Lifted-Product QLDPC Codes in the Polynomial Domain

Vahid Nourozi[†], Mohsen Moradi[*], Roxana Smarandache[‡], and David G. M. Mitchell[†],

[†]Klipsch School of Electrical and Computer Engineering, New Mexico State University
Las Cruces, NM 88003, USA, Email: nourozi@nmsu.edu; dgmm@nmsu.edu.
[*]School of Electrical, Computer and Energy Engineering, Arizona State University
Tempe, AZ 85287, USA, Email: mmorad11@asu.edu.
[‡]Departments of Mathematics and Electrical Engineering, University of Notre Dame
Notre Dame, IN 46556, USA, Email: rsmarand@nd.edu.

***Abstract*—This paper presents a finite-length polynomial-domain formulation of lifted-product quantum low-density parity-check (QLDPC) codes. We formulate the code construction over the quotient ring $\mathbb{F}_2[D]/(D^L+1)$, where polynomial base matrices are lifted entrywise to binary circulant blocks. This representation gives a compact algebraic description of the lifted-product parity-check matrices and allows CSS orthogonality to be analyzed before binary expansion. We show that the standard circulant lifting map is compatible with polynomial conjugation, which implies that the resulting binary matrices satisfy the CSS commutation constraint. The construction is illustrated with a constraint length 7, rate $1/2$ NASA convolutional code example, and numerical examples are provided from a 3×4 polynomial parity-check matrix. The finite-length performance of selected constructed codes is then evaluated over the depolarizing channel using various benchmark decoders. The resulting framework gives a structured and implementation-friendly viewpoint to construct finite-length lifted-product QLDPC codes from small polynomial base matrices.**

I. Introduction

QUANTUM error correction is essential for reliable quantum information processing in the presence of noise and decoherence. Within this area, Calderbank–Shor–Steane (CSS) codes provide one of the main algebraic frameworks to construct stabilizer codes from classical linear codes [1]–[3]. Among modern CSS-based families, quantum low-density parity-check (QLDPC) codes have attracted particular attention because they offer sparse parity-check operators together with the possibility of nonzero asymptotic rate and growing minimum distance [4], [5]. A foundational step in this direction was the hypergraph-product (HGP) construction of Tillich and Zémor, which showed how tensor-product structure can be used to obtain quantum LDPC codes with positive rate and minimum distance proportional to the square root of the block length [6].

More recently, Panteleev and Kalachev introduced the lifted-product (LP) framework, which generalizes product constructions for quantum codes and chain complexes and led to quantum LDPC codes with almost linear growth of minimum distance [7]. In subsequent work, they showed that lifted products over non-abelian groups yield asymptotically good quantum LDPC codes, thereby establishing a major breakthrough in the theory of QLDPC constructions [8]. These results make the lifted product one of the central modern tools for building structured quantum codes. At the same time, practical implementations often require finite-length codes with explicit algebraic descriptions, controlled block size, and constructions that remain compatible with structured hardware-oriented representations.

One natural way to realize such structure is through polynomial and quasi-cyclic descriptions. Classical LDPC block and convolutional codes based on circulant matrices provide a convenient algebraic language for lifting small base matrices into large sparse binary parity-check matrices [9]–[11]. In the LP setting, this point of view is especially useful because it allows the base matrices to be written over the quotient ring $\mathbb{F}_2[D]/(D^L+1)$ and then lifted entrywise to binary circulant blocks. Recent work on finite-length lifted-product QLDPC codes has shown that, in the quasi-cyclic setting, detailed combinatorial constraints on the base matrices can strongly affect the resulting quantum minimum distance and degeneracy properties [12], [13]. This highlights the need for a clean algebraic formulation of the LP construction that makes the orthogonality mechanism transparent in the polynomial domain.

In this paper, we explore the finite-length polynomial-domain formulation of LP-QLDPC codes. In particular, we formulate the LP parity-check matrices directly over the quotient ring $R_L = \mathbb{F}_2[D]/(D^L+1)$, so that small polynomial base matrices provide compact descriptions of the corresponding circulant-lifted binary parity-check matrices. We then prove that standard circulant lifting is conjugate-compatible and use this property to give a compact polynomial-domain proof of the CSS commutation condition $H_X H_Z^T = 0$. This framework also connects convolutional-code polynomial parity-check matrices with finite-length LP-QLDPC construction through tail-biting circulant lifting. This provides a polynomial-domain construction and verification framework that can be used together with existing finite-length search and distance-optimization methods. The approach is illustrated with a constraint length 7, rate $R = 1/2$ NASA convo-

lutional code example, and additional numerical examples are provided from a 3×4 polynomial parity-check matrix. The finite-length performance of selected constructed codes is then evaluated over the depolarizing channel using various benchmark decoders.

