4$, constructed as in [1]. This code represents a quantum *not dual-containing* CSS code with $R_Q = 1/2$. Code length, dimension and quantum code rate are comparable to our code with $|\mathbf{s}| = 5$ and $\ell = 8$. The improved performance of the code from [1] can be attributed to its non-dual-containing structure, which allows avoidance of 4-cycles.

We also note that the code with $|\mathbf{s}| = 3$, $\ell = 5$ derived by Construction B outperforms the one from Construction A with $|w| = 3$, $u = 8$ and $\ell = 4$. In fact, they have the same code length $n = 128$ and achieve comparable performance, but the code from Construction B offers twice the quantum rate R_Q.

VI. Conclusion

We have studied some properties of dyadic and QD matrices. Furthermore, we have discussed methods for constructing sparse quantum CSS codes with a QD structure and assessed their performance. We plan to analyze the minimum distance properties, other constructions that are not dual-containing, and the error rate performance of the studied quantum codes under more advanced decoding algorithms in future works.

References

[1] M. Hagiwara and H. Imai, "Quantum Quasi-Cyclic LDPC Codes," in *2007 IEEE International Symposium on Information Theory*, 2007, pp. 806–810.

[2] 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.

[3] B. Rajan and M. H. Lee, "Quasicyclic dyadic codes in Walsh-Hadamard domain," in *Proceedings. 2001 IEEE International Symposium on Information Theory*, 2001, p. 37.

[4] G. Banegas, P. S. Barreto, E. Persichetti, and P. Santini, "Designing efficient dyadic operations for cryptographic applications," *Journal of Mathematical Cryptology*, vol. 14, no. 1, pp. 95–109, 2020.

[5] M. Martinez, T. Pllaha, and C. A. Kelley, "Codes based on dyadic matrices and their generalizations," *Advances in Mathematics of Communications*, 2024.

[6] R. Misoczki and P. S. L. M. Barreto, "Compact McEliece Keys from Goppa Codes," in *Selected Areas in Cryptography (SAC 2009)*, M. J. Jacobson, V. Rijmen, and R. Safavi-Naini, Eds., ser. Lecture Notes in Computer Science, vol. 5867, Springer Berlin Heidelberg, 2009, pp. 376–392.

[7] E. Persichetti, "Compact McEliece Keys Based on Quasi-Dyadic Srivastava Codes," *Journal of Mathematical Cryptology*, vol. 6, no. 2, pp. 149–169, 2012.

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

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

[10] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, pp. 1098–1105, 2 Aug. 1996.

[11] A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.*, vol. 77, pp. 793–797, 5 Jul. 1996.

[12] M. P. C. Fossorier, "Quasi-Cyclic Low-Density Parity-Check Codes From Circulant Permutation Matrices," *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1788–1793, Aug. 2004.

[13] 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.

[14] M. Fossorier, M. Mihaljevic, and H. Imai, "Reduced complexity iterative decoding of low-density parity check codes based on belief propagation," *IEEE Transactions on Communications*, vol. 47, no. 5, pp. 673–680, 1999.