

High-threshold and low-overhead fault-tolerant quantum memory

Sergey Bravyi¹, Andrew W. Cross¹, Jay M. Gambetta¹, Dmitri Maslov¹, Patrick Rall², and Theodore J. Yoder¹

¹IBM Quantum, IBM T.J. Watson Research Center, Yorktown Heights, NY 10598 (USA)

²IBM Quantum, MIT-IBM Watson AI Lab, Cambridge, MA 02142 (USA)

August 16, 2023

Abstract

Quantum error correction becomes a practical possibility only if the physical error rate is below a threshold value that depends on a particular quantum code, syndrome measurement circuit, and a decoding algorithm. Here we present an end-to-end quantum error correction protocol that implements fault-tolerant memory based on a family of LDPC codes with a high encoding rate that achieves an error threshold of 0.8% for the standard circuit-based noise model. This is on par with the surface code which has remained an uncontested leader in terms of its high error threshold for nearly 20 years. The full syndrome measurement cycle for a length- n code in our family requires n ancillary qubits and a depth-7 circuit composed of nearest-neighbor CNOT gates. The required qubit connectivity is a degree-6 graph that consists of two edge-disjoint planar subgraphs. As a concrete example, we show that 12 logical qubits can be preserved for ten million syndrome cycles using 288 physical qubits in total, assuming the physical error rate of 0.1%. We argue that achieving the same level of error suppression on 12 logical qubits with the surface code would require more than 4000 physical qubits. Our findings bring demonstrations of a low-overhead fault-tolerant quantum memory within the reach of near-term quantum processors.

1 Introduction

Quantum computing attracted attention due to its ability to offer asymptotically faster solutions to a set of computational problems compared to the best known classical algorithms [1]. It is believed that a scalable functioning quantum computer may help solve computational problems in such areas as scientific discovery, materials research, chemistry, and drug design, to name a few [2, 3, 4, 5].

The main obstacle to building a quantum computer is the fragility of quantum information, owing to various sources of noise affecting it. Since isolating a quantum computer from external effects and controlling it to induce a desired computation are in conflict with each other, noise appears to be inevitable. The sources of noise include imperfections in qubits, materials used, controlling apparatus, State Preparation and Measurement (SPAM) errors, and a variety of external factors ranging from local man-made, such as stray electromagnetic fields, to those inherent to the Universe, such as cosmic rays. See Ref. [6] for a summary. While some sources of noise can be eliminated with better control [7], materials [8], and shielding [9, 10, 11], a number of other sources appear to be difficult if at all possible to remove. The latter kind can include spontaneous and stimulated emission in trapped ions [12, 13], and the interaction with the bath (Purcell Effect) [14] in superconducting circuits—covering both leading quantum technologies. Thus, error correction becomes a key requirement for building a functioning scalable quantum computer.

The possibility of quantum fault tolerance was established earlier [15]. Encoding a logical qubit redundantly into many physical qubits enables one to diagnose and correct errors by repeatedly measuring syndromes of parity check operators. However, error correction is only beneficial if the hardware error rate is below a certain threshold value that depends on a particular error correction protocol. The first proposals for quantum error correction, such as concatenated codes [16, 17, 18], focused on demonstrating the theoretical possibility of error suppression. As understanding of quantum error correction and the capabilities of quantum technologies matured, the focus shifted to finding practical quantum error correction protocols. This resulted in the development of the surface code [19, 20, 21, 22] that offers a high error threshold close to 1%, fast decoding algorithms, and compatibility with the existing quantum processors relying on 2-dimensional (2D) square lattice qubit connectivity. Small examples of the surface code with a single logical qubit have been already demonstrated experimentally by several groups [23, 24, 25, 26, 27]. However, scaling up the surface code to a hundred or more logical qubits would be prohibitively expensive due to its poor encoding efficiency. This spurred interest in more general quantum codes known as Low-Density Parity-Check (LDPC) codes [28]. Recent progress in the study of LDPC codes suggests that they can achieve quantum fault-tolerance with a much higher encoding efficiency [29]. Here, we focus on the study of LDPC codes, as our goal is to find quantum error correction codes and protocols that are both efficient and possible to demonstrate in practice, given the limitations of quantum computing technologies.

A quantum error correcting code is of LDPC type if each check operator of the code acts only on a few qubits and each qubit participates only in a few checks. Multiple variants of the LDPC codes have been proposed recently including hyperbolic surface codes [30], hypergraph product [31], balanced product codes [32], two-block codes based on finite groups [33, 34, 35, 36], and quantum Tanner codes [37, 38]. The latter were shown [37, 38] to be asymptotically “good” in the sense of offering a constant encoding rate and linear distance – a parameter quantifying the number of correctable errors. In contrast, the surface code has an asymptotically zero encoding rate and only square-root distance. Replacing the surface code with a high-rate, high-distance LDPC code could have major practical implications. First, fault-tolerance overhead (the ratio between the number of physical and logical qubits) could be reduced dramatically. Secondly, high-distance codes exhibit a very sharp decrease in the logical error rate: as the physical error probability crosses the threshold value, the amount of error suppression achieved by the code can increase by orders of magnitude even with a small reduction of the physical error rate. This feature makes high-distance LDPC codes attractive for near-term demonstrations which are likely to operate in the near-threshold regime. However, the performance of more general LDPC codes for realistic noise models including memory, gate, and SPAM errors remained largely unknown due to the absence of efficient decoding algorithms. Furthermore, it was believed that realizing more general LDPC codes on hardware requires prohibitively high qubit connectivity.