II. Background

A. Polynomial Rings and Quotient Structures

Definition 1 (Polynomial Ring)**.** *The polynomial ring $\mathbb{F}_2[D]$ consists of all polynomials in the indeterminate D with coefficients in the field $\mathbb{F}_2$, with addition and multiplication defined by standard polynomial arithmetic modulo 2.*

Definition 2 (Quotient Ring)**.** *For a positive integer L, the quotient ring $R_L \triangleq \mathbb{F}_2[D]/(D^L+1)$ is the set of equivalence classes of polynomials in $\mathbb{F}_2[D]$ under the equivalence relation $p(D) \sim q(D)$ if and only if $p(D)-q(D)$ is divisible by D^L+1.*

Since the field has characteristic two, the relation $D^L + 1 = 0$ in R_L implies $D^L = 1$. Hence, exponents are reduced modulo L, and $D^{-1} \cong D^{L-1}$ in R_L.

Definition 3 (Polynomial conjugation)**.** *For $p(D) = \sum_{i=0}^{L-1} a_i D^i \in R_L$, define the conjugate (involution) $p(D)^* \in R_L$ by*

$$p(D)^* \triangleq \sum_{i=0}^{L-1} a_i D^{-i} = \sum_{i=0}^{L-1} a_i D^{(L-i) \bmod L}.$$

Definition 4 (CSS Code)**.** *An [[N,K,d]] CSS quantum code is specified by two binary parity-check matrices $H_X, H_Z \in \mathbb{F}_2^{r_X \times N}$ and $\mathbb{F}_2^{r_Z \times N}$ satisfying the CSS commutation condition*

$$H_X H_Z^T = 0.$$

Equivalently, $\mathrm{row}(H_X) \subseteq \ker(H_Z), \quad \mathrm{row}(H_Z) \subseteq \ker(H_X)$. *The number of logical qubits is $K = N - \mathrm{rank}(H_X) - \mathrm{rank}(H_Z)$. The quantum minimum distance is $d = \min\{d_X, d_Z\}$, where*

$$d_X = \min\{\mathrm{wt}(x) | x \in \ker(H_Z) \setminus \mathrm{row}(H_X)\},$$

and

$$d_Z = \min\{\mathrm{wt}(z) | z \in \ker(H_X) \setminus \mathrm{row}(H_Z)\}.$$

B. Circulant Matrices and Lifting

In this section, we formalize the basic objects that we will use repeatedly: circulant permutation matrices, the lifting operation from polynomials to circulant matrices, and the resulting polynomial–circulant correspondence [9].

Definition 5 (Circulant permutation matrix)**.** *Let $L \in \mathbb{N}$ and $0 \le s < L$. The $L \times L$* circulant permutation matrix $\mathrm{Circ}_L(s)$ *is defined by*

$$\big(\mathrm{Circ}_L(s)\big)_{i,j} = \begin{cases} 1, & \text{if } j \equiv i + s \pmod{L}, \\ 0, & \text{otherwise}, \end{cases}$$

for $i, j \in \{0, 1, \ldots, L-1\}$. Equivalently, $\mathrm{Circ}_L(s)$ represents a cyclic shift of the identity matrix row-by-row by s positions to the right.

We now formalize the lifting operation that associates a binary circulant matrix to each polynomial in $\mathbb{F}_2[D]/(D^L+1)$. (This operation gives a finite circulant, or tail-biting, block representation of polynomial convolutional-code components.)

Definition 6 (Lifting operation for polynomials)**.** *Fix $L \in \mathbb{N}$ and consider the ring $\mathbb{F}_2[D]/(D^L+1)$. For a polynomial*

$$p(D) = \sum_{i=0}^{L-1} a_i D^i \in \mathbb{F}_2[D]/(D^L+1), \qquad a_i \in \mathbb{F}_2,$$

the lifting operation $\mathcal{L}_L$ *maps $p(D)$ to an $L \times L$ binary matrix*

$$\mathcal{L}_L(p) \triangleq \sum_{i=0}^{L-1} a_i \,\mathrm{Circ}_L(i),$$

where the sum is taken over $\mathbb{F}_2$ (entrywise modulo 2).

