

### C. Orthogonality Condition for Base Matrices

A necessary and sufficient condition for a pair of QC-LDPC codes to satisfy the symplectic inner product condition is given in [29]. We revisit the even multiplicity condition described therein first.

*Definition 1 (Even multiplicity):* A vector  $\mu = (\mu_1, \mu_2, \dots, \mu_n)$  is said to have even multiplicity if, for every integer  $k \in \mathbb{Z}$ , the number of indices  $i \in \{1, 2, \dots, n\}$  such that  $\mu_i = k$  is even.

By definition, the vector has even multiplicity if each integer entry in  $\mu$  appears an even number of times while discounting the  $-\infty$  entries or the empty cells if any.

*Even multiplicity and orthogonal base matrices:* Let  $B$  be a base matrix in exponent form of size  $m \times n$  with circulant size  $L$ , where the entries  $b_{i,j} \in \{-\infty, 0, 1, \dots, L-1\}$ . Define the  $i$ -th row vector  $\mathbf{r}_i$  for  $i = 1, 2, \dots, m$  as  $\mathbf{r}_i = [b_{i,1}, b_{i,2}, \dots, b_{i,n}]$ . If the modulo- $L$  difference of any two distinct rows  $\mathbf{r}_i$  and  $\mathbf{r}_j$ : i.e.,  $\mathbf{r} = \mathbf{r}_i - \mathbf{r}_j$ , modulo- $L$ , has even multiplicity, then the corresponding binary matrices after lifting  $\mathbb{L}(\mathbf{r}_i)$  and  $\mathbb{L}(\mathbf{r}_j)$  are orthogonal [29], [30]. The minus  $-$  operation is performed modulo- $L$  and for the  $\infty$  entries is as follows:  $b_{i,j} - \infty = \infty - b_{i,j} = \infty - \infty := -\infty$ .

*Theorem 1:* LP-QLDPC code PCMs  $\mathbf{H}_X$  and  $\mathbf{H}_Z$  are orthogonal if the rows of quasi-cyclic base matrices  $B_X$  and  $B_Z$  have even multiplicity.

*Proof:* To prove the orthogonality property for quasi-cyclic LP-QLDPC code parity check matrices, one can check the even multiplicity property for the base matrices  $B_X$  and  $B_Z$ . Their rows obey the condition for orthogonality - the even multiplicity of integers in the modulo- $L$  differences of the rows, where  $L$  is the circulant size. Take any pair of rows such that  $\mathbf{r}_i$  is taken from  $B_X$ , and  $\mathbf{r}_j$  from  $B_Z$ . These rows can be split based on the left part and right part - with exactly one overlap in each of the parts. Thus, the difference  $\mathbf{r} = \mathbf{r}_i - \mathbf{r}_j$ , modulo- $L$  will only have two integer terms. Suppose that the two overlapping terms are equal; then, the resulting difference vector has a pair of zeros. If the overlapping terms  $p$  and  $q$  are not equal,  $p \neq q$ , then the corresponding terms in the difference appear as  $p - q$  and  $q^* - p^*$ , respectively. Since the conjugate terms are  $q^* = L - q$  and  $p^* = L - p$ , the overlapping terms are indeed equal, satisfying the even multiplicity condition. Therefore, the two parity check matrices are orthogonal to each other.  $\square$

### IV. MINIMUM DISTANCE OF LP-QLDPC CODES

In the following, we examine the symmetric LP-QLDPC codes constructed from type-1 quasi-cyclic base matrices to understand how certain combinations of CPM values reduce the quantum minimum distance  $d_{\min}^Q$  from the minimum distance of the base code  $d_{\min}^C$ . We first show how the minimum distance is limited to the Hamming weight of the stabilizer generators. We also prove that using a base matrix with only two rows ( $m = 2$  as in Eq. (11)) always limits the LP-QLDPC code to have a minimum distance  $d_{\min}^Q \leq n + 2$ . In general, we are interested in the following question: What constraints on the base code of an LP-QLDPC code reduce its minimum distance? This will guide us toward code construction recipes guarantee degeneracy for the obtained LP-QLDPC code. First, we provide examples of the choices of base codes of different sizes:  $m$  and  $n$  to demonstrate the reduction of the minimum distance of LP-QLDPC codes.

*Example 1 Continued:* Consider the LP-QLDPC code constructed from the example base matrix we saw earlier with  $m = 2, n = 3, L = 7$ ,

$$B = \begin{bmatrix} 1 & 2 & 4 \\ 6 & 5 & 3 \end{bmatrix}. \quad (23)$$

We start with a classical LDPC code  $\mathcal{C} : [21, 8, 6]$ . Hence, the desired minimum distance of LP code is  $d_{\min}^C = 6$ . However, we verified that the  $d_{\min}^Q = m + n = 5$ . Note that for quasi-cyclic base matrices, it is enough to look at equivalent base matrices expressed in canonical form. Two base matrices are equivalent if their respective Tanner graphs are identical upon variable and/or check node permutations. Given a base matrix,  $B$  exchanging rows/columns, or adding a fixed integer to each element in row/column maintains equivalence. The rows and columns of the quasi-cyclic code can be reordered to put 0s in the first row and column to make an equivalent parity check matrix making the analysis easier. For instance, we have the equivalent matrix

$$B = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 3 \end{bmatrix}. \quad (24)$$

*Example 2:* Classical code  $\mathcal{C} : [104, 30, 14]$  with the base matrix given in Example 3 of [18]. We obtain the base matrix for the classical LDPC code  $\mathcal{C} : [104, 30, 14]$ . The base matrix  $B$  in Eq. (25) corresponds to a  $(3, 4)$  regular LDPC code with circulant size  $L = 26$ . The minimum distance of the base code is  $d_{\min}^C = 14$ .

$$B = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 6 & 4 & 10 \\ 0 & 8 & 14 & 22 \end{bmatrix}. \quad (25)$$

We now construct a symmetric LP-QLDPC code from Eq. (25) to get a  $[[650, 50, 7]]$  code. Here, we have  $N = 26 \times (3^2 + 4^2)$  physical qubits encoding  $K = 50$  logical qubits with a minimum distance  $d_{\min}^Q = 7$  instead of 14. Note that the quantum minimum distance is again equal to  $m + n$ .