Here we present several concrete examples of high-rate LDPC codes with a few hundred physical qubits equipped with a low-depth syndrome measurement circuit, an efficient decoding algorithm, and a fault-tolerant protocol for addressing individual logical qubits. These codes exhibit an error threshold close to 1%, show excellent performance in the near-threshold regime, and offer nearly 15X reduction of the encoding overhead compared with the surface code. Hardware requirements for realizing our error correction protocols are relatively mild, as each physical qubit is coupled by two-qubit gates with only six other qubits. Although the qubit connectivity graph is not locally embeddable into a 2D grid, it can be decomposed into two planar degree-3 subgraphs. As we argue below, such qubit connectivity is well-suited for architectures based on superconducting qubits. Before stating our results, let us describe several must-have features for a quantum error-correcting code to be suitable for near-term experimental demonstrations and formally pose the problem addressed in this work.

2 Code selection criteria

In this work, we study the problem of realizing a fault-tolerant quantum memory with a small qubit overhead and a large code distance. Our goal is to construct a combination of the LDPC code, syndrome measurement circuitry, and

the decoding (error correction) algorithms, suitable for a near-term demonstration, but also offering long-term utility, while taking into account the capabilities and limitations of the superconducting circuits quantum hardware. In other words, we seek to develop a practical error correction protocol. Our selection criteria reflect this goal.

We focus on encoding $k \gg 1$ logical qubits into n data qubits and use c ancillary check qubits to measure the error syndrome. In total, the code relies on $n + c$ physical qubits. The net encoding rate is therefore

$$r = \frac{k}{n + c}.$$

For example, the standard surface code architecture encodes $k = 1$ logical qubit into $n = d^2$ data qubits for a distance- d code and uses $c = n - 1$ check qubits for syndrome measurements. The net encoding rate is $r \approx 1/(2d^2)$, which quickly becomes impractical as one is forced to choose a large code distance, due to, for instance, the physical errors being close to the threshold value. In contrast, we seek a high-rate LDPC code with $r \gg 1/d^2$.

To prevent the accumulation of errors one must be able to measure the error syndrome frequently enough. This is accomplished by a syndrome measurement (SM) circuit that couples data qubits in the support of each check operator with the respective ancillary qubit by a sequence of CNOT gates. Check qubits are then measured revealing the value of the error syndrome. The time it takes to implement the SM circuit is proportional to its depth — the number of gate layers composed of non-overlapping CNOTs. Since new errors continue to occur while the SM circuit is executed, its depth should be minimized. Thus we seek an LDPC code with a high rate r and low-depth SM circuit.

A noisy version of the SM circuit may include several types of faulty operations such as memory errors on data or check qubits, faulty CNOT gates, qubit initializations and measurements. We consider the circuit-based noise model [22] where each operation fails with the probability p . Faults on different operations are independent. A logical error occurs when the final error-corrected state of k logical qubits differs from the initial encoded state. The probability of a logical error p_L depends on the error rate p , details of the SM circuits, and a decoding algorithm. A pseudo-threshold p_0 of an error correction protocol is defined as a solution of the break-even equation $p_L(p) = kp$. Here kp is an estimate of the probability that at least one of k unencoded qubits suffers from an error. To achieve a significant error suppression in the regime $p \sim 10^{-3}$, which is relevant for near-term demonstrations, it is desirable to have pseudo-threshold close to 1% or higher. For example, the surface code architecture achieves pseudo-threshold $p_0 \approx 1\%$ for a large enough code distance [22]. We seek a high-rate LDPC code with a low-depth SM circuit and a high pseudo-threshold.

A logical error is undetectable if it can be generated without triggering any syndromes. Such errors span at least d data qubits for a distance- d code. Let us say that a SM circuit has distance d_{circ} if it takes at least d_{circ} faulty operations in the circuit to generate an undetectable logical error. By definition, $d_{\text{circ}} \leq d$ for any distance- d code and typically $d_{\text{circ}} < d$ since a few faulty operations in the SM circuit may create a high-weight error on the data qubits. We say that a SM circuit is distance-preserving if $d_{\text{circ}} = d$ meaning the circuit is designed so as to avoid accumulating high-weight errors, which is the best one can hope for. It is preferred (but not required) that the SM circuit is distance-preserving.

Another criterion is dictated by the limited qubit connectivity of near-term quantum devices. Each quantum code can be described by a Tanner graph G such that each vertex of G represents either a data qubit or a check operator. A check vertex i and a data vertex j are connected by an edge if the i -th check operator acts non-trivially on the j -th data qubit (by applying Pauli X or Z). Figure 1 shows the Tanner graph describing a distance-3 surface code. To keep the SM circuit depth small, it is desirable that two-qubit gates such as CNOT can be applied along every edge of the Tanner graph. By construction, the Tanner graph of any LDPC code has a small degree. One drawback of high-rate LDPC codes is that their Tanner graphs may not be locally embeddable into the 2D grid [39, 40]. This poses a challenge for hardware implementation with superconducting qubits coupled by microwave resonators. A useful VLSI design concept is graph *thickness*, see [41, 29] for details. A graph $G = (V, E)$ is said to have thickness θ if one can partition its set of edges E into disjoint union of θ sets $E_1 \sqcup E_2 \sqcup \dots \sqcup E_\theta = E$ such that each subgraph (V, E_i) is planar. Informally, a graph with thickness θ can be viewed as a vertical stack of θ planar graphs. Qubit connectivity described by a planar graph (thickness $\theta = 1$) is the simplest one from hardware perspective since the couplers do not

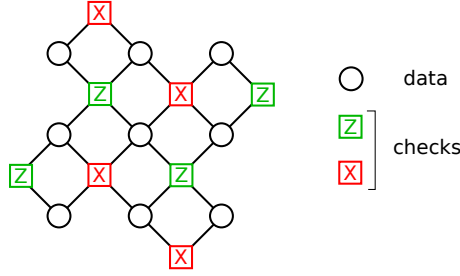


Figure 1: Tanner graph for the distance-3 surface code.

cross. Graphs with thickness $\theta = 2$ might still be implementable since two planar layers of couplers and their control lines can be attached to the top and the bottom side of the chip hosting qubits, and the two sides mated (see Section 9 for a detailed discussion). Graphs with thickness $\theta \geq 3$ are much harder to implement. Thus we seek a high-rate LDPC code with a low-depth SM circuit, high pseudo-threshold, and a low-degree Tanner graph with thickness $\theta \leq 2$.