Intuitively, the coefficient $a_i = 1$ tells us to add the circulant permutation matrix corresponding to a shift by i positions; if $a_i = 0$, that shift is absent. The first row of $\mathcal{L}_L(p)$ is exactly the coefficient vector $(a_0, a_1, \ldots, a_{L-1})$, and all other rows are its cyclic shifts. Now we extend this lifting operation entrywise to polynomial matrices.

Definition 7 (Polynomial–circulant correspondence)**.** *Let $P(D) = \big(p_{ij}(D)\big)$ be an $m \times n$ matrix with entries in $\mathbb{F}_2[D]/(D^L+1)$. The* lifting *(or* polynomial–circulant correspondence*) associates to $P(D)$ the binary matrix*

$$\mathcal{L}_L\big(P(D)\big) \triangleq \big(\mathcal{L}_L(p_{ij}(D))\big)_{i,j} \in \mathbb{F}_2^{mL \times nL},$$

i.e., each scalar entry $p_{ij}(D)$ is replaced by the $L \times L$ circulant matrix $\mathcal{L}_L\big(p_{ij}(D)\big)$ from Definition 6. The resulting $mL \times nL$ matrix is block-circulant with $L \times L$ blocks.

C. Depolarizing Channel Model and BP-based Decoders

To evaluate the finite-length error-correction performance of our constructed codes, we will later use several standard BP-based decoders over the depolarizing channel. The quaternary belief propagation (QBP) decoder [14] performs message passing on the CSS Tanner graphs while keeping a local belief over the four Pauli symbols $\{I, X, Y, Z\}$. Under the depolarizing channel, the error on qubit i satisfies

$$\Pr(q_i = I) = 1 - p,$$

$$\Pr(q_i = X) = \Pr(q_i = Y) = \Pr(q_i = Z) = \frac{p}{3}.$$

Unlike independent X- and Z-component decoding, QBP accounts for the coupling introduced by the Y error. The decoder iteratively updates the messages and returns a hard Pauli estimate, which is then checked for syndrome consistency and logical correctness.

In QBP with guided decimation (QBPGD) [15], short runs (T iterations) of the QBP decoder are interleaved with G reliability-based decimation steps. At each decimation step, one highly reliable qubit is fixed, and QBP is then restarted on the reduced problem. This procedure helps break symmetric message-passing failures caused by short cycles and degeneracy, but it can increase the decoding cost because several QBP runs may be required. We also evaluate our codes using a reinforcement-learning-based sequential decoder (RL-S) [16]. It uses the same underlying BP message-update rules, but replaces the flooding schedule with a learned sequential

variable-node update order. The learned policy is trained offline and then used during inference to select the next variable node based on a local syndrome-driven state.

III. The Conjugate Transpose Operation in Quotient Rings

We now define and establish basic algebraic properties of the conjugate transpose in $\mathbb{F}_2[D]/(D^L+1)$. This operation is crucial for our approach, since it underpins the orthogonality proofs and design of LP codes.

A. Algebraic Properties

By Definition 3, polynomial conjugation is the map $p(D) \mapsto p^*(D) = p(D^{-1})$ interpreted in the quotient ring (with $D^L \equiv 1$). Conjugation is essentially a reversal of polynomial coefficients (and an inversion of the indeterminate, since $D^{-1} \equiv D^{L-1}$ in the ring).

Remark 1. *In the quotient ring $\mathbb{F}_2[D]/(D^L+1)$ we have $D^L \equiv 1$, hence $D^{-1} \equiv D^{L-1}$. If $p(D) = \sum_i a_i D^i$, then*

$$p(D^{-1}) \;=\; \sum_i a_i D^{-i} \;\equiv\; \sum_i a_i D^{L-i \bmod L},$$

which coincides with the exponent-wise definition of $p^*(D)$ in Definition 3.