Finally, the code must perform a useful function within a larger architecture for quantum computation, the simplest of which is a quantum memory. In a quantum memory it must be possible to measure every logical qubit in at least one Pauli basis, permitting initialization and readout of individual qubits. Furthermore it should be possible to connect the code to another error correction code and facilitate Pauli product measurements between their logical qubits. This enables load-store operations that transfer quantum data out of and into the code via quantum teleportation. For the purpose of the shorter-term goal of demonstrating the code in practice, the code should also feature enough logical operations to facilitate experiments to verify correct operation.

Our code selection criteria are summarized below.

1. We desire a code with a large distance d and a high encoding rate $r \gg 1/d^2$,
2. that is complemented by a short-depth syndrome measurement circuit,
3. offers a pseudo-threshold close to 1% (or higher) for the circuit-based noise model,
4. is constructed over thickness-2 or less Tanner graph,
5. and possesses fault-tolerant load-store operations as well as readout and initialization of individual qubits.

3 Main results

Here we give concrete examples of LDPC codes equipped with syndrome measurement circuits and efficient decoding algorithms that meet all above conditions. Our examples fall into the family of tensor product generalized bicycle codes proposed by Kovalev and Pryadko [33]. For brevity, we refer to this family as *quasi-cyclic codes*. These are stabilizer codes of CSS-type [42, 43] that can be described by a collection of few-qubit check (stabilizer) operators composed of Pauli X and Z . At a high level, a quasi-cyclic code is similar to the two-dimensional toric code [19]. In particular, physical qubits of a quasi-cyclic code can be laid out on a two-dimensional grid with periodic boundary conditions such that all check operators are obtained from a single pair of X - and Z -checks by applying horizontal and vertical shifts of the grid. However, in contrast to the plaquette and vertex stabilizers describing the toric code, check operators of a quasi-cyclic code are not geometrically local. Furthermore, each check acts on six qubits rather than

four qubits, see Figure 2 for an example. We give a formal definition of quasi-cyclic codes in Section 4. The Tanner graph of any quasi-cyclic code has vertex degree six. Although this graph may not be locally embeddable into a 2D grid, we show that it has thickness $\theta = 2$, as desired. This result may be surprising since it is known that a general degree-6 graph can have thickness $\theta = 3$, see [41].

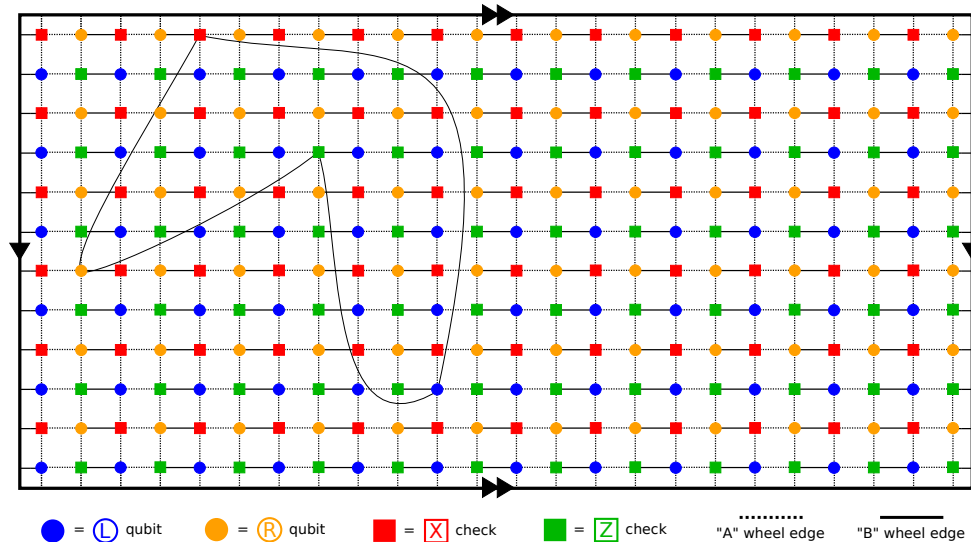


Figure 2: Tanner graph of a quasi-cyclic code with parameters $[[144, 12, 12]]$ embedded into a torus. Data qubits associated with the registers $q(L)$ and $q(R)$ defined in Section 5 are shown by bLue and oRange circles. Red and green squares stand for check qubits associated with X - and Z -type check operators. Any edge of the Tanner graph connects a data and a check vertex. Each vertex has six incident edges including four short-range edges (pointing north, south, east, and west) and two long-range edges. To avoid clutter, we only show long-range edges incident to a pair of red and green vertices. Dashed and solid edges indicate two planar subgraphs spanning the Tanner graph, each of which is isomorphic to a “wheel graph”, see Section 4.

Below we use the standard notation $[[n, k, d]]$ for code parameters. Here n is the code length (the number of data qubits), k is the number of logical qubits, and d is the code distance. Table 1 shows small examples of quasi-cyclic codes along with several metrics of the error suppression achieved by each codes. The distance-12 code $[[144, 12, 12]]$ may be the most promising for near-term demonstrations, as it combines large distance and high net encoding rate $r = 1/24$. For comparison, the distance-13 surface code has net encoding rate $r = 1/338$. Below we show that the distance-12 quasi-cyclic code outperforms the distance-13 surface code for the experimentally relevant range of error rates, see Figure 4. To the best of our knowledge, all codes shown in Table 1 are new.

To quantify the level of error suppression achieved by a code we introduce SM circuits that repeatedly measure the syndrome of each check operator. The full cycle of syndrome measurement for a length- n quasi-cyclic code requires n ancillary check qubits to store the measured syndromes. According, the net encoding rate is $r = k/(2n)$. Check qubits are coupled with the data qubits by applying a sequence of **CNOT** gates. The full cycle of syndrome measurement requires only 7 layers of **CNOTs** regardless of the code length. The check qubits are initialized and measured at the beginning and at the end of the syndrome cycle respectively, see Section 5 for details. We emphasize that our SM circuit applies to any quasi-cyclic code beyond those listed in Table 1. The circuit respects the cyclic shift symmetry of the underlying code. Assuming that the physical qubits (data or check) are located at vertices of the Tanner graph,

$[[n, k, d]]$	Net Encoding Rate r	Circuit-level distance d_{circ}	Pseudo-threshold p_0	$p_L(0.001)$	$p_L(0.0001)$
$[[72, 12, 6]]$	1/12	≤ 6	0.007(8)	4×10^{-5}	3×10^{-8}
$[[90, 8, 10]]$	1/23	≤ 8	0.007(3)	2×10^{-6}	1×10^{-10}
$[[108, 8, 10]]$	1/27	≤ 8	0.007(7)	9×10^{-7}	5×10^{-11}
$[[144, 12, 12]]$	1/24	≤ 10	0.008(3)	4×10^{-8}	2×10^{-13}
$[[288, 12, 18]]$	1/48	≤ 18	0.008(2)	5×10^{-12}	3×10^{-21}

Table 1: Small examples of quasi-cyclic LDPC codes and their performance for the circuit-based noise model. All codes have weight-6 checks, thickness-2 Tanner graph, and a depth-7 syndrome measurement circuit. A code with parameters $[[n, k, d]]$ requires $2n$ physical qubits in total and achieves the net encoding rate $r = k/2n$ (we round r down to the nearest inverse integer). Circuit-level distance d_{circ} is the minimum number of faulty operations in the syndrome measurement circuit required to generate an undetectable logical error. The pseudo-threshold p_0 is a solution of the break-even equation $p_L(p) = kp$, where p and p_L are the physical and logical error rates respectively. The logical error rate p_L was computed numerically for $p \geq 10^{-3}$ and extrapolated to lower error rates.

all CNOT gates in the SM circuit act on nearest-neighbor qubits. Thus the required qubit connectivity is described by a degree-6 thickness-2 graph, as desired. We conjecture, based on the numerical simulations, that our SM circuit is distance-preserving for the code $[[72, 12, 6]]$, see Table 1 for the upper bounds on d_{circ} (the upper bound $d_{\text{circ}} \leq 18$ for the 288-qubit code is unlikely to be tight).

The full error correction protocol performs $N_c \gg 1$ syndrome measurement cycles and calls a decoder — a classical algorithm that takes as input the measured syndromes and outputs a guess of the final error on the data qubits. Error correction succeeds if the guessed and the actual error coincide modulo a product of check operators. In this case the two errors have the same action on any encoded (logical) state. Thus applying the inverse of the guessed error would return data qubits to the initial logical state. Otherwise, if the guessed and the actual error differ by a non-trivial logical operator, error correction fails resulting in a logical error. Our numerical experiments are based on the Belief Propagation with an Ordered Statistics Decoder (BP-OSD) proposed by Panteleev and Kalachev [34]. The original work [34] described BP-OSD in the context of a toy noise model with memory errors only. Here we show how to extend BP-OSD to the circuit-based noise model. We also show that BP-OSD can be applied to other problems in quantum fault-tolerance such as estimating the distance of a quantum LDPC code, see Section 6 for details. These tasks can be accomplished with a relatively minor extension of the publicly available BP-OSD software developed by Roffe et al. [44]

Let $P_L(N_c)$ be the logical error probability after performing N_c syndrome cycles. Define the logical error rate as $p_L = 1 - (1 - P_L(N_c))^{1/N_c} \approx P_L(N_c)/N_c$. Informally, p_L can be viewed as the logical error probability per syndrome cycle. Following common practice, we choose $N_c = d$ for a distance- d code. Figure 3 shows the logical error rate achieved by codes from Table 1. The logical error rate was computed numerically for $p \geq 10^{-3}$ and extrapolated to lower error rates using a fitting formula $p_L = p^{d'_{\text{circ}}/2} e^{c_0 + c_1 p + c_2 p^2}$, where c_0, c_1, c_2 are fitting parameters and d'_{circ} is an upper bound on d_{circ} from Table 1. The observed pseudo-threshold is close to 0.008, which is nearly the same as the error threshold of the surface code [45]. To the best of our knowledge, this provides the first example of high-rate LDPC codes achieving the pseudo-threshold close to 1% under the circuit-based noise model.