B. Matrix Conjugate Operations

Lemma 1 (Basic properties of *)**.** *The map $^* : R_L \to R_L$ is $\mathbb{F}_2$-linear, involutive, and multiplicative:*

$$(p+q)^* = p^* + q^*, \qquad (p^*)^* = p, \qquad (pq)^* = p^* q^*.$$

Proof. Linearity and involution follow immediately from the definition. For multiplicativity, note that * acts as $D \mapsto D^{-1}$, and $(D^{-1})^k = D^{-k}$ in R_L. □

Definition 8 (Matrix Conjugate Transpose)**.** *For a polynomial matrix $B = [b_{ij}(D)]$ (with entries in $\mathbb{F}_2[D]/(D^L+1)$), the conjugate transpose B^* is defined by:*

$$\big(B^*\big)_{ij}(D) = \big(b_{ji}(D)\big)^*.$$

That is, B^* is the transpose of B with each entry replaced by its conjugate polynomial.

This operation is analogous to the Hermitian transpose in complex matrices, but within the ring $\mathbb{F}_2[D]/(D^L+1)$ and with conjugation as defined.

Proposition 1 (Conjugate Transpose Properties)**.** *For any conformable polynomial matrices A, B:*

- $(A+B)^* = A^* + B^*$.
- $(A \cdot B)^* = B^* \cdot A^*$.
- $(A^*)^* = A$.
- $(A \otimes B)^* = A^* \otimes B^*$.

IV. Lifted-Product Construction and Orthogonality

A. Lifting map and the conjugate-compatibility condition

We use the standard circulant lifting map from R_L to binary $L \times L$ circulant matrices.

Lemma 2 (Ring-homomorphism property)**.** *For all $p, q \in R_L$,*

$$\mathcal{L}_L(p+q) = \mathcal{L}_L(p) + \mathcal{L}_L(q), \qquad \mathcal{L}_L(pq) = \mathcal{L}_L(p)\,\mathcal{L}_L(q),$$

and the same holds entrywise for lifted matrices (block-circulant matrix multiplication).

Proof. This follows from a standard property of circulant polynomial representations: multiplication of circulant matrices corresponds to multiplication in R_L. □

Definition 9 (Conjugate-compatible lifting (explicit condition))**.** *We say that the lifting map $\mathcal{L}_L$ is* conjugate-compatible *with * if, for every $p \in R_L$,*

$$\mathcal{L}_L(p^*) = \mathcal{L}_L(p)^T.$$

Lemma 3 (Conjugate-compatibility holds for standard circulant lifting)**.** *The lifting map in Definition 6 is conjugate-compatible: $\mathcal{L}_L(p^*) = \mathcal{L}_L(p)^T$ for all $p \in R_L$. Consequently, for any matrix B over R_L,*

$$\mathcal{L}_L(B^*) = \mathcal{L}_L(B)^T.$$

Proof. It suffices to verify the claim on monomials. For $p(D) = D^i$,

$$p(D)^* = D^{-i} = D^{(L-i) \bmod L}.$$

Also, $\mathrm{Circ}_L(i)^T = \mathrm{Circ}_L(-i) = \mathrm{Circ}_L((L-i) \bmod L)$. Thus $\mathcal{L}_L((D^i)^*) = \mathcal{L}_L(D^i)^T$. This is then extended by $\mathbb{F}_2$-linearity to all $p \in R_L$ and then entrywise to matrices. □

B. Lifted-product polynomial check matrices

Let $B_1 \in R_L^{m_1 \times n_1}$ and $B_2 \in R_L^{m_2 \times n_2}$ be arbitrary polynomial parity-check base matrices. Define the asymmetric LP polynomial check matrices

$$B_X \triangleq \left[\, B_1 \otimes I_{n_2} \;\middle|\; I_{m_1} \otimes B_2^* \,\right], \text{ and} \tag{1}$$

$$B_Z \triangleq \left[\, I_{n_1} \otimes B_2 \;\middle|\; B_1^* \otimes I_{m_2} \,\right], \tag{2}$$

where $\otimes$ denotes the Kronecker product over the coefficient ring R_L and I_k is the $k \times k$ identity matrix. Then define the lifted binary parity-check matrices by

$$H_X \triangleq \mathcal{L}_L(B_X) \text{ and } H_Z \triangleq \mathcal{L}_L(B_Z).$$

C. Conditional LP orthogonality theorem

Theorem 1 (Polynomial-domain LP orthogonality)**.** *Assume the lifting map $\mathcal{L}_L$ is conjugate-compatible (Definition 9). Then for any base matrices B_1, B_2 over R_L, the lifted-product matrices satisfy*

$$H_X H_Z^T = 0 \quad \textit{over } \mathbb{F}_2.$$

Proof. We first prove the polynomial-domain identity

$$B_X\, B_Z^* = 0 \quad \text{in } R_L. \tag{3}$$

From (2) we have

$$B_Z^* = \begin{bmatrix} (I_{n_1} \otimes B_2)^* \\ (B_1^* \otimes I_{m_2})^* \end{bmatrix} = \begin{bmatrix} I_{n_1} \otimes B_2^* \\ B_1 \otimes I_{m_2} \end{bmatrix},$$

using $I_k^* = I_k$ and $(B_1^*)^* = B_1$, and the standard identity $(A \otimes C)^* = A^* \otimes C^*$. Now multiply B_X (a horizontal concatenation) by B_Z^* (a vertical concatenation):

$$B_X B_Z^* = (B_1 \otimes I_{n_2})(I_{n_1} \otimes B_2^*) + (I_{m_1} \otimes B_2^*)(B_1 \otimes I_{m_2}).$$

Because the coefficient ring R_L is commutative, the mixed-product rule for Kronecker products applies:

$$(A \otimes C)(B \otimes D) = (AB) \otimes (CD),$$

for all conformable matrices over R_L. Hence

$$(B_1 \otimes I_{n_2})(I_{n_1} \otimes B_2^*) = (B_1 I_{n_1}) \otimes (I_{n_2} B_2^*) = B_1 \otimes B_2^*,$$

and similarly

$$(I_{m_1} \otimes B_2^*)(B_1 \otimes I_{m_2}) = (I_{m_1} B_1) \otimes (B_2^* I_{m_2}) = B_1 \otimes B_2^*.$$

Therefore

$$B_X B_Z^* = (B_1 \otimes B_2^*) + (B_1 \otimes B_2^*) = 0$$

because $\mathrm{char}(R_L) = 2$. This proves (3).

Now we lift to binary matrices. By Lemma 2,

$$\mathcal{L}_L(B_X B_Z^*) = \mathcal{L}_L(B_X)\, \mathcal{L}_L(B_Z^*).$$

By conjugate-compatibility (Lemma 3),

$\mathcal{L}_L(B_Z^*) = \mathcal{L}_L(B_Z)^T = H_Z^T$. Thus

$$\begin{aligned} H_X H_Z^T &= \mathcal{L}_L(B_X)\, \mathcal{L}_L(B_Z)^T = \mathcal{L}_L(B_X)\, \mathcal{L}_L(B_Z^*) \\ &= \mathcal{L}_L(B_X B_Z^*) = \mathcal{L}_L(0) = 0. \end{aligned}$$

□

Remark 2. *Theorem 1 shows that the CSS commutation condition can be certified before binary expansion. Instead of forming the full binary matrices H_X and H_Z and then checking $H_X H_Z^T = 0$, one may verify the corresponding polynomial-domain identity over R_L.*

Example 1 (NASA constraint length 7 symmetric LP example)**.** *Consider the NASA constraint length 7, rate $R = 1/2$ convolutional code [17] with polynomial base matrix*

$$B(D) = \begin{bmatrix} h_{11}(D) & h_{12}(D) \end{bmatrix} \in R_7^{1\times 2}, \quad R_7 = \mathbb{F}_2[D]/(D^7+1),$$

where

$$h_{11}(D) = 1 + D + D^3 + D^4 + D^6,$$
$$h_{12}(D) = 1 + D^3 + D^4 + D^5 + D^6.$$

We take the symmetric lifted-product construction, so that $B_1 = B_2 = B$, $m = 1$, $n = 2$.

By Definition 3, the conjugates are

$$h_{11}^*(D) = h_{11}(D), \quad h_{12}^*(D) = 1 + D + D^2 + D^3 + D^4.$$

Hence the polynomial LP check matrices are

$$\begin{aligned} B_X &= \left[\, B \otimes I_2 \;\middle|\; I_1 \otimes B^* \,\right] \\ &= \begin{pmatrix} h_{11}(D) & 0 & h_{12}(D) & 0 & h_{11}^*(D) \\ 0 & h_{11}(D) & 0 & h_{12}(D) & h_{12}^*(D) \end{pmatrix}. \end{aligned}$$

and

$$\begin{aligned} B_Z &= \left[\, I_2 \otimes B \;\middle|\; B^* \otimes I_1 \,\right] \\ &= \begin{pmatrix} h_{11}(D) & h_{12}(D) & 0 & 0 & h_{11}^*(D) \\ 0 & 0 & h_{11}(D) & h_{12}(D) & h_{12}^*(D) \end{pmatrix}. \end{aligned}$$