For example, suppose that the physical error rate is $p = 10^{-3}$, which is a realistic goal for near-term demonstrations. Encoding 12 logical qubits using the distance-12 code from Table 1 would offer the logical error rate below 10^{-7} which is enough to preserve 12 logical qubits for nearly ten million syndrome cycles. The total number of physical qubits

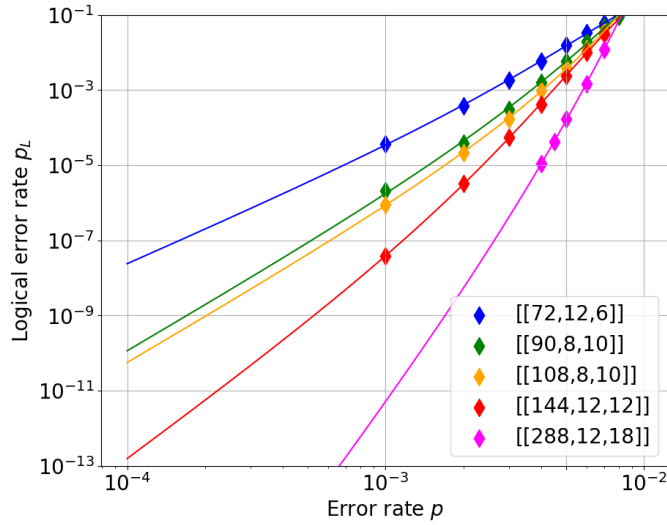


Figure 3: Logical vs physical error rate for small examples of quasi-cyclic LDPC codes. A numerical estimate of p_L (diamonds) was obtained by simulating d syndrome cycles for a distance- d code. Most of the data points have error bars $\approx p_L/10$ due to sampling errors.

required for this encoding is 288. The distance-18 code from Table 1 would require 576 physical qubits while suppressing the error rate from 10^{-3} to 10^{-11} enabling nearly hundred billion syndrome cycles. For comparison, encoding 12 logical qubits into separate patches of the surface code would require more than 4000 physical qubits to suppress the error rate from 10^{-3} to 10^{-7} , see Figure 4. In this example the distance-12 quasi-cyclic code offers nearly 15X saving in the number of physical qubits compared with the surface code.

We also find that the majority of quasi-cyclic LDPC codes admit extensions that allow them to function as a logical memory. In Section 8 we show how to use methods from [46] to attach an ancilla system to the code that permits logical measurement of all logical qubits in one of the X or Z bases. Which logical qubit is being measured can be controlled via a set of fault tolerant unitary operations. The extended Tanner graph is not only thickness-2, but the extension from the ancilla system is “effectively planar” (in a sense we define later) facilitating interconnection with other codes on the same chip.

Our findings bring experimental demonstration of high-rate LDPC codes within the reach of near-term quantum processors which are expected to offer a few hundred physical qubits, gate error rates close to 10^{-3} , and long range qubit connectivity [47].

The rest of this paper is organized as follows. Section 4 formally defines quasi-cyclic LDPC codes and proves their basic properties. The construction of the syndrome measurement circuit is detailed in Section 5. The circuit-based noise model and BP-OSD decoder for this noise model are discussed in Section 6 with some implementation details deferred to Section 7. We describe fault tolerant memory capabilities in Section 8. A summary of our findings and some open questions can be found in Section 9.

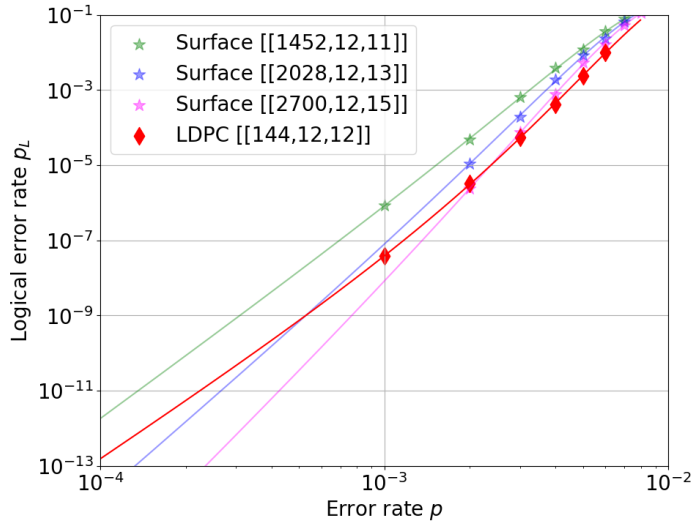


Figure 4: Comparison between the quasi-cyclic LDPC code $[[144, 12, 12]]$ and surface codes with 12 logical qubits and distance $d \in \{11, 13, 15\}$. The distance- d surface code with 12 logical qubits has length $n = 12d^2$ since each logical qubit is encoded into a separate $d \times d$ patch of the surface code lattice. The plot shows the logical error rate p_L estimated by performing d syndrome cycles for a distance- d code. Most of the data points have error bars $\approx p_L/10$ due to sampling errors.

4 Quasi-cyclic quantum LDPC codes

Let I_ℓ and S_ℓ be the identity matrix and the cyclic shift matrix of size $\ell \times \ell$ respectively. The i -th row of S_ℓ has a single nonzero entry equal to one at the column $i + 1 \pmod{\ell}$. For example,

$$S_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad S_3 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

Consider matrices

$$x = S_\ell \otimes I_m \quad \text{and} \quad y = I_\ell \otimes S_m.$$

Note that $xy = yx$ and $x^\ell = y^m = I_{\ell m}$. A quasi-cyclic code is defined by a pair of matrices

$$A = A_1 + A_2 + A_3 \quad \text{and} \quad B = B_1 + B_2 + B_3 \tag{1}$$

where each matrix A_i and B_j is a power of x or y . Here and below the addition and multiplication of binary matrices is performed modulo two, unless stated otherwise. Thus, we also assume the A_i are distinct and the B_j are distinct to avoid cancellation of terms. For example, one could choose $A = x^3 + y + y^2$ and $B = y^3 + x + x^2$. Note that A and B have exactly three non-zero entries in each row and each column. Furthermore, $AB = BA$ since $xy = yx$. The above data defines a quasi-cyclic LDPC code denoted $\text{QC}(A, B)$ with length $n = 2\ell m$ and check matrices

$$H^X = [A|B] \quad \text{and} \quad H^Z = [B^T|A^T]. \tag{2}$$

Here the vertical bar indicates stacking matrices horizontally and T stands for the matrix transposition. Both matrices H^X and H^Z have size $(n/2) \times n$. Each row $v \in \mathbb{F}_2^n$ of H^X defines an X -type check operator $X(v) = \prod_{j=1}^n X_j^{v_j}$. Each