Now apply the standard circulant lifting map $\mathcal{L}_7(\cdot)$ entry-wise to obtain the binary parity-check matrices

$$H_X = \mathcal{L}_7(B_X), \qquad H_Z = \mathcal{L}_7(B_Z).$$

Since $m = 1$, $n = 2$, and $L = 7$, both lifted matrices have $(n^2+m^2)L = (2^2+1^2)\cdot 7 = 35$ columns and $mnL = 1\cdot 2\cdot 7 = 14$ rows. Therefore, $H_X, H_Z \in \mathbb{F}_2^{14\times 35}$.

Moreover, the standard circulant lift is conjugate-compatible, i.e.,

$$\mathcal{L}_7(p^*(D)) = \mathcal{L}_7(p(D))^T, \quad \text{for all} \quad p(D) \in R_7.$$

Therefore, by Theorem 1, $H_X H_Z^T = 0$, so the lifted pair (H_X, H_Z) defines a valid CSS code.

This example is intended only to illustrate the polynomial-domain construction in Theorem 1 and the conjugate-compatible lifting argument that guarantees $H_X H_Z^T = 0$.

V. Numerical Results

In this section, we provide finite-length examples obtained from the polynomial-domain lifted-product construction of Theorem 1 and evaluate the resulting QLDPC codes using the benchmark decoders described in Section II-C. For QBP and RL-S, we set a maximum number of iterations T as noted in each figure. For QGBPD, we set T =100 and $G = n$, for a total maximum of GT iterations. We use

$$B_1(D) = B_2(D) = H(D),$$

where

$$H(D) = \begin{pmatrix} D^{50} & D^{105} & D^{74} & D^4 \\ D^8 + D^{30} & D^7 + D^{105} & D^{80} & D^{73} \\ D^{28} & D^{37} & D^{73} & D^{13} \end{pmatrix}.$$

The base matrix $H(D)$ was selected through a computational search over small 3×4 polynomial matrices. We focused on full-support polynomial seeds that remain sparse after circulant lifting while providing enough algebraic structure to produce nonzero-rate LP codes with balanced X- and Z-distance behavior. The selected seed gave the strongest finite-length results among the candidates considered. For each lifting size L, the entries of $H(D)$ are reduced modulo D^L+1, and the lifted-product CSS parity-check matrices are formed according to Theorem 1 with $B_1 = B_2 = H$.

The parameters of the codes obtained from the available computations are summarized in Table I. The table shows that changing the lifting size L produces a family of structured finite-length QLDPC codes with different block lengths, dimensions, and distance estimates. In the following simulations, we focus on selected members of this family and compare QBP, QBPGD, and RL-S over the depolarizing channel. For these decoders, T is the maximum number of iterations allowed and in the case of QBPGD the total is multiplied by the rounds of decimation G. The reported metric is the block error rate, *i.e.*, the probability that the decoder either fails to return a consistent syndrome or returns a recovery in the wrong logical coset.

TABLE I
Parameters of the lifted-product codes obtained from the 3×4 polynomial base matrix with $B_1(D) = B_2(D) = H(D)$.

L	n	k	d_X	d_Z	d
10	250	18	8	8	8
11	275	15	12	12	12
12	300	20	12	12	12
13	325	17	14	14	14
14	350	22	12	12	12
15	375	19	16	16	16
16	400	24	13	13	13
17	425	21	18	18	18
24	600	32	≤ 20	≤ 20	≤ 20
41	1025	45	≤ 26	≤ 26	≤ 26
83	2075	87	≤ 34	≤ 34	≤ 34

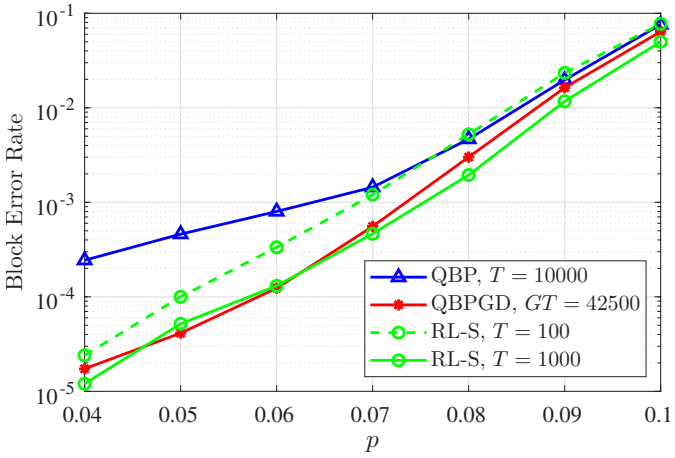

Fig. 1. Block error rate comparison for the constructed $[[425, 21, 18]]$ lifted-product QLDPC code obtained from the 3×4 polynomial base matrix with lifting size $L = 17$.

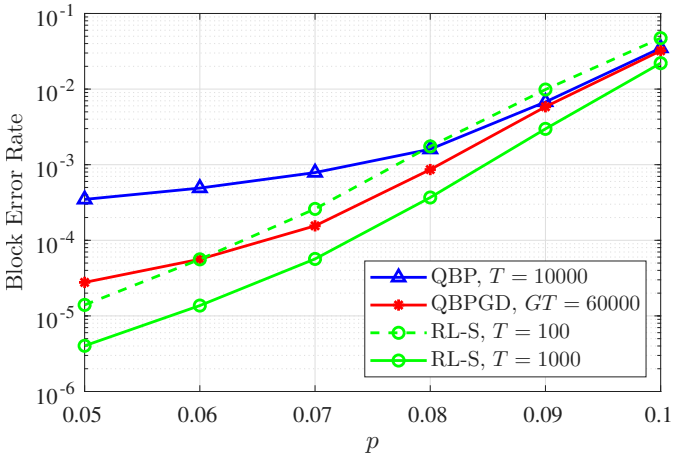

Fig. 2. Block error rate comparison for the constructed $[[600, 32, d \leq 20]]$ lifted-product QLDPC code obtained from the 3×4 polynomial base matrix with lifting size $L = 24$.

Fig. 1 shows the block error rate performance of our constructed $[[425, 21, 18]]$ code corresponding to $L = 17$. We compare QBP, QBPGD, and RL-S with different iteration budgets. The results show that the constructed code can be decoded effectively by BP-based methods over the depolarizing channel. Fig. 2 considers the constructed length $n = 600$ code obtained with lifting size $L = 24$. For this code, $k = 32$ and a minimum distance search gives $d_X, d_Z, d \leq 20$, as shown in Table I. The same set of benchmark decoders is used over the depolarizing channel. The results show that the RL-S scheme improves the block error rate relative to QBP. In particular, RL-S with a larger iteration budget gives the best performance among the plotted decoders.

Finally, Fig. 3 evaluates a larger constructed code with block length $n = 2075$, corresponding to lifting size $L = 83$. For this code, $k = 87$ and a minimum distance search gives $d_X, d_Z, d \leq 34$. For this construction, we observe that the QBP and QBPGD show a severe error floor, but that the RL-S decoder does not. This is due, in part, to the large number

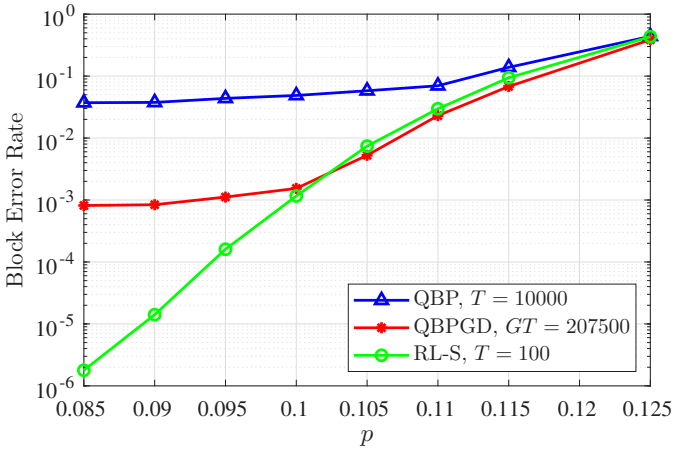

Fig. 3. Block error rate comparison for the constructed $[[2075, 87, d \leq 34]]$ lifted-product QLDPC code obtained from the 3×4 polynomial base matrix with lifting size $L = 83$.

of 4-cycles in the graph (30,378 4-cycles). The observed improvement is consistent with our previous results for RL decoding of polar codes [18], for which the graphs also have large numbers of 4-cycles and for which the agent can effectively optimize the message passing schedule to mitigate that weakness.