Notation	Name	Definition
$\text{rs}(H)$	row space	Linear span of rows of H
$\text{cs}(H)$	column space	Linear span of columns of H
$\text{ker}(H)$	nullspace	Vectors orthogonal to each row of H
$\text{rk}(H)$	rank	$\text{rk}(H) = \dim(\text{rs}(H)) = \dim(\text{cs}(H))$

Table 2: Notations for linear spaces associated with a binary matrix H . Here the linear span, orthogonality, and dimension are computed over the binary field $\mathbb{F}_2 = \{0, 1\}$. If H has size $s \times n$ then $\text{rs}(H) \subseteq \mathbb{F}_2^n$, $\text{cs}(H) \subseteq \mathbb{F}_2^s$, and $\text{ker}(H) \subseteq \mathbb{F}_2^n$.

$[[n, k, d]]$	Net Encoding Rate r	ℓ, m	A	B	
$[[72, 12, 6]]$	1/12	6, 6	$x^3 + y + y^2$	$y^3 + x + x^2$	
$[[90, 8, 10]]$	1/23	15, 3	$x^9 + y + y^2$	$1 + x^2 + x^7$	
$[[108, 8, 10]]$	1/27	9, 6	$x^3 + y + y^2$	$y^3 + x + x^2$	
$[[144, 12, 12]]$	1/24	12, 6	$x^3 + y + y^2$	$y^3 + x + x^2$	
$[[288, 12, 18]]$	1/48	12, 12	$x^3 + y^2 + y^7$	$y^3 + x + x^2$	
$[[360, 12, \leq 24]]$	1/60	30, 6	$x^9 + y + y^2$	$y^3 + x^{25} + x^{26}$	
$[[756, 16, \leq 34]]$	1/95	21, 18	$x^3 + y^{10} + y^{17}$	$y^5 + x^3 + x^{19}$	

Table 3: Small examples of quasi-cyclic LDPC codes and their parameters. All codes have weight-6 checks, thickness-2 Tanner graph, and a depth-7 syndrome measurement circuit. Code distance was computed by the mixed integer programming approach of Ref. [48]. Notation $\leq d$ indicates that only an upper bound on the code distance is known at the time of this writing. We round r down to the nearest inverse integer. The codes have check matrices $H^X = [A|B]$ and $H^Z = [B^T|A^T]$ with A and B defined in the last two columns. The matrices x, y obey $x^\ell = y^m = 1$ and $xy = yx$.

row $v \in \mathbb{F}_2^n$ of H^Z defines a Z -type check operator $Z(v) = \prod_{j=1}^n Z_j^{v_j}$. Any X -check and Z -check commute since they overlap on even number of qubits (note that $H^X(H^Z)^T = AB + BA = 0 \pmod{2}$). To describe the code parameters we use certain linear subspaces associated with the check matrices, see Table 1 for our notations. Then the code $\text{QC}(A, B)$ has parameters $[[n, k, d]]$ with

$$n = 2\ell m, \quad k = 2 \cdot \dim(\text{ker}(A) \cap \text{ker}(B)) \quad \text{and} \quad d = \min\{|v|: v \in \text{ker}(H^X) \setminus \text{rs}(H^Z)\}, \quad (3)$$

see Lemma 1. Here $|v| = \sum_{i=1}^n v_i$ is the Hamming weight of a vector $v \in \mathbb{F}_2^n$.

Table 3 describes the polynomials A and B that give rise to examples of high-rate, high-distance quasi-cyclic codes found by a numerical search. This includes all codes from Table 1 and two examples of higher distance codes. To the best of our knowledge, all these examples are new. The code $[[360, 12, \leq 24]]$ improves upon a code $[[882, 24, \leq 24]]$ with weight-6 checks found by Panteleev and Kalachev in [34] (assuming that our distance upper bound is tight). Indeed, taking two independent copies of the 360-qubit code gives parameters $[[720, 24, \leq 24]]$.

By construction, the code $\text{QC}(A, B)$ has weight-6 check operators and each qubit participates in six checks (three X -type plus three Z -type checks). Accordingly, the code $\text{QC}(A, B)$ has a degree-6 Tanner graph. Below we show that the Tanner graph has thickness $\theta \leq 2$, as desired, see Lemma 2.

We note that the recent work by Wang, Lin, and Pryadko [36, 35] described examples of group-based codes closely

related to the codes considered here. Some of the group-based codes with weight-8 checks found in [35] outperform our quasi-cyclic codes with weight-6 checks in terms of the parameters n, k, d . It remains to be seen whether group-based codes can achieve a similar or better level of error suppression for the circuit-based noise model.

In the rest of this section we establish some properties of quasi-cyclic LDPC codes.

Lemma 1. *The code $\text{QC}(A, B)$ has parameters $[[n, k, d]]$, where*

$$n = 2\ell m, \quad k = 2 \cdot \dim(\ker(A) \cap \ker(B)), \quad \text{and} \quad d = \min\{|v|: v \in \ker(H^X) \setminus \text{rs}(H^Z)\}.$$

The code offers equal distance for X -type and Z -type errors.

Proof. It is known [42, 43] that

$$k = n - \text{rk}(H^X) - \text{rk}(H^Z).$$

We claim that $\text{rk}(H^X) = \text{rk}(H^Z)$. Indeed, define a self-inverse permutation matrix C_ℓ of size $\ell \times \ell$ such that the i -th column of C_ℓ has a single nonzero entry equal to one at the row $j = -i \pmod{\ell}$. Define C_m similarly and let $C = C_\ell \otimes C_m$. Since $C_\ell S_\ell C_\ell = S_\ell^T$ and $C_m S_m C_m = S_m^T$, one gets

$$A^T = CAC \quad \text{and} \quad B^T = CBC. \quad (4)$$

Therefore one can write

$$H^Z = [B^T | A^T] = [CBC | CAC] = C[A | B] \begin{bmatrix} 0 & C \\ C & 0 \end{bmatrix} = CH^X \begin{bmatrix} 0 & C \\ C & 0 \end{bmatrix}.$$

Thus H^Z is obtained from H^X by multiplying on the left and on the right by invertible matrices. This implies $\text{rk}(H^X) = \text{rk}(H^Z)$. Therefore

$$\begin{aligned} k &= n - 2 \cdot \text{rk}(H^Z) = n - 2 \left(\frac{n}{2} - \dim(\ker((H^Z)^T)) \right) = n - 2 \left(\frac{n}{2} - \dim(\ker(A) \cap \ker(B)) \right) \\ &= 2 \cdot \dim(\ker(A) \cap \ker(B)). \end{aligned}$$

Here we noted that H^Z has size $(n/2) \times n$ and $\ker((H^Z)^T) = \ker(A) \cap \ker(B)$ since $H^Z = [B^T | A^T]$.

It is known [42, 43] that a CSS code with check matrices H^X and H^Z has distance $d = \min(d^X, d^Z)$, where d^X and d^Z are the code distances for X -type and Z -type errors defined as

$$d^X = \min\{|v|: v \in \ker(H^Z) \setminus \text{rs}(H^X)\} \quad \text{and} \quad d^Z = \min\{|v|: v \in \ker(H^X) \setminus \text{rs}(H^Z)\}.$$

We claim that $d^Z \leq d^X$. Indeed, let $X(f) = \prod_{j=1}^n X_j^{f_j}$ be a minimum weight logical X -type Pauli operator such that $|f| = d^X$. Then $H^Z f = 0$ and $f \notin \text{rs}(H^X)$. Thus there exists a logical Z -type operator $Z(g) = \prod_{j=1}^n Z_j^{g_j}$ anti-commuting with $X(f)$. In other words, $H^X g = 0$ and $f^T g = 1$. Here, f and g are length- n binary vectors. Write $f = (\alpha, \beta)$ and $g = (\gamma, \delta)$, where $\alpha, \beta, \gamma, \delta$ are length- $(n/2)$ vectors. Conditions $H^Z f = 0$ and $H^X g = 0$ are equivalent to

$$B^T \alpha = A^T \beta \quad \text{and} \quad A \gamma = B \delta. \quad (5)$$

Here and below all arithmetics is modulo two. Define length- n vectors

$$e = (C\delta, C\gamma) \quad \text{and} \quad h = (C\beta, C\alpha). \quad (6)$$

From Eqs. (4,5) one gets

$$H^X h = [A | B] \begin{bmatrix} C\beta \\ C\alpha \end{bmatrix} = AC\beta + BC\alpha = C(A^T \beta + B^T \alpha) = 0.$$

Likewise,

$$H^Z e = [B^T | A^T] \begin{bmatrix} C\delta \\ C\gamma \end{bmatrix} = B^T C\delta + A^T C\gamma = C(B\delta + A\gamma) = 0.$$

Furthermore,

$$h^T e = \beta^T C C \delta + \alpha^T C C \gamma = \beta^T \delta + \alpha^T \gamma = f^T g = 1.$$

Thus $X(e)$ and $Z(h)$ are non-identity logical operators. It follows that $d^Z \leq |h|$. We get

$$d^Z \leq |h| = |C\beta| + |C\alpha| = |\beta| + |\alpha| = |f| = d^X.$$

Thus $d^Z \leq d^X$. Similar argument shows that $d^X \leq d^Z$, that is, $d^X = d^Z$. \square

In the following, we partition the set of data qubits as $[n] = LR$, where L and R are the left and right blocks of $n/2 = \ell m$ data qubits. Then, data qubits L and R and checks X and Z may each be labeled by integers $\mathbb{Z}_{\ell m} = \{0, 1, \dots, \ell m - 1\}$ which are indices into the matrices A, B . Alternatively, qubits and checks can be labeled by monomials from $\mathcal{M} = \{1, y, \dots, y^{m-1}, x, xy, \dots, xy^{m-1}, \dots, x^{\ell-1}y^{m-1}\}$ in this order, so that $i \in \mathbb{Z}_{\ell m}$ labels the same qubit or check as $x^{a_i}y^{i-ma_i}$ for $a_i = \text{floor}(i/m)$. Using the monomial labeling, L data qubit $\alpha \in \mathcal{M}$ is part of X checks $A_i^T \alpha$ and Z checks $B_i \alpha$ for $i = 1, 2, 3$. Similarly, R data qubit $\beta \in \mathcal{M}$ is part of X checks $B_i^T \beta$ and Z checks $A_i \beta$. A unified notation assigns each qubit or check a label $q(T, \alpha)$ where $T \in \{L, R, X, Z\}$ denotes its type and $\alpha \in \mathcal{M}$ its monomial label¹.