VI. Concluding Remarks

We presented a polynomial-domain formulation of finite-length lifted-product QLDPC codes over the quotient ring $R_L = \mathbb{F}_2[D]/(D^L + 1)$. In this formulation, small polynomial base matrices are lifted entrywise to binary circulant blocks, giving a compact representation of the full binary parity-check matrices. The main algebraic contribution is the identification and use of conjugate-compatible circulant lifting. This property allows the CSS commutation condition $H_X H_Z^T = 0$ to be proved directly in the polynomial domain before binary expansion. This viewpoint connects classical convolutional-code polynomial descriptions with finite-length LP-QLDPC code construction. We illustrated the construction using a constraint length 7 NASA convolutional code and a 3×4 polynomial base matrix, producing a family of structured finite-length QLDPC codes. Selected examples were evaluated over the depolarizing channel using BP-based decoders, showing that the constructed codes are compatible with practical iterative decoding methods.

The present work should be viewed as a description and verification framework that can be used for new LP-QLDPC code design rather than a new asymptotic LP result. Future work includes combining this polynomial-domain formulation with systematic distance-search constraints, optimizing the choice of polynomial base matrices, and designing syndrome-extraction schedules adapted to the resulting circulant-lifted structure.

Acknowledgement

This material is based upon work supported by the National Science Foundation under Grant No. CCF-2145917.

REFERENCES

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

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

[3] D. Gottesman, *Stabilizer codes and quantum error correction*. California Institute of Technology, 1997.

[4] D. J. MacKay, G. Mitchison, and P. L. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2315–2330, 2004.

[5] N. P. Breuckmann and J. N. Eberhardt, "Balanced product quantum codes," *IEEE Transactions on Information Theory*, vol. 67, no. 10, pp. 6653–6674, 2021.

[6] J.-P. Tillich and G. Zémor, "Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength," *IEEE Transactions on Information Theory*, vol. 60, no. 2, pp. 1193–1202, 2013.

[7] P. Panteleev and G. Kalachev, "Quantum LDPC codes with almost linear minimum distance," *IEEE Transactions on Information Theory*, vol. 68, no. 1, pp. 213–229, 2022.

[8] ——, "Asymptotically good quantum and locally testable classical LDPC codes," in *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, 2022, pp. 375–388.

[9] R. M. Tanner, D. Sridhara, A. Sridharan, T. E. Fuja, and J. Costello, Daniel J., "LDPC block and convolutional codes based on circulant matrices," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 2966–2984, 2004.

[10] R. Smarandache and P. O. Vontobel, "Quasi-cyclic LDPC codes: Influence of proto-and Tanner-graph structure on minimum Hamming distance upper bounds," *IEEE Transactions on Information Theory*, vol. 58, no. 2, pp. 585–607, 2012.

[11] A. A. Kovalev and L. P. Pryadko, "Quantum Kronecker sum-product low-density parity-check codes with finite rate," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 88, no. 1, p. 012311, 2013.

[12] N. Raveendran, D. Declercq, and B. Vasić, "On the minimum distances of finite-length lifted product quantum LDPC codes," *arXiv preprint arXiv:2503.07567*, 2025.

[13] P. Panteleev and G. Kalachev, "Degenerate quantum LDPC codes with good finite length performance," *Quantum*, vol. 5, p. 585, 2021.

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

[15] H. Yao, W. Abu Laban, C. Häger, A. Graell i Amat, and H. D. Pfister, "Belief propagation decoding of quantum LDPC codes with guided decimation," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, 2024, pp. 2478–2483.

[16] M. Moradi, V. Nourozi, S. Habib, and D. G. M. Mitchell, "Learning to decode quantum LDPC codes via belief propagation," 2026.

[17] J. Hamkins, "A joint receiver-decoder for convolutionally coded binary phase-shift keying (BPSK)," *TMO Progress Report*, pp. 42–139, 1999.

[18] M. Moradi, S. Habib, and D. G. M. Mitchell, "Enhancing belief propagation decoding of polar codes: A reinforcement learning approach," *IEEE Communications Letters*, vol. 29, no. 6, pp. 1285–1289, 2025.