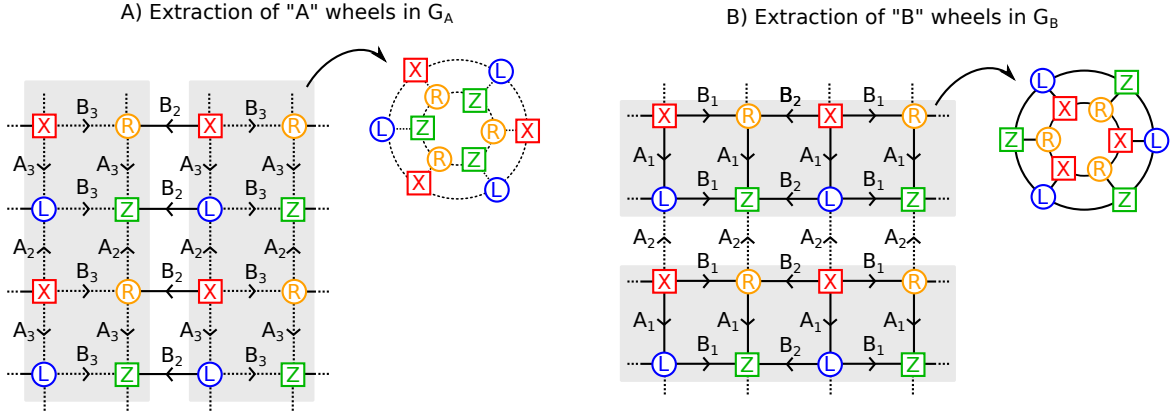


Figure 5: A). B) Two different grids over a torus defined using different subsets of $A_1, A_2, A_3, B_1, B_2, B_3$. Edge labels indicate adjacency matrices that generate the respective edges. By extracting either horizontal or vertical strips from these grids, we obtain planar ‘wheel graphs’ whose union contains all edges in the Tanner graph. The ‘A’ wheels (dashed lines) cover A_2, A_3, B_3 and the ‘B’ wheels (solid lines) cover B_1, B_2, A_1 . To avoid clutter, each grid shows only a subset of edges present in the Tanner graph.

Lemma 2. *The Tanner graph G of the code $QC(A, B)$ has thickness $\theta \leq 2$. A decomposition of G into two planar layers can be computed in time $O(n)$. Each planar layer of G is a degree-3 graph.*

¹The monomial notations should not be confused with the matrix notations used earlier in this section. For example, multiplication of monomials such as $B_i \alpha$ is different from multiplying a vector α by a matrix B_i .

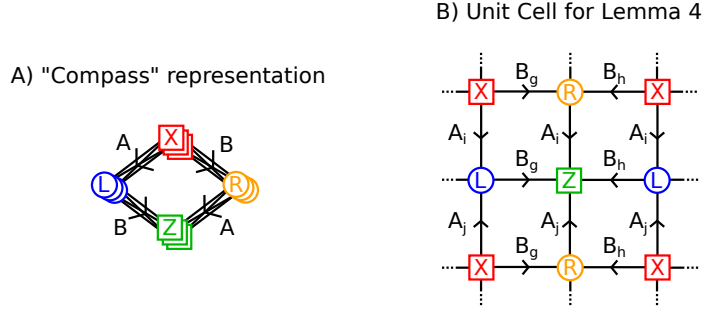


Figure 6: A) “Compass” diagram that shows the direction in which matrices A, B are applied to travel between different nodes. B) The unit cell of the construction of a toric layout in the proof of Lemma 4.

Proof. Let $G = (V, E)$ be the Tanner graph. Partition G into subgraphs $G_A = (V, E_A)$ and $G_B = (V, E_B)$ that describe CSS codes with check matrices

$$\text{Tanner graph } G_A: \quad H_A^X = [A_2 + A_3 | B_3] \quad \text{and} \quad H_A^Z = [B_3^T | A_2^T + A_3^T] \quad (7)$$

$$\text{Tanner graph } G_B: \quad H_B^X = [A_1 | B_1 + B_2] \quad \text{and} \quad H_B^Z = [B_1^T + B_2^T | A_1^T]. \quad (8)$$

Since $A = A_1 + A_2 + A_3$ and $B = B_1 + B_2 + B_3$, every edge of G appears either in G_A or G_B , where the two subgraphs are named by whether they contain more A_i edges or more B_i edges. Then G_A and G_B are regular degree-3 graphs (since A_i and B_j are permutation matrices).

Consider the graph G_A . Each X -check vertex is connected to a pair of data vertices $i_1, i_2 \in L$ via the matrices A_2, A_3 and a data vertex $i_3 \in R$ via the matrix B_3 . Each Z -check vertex is connected to a pair of data vertices $i_1, i_2 \in R$ via the matrices A_2^T, A_3^T and a data vertex $i_3 \in L$ via the matrix B_3^T .

We claim that each connected component of G_A can be represented by a “wheel graph” illustrated in Figure 5. A wheel graph consists of two disjoint cycles of the same length p interconnected by p radial edges. The outer cycle alternates between X -check and L -data vertices.

Edges of the outer cycle alternate between those generated by A_3 (as one moves from a check to a data vertex) and A_2^T (as one moves from a data to a check vertex). The length of the outer cycle is equal to the order of the matrix $A_3 A_2^T$, that is, the smallest integer p such that $(A_3 A_2^T)^p = I_{\ell_m}$. For example, consider the code $[[144, 12, 12]]$ from Table 3. Then $A = x^3 + y + y^2$, $A_2 = y$, and $A_3 = y^2$. Thus $A_3 A_2^T = y^2 y^{-1} = y$ which has order $m = 6$. The inner cycle of a wheel graph alternates between Z -check and R -data vertices.

Edges of the inner cycle alternate between those generated by A_3^T (as one moves from a check to a data vertex) and A_2 (as one moves from a data to a check vertex). The length of the inner cycle is equal to the order of the matrix $A_3^T A_2$ which is the just the transpose of $A_3 A_2^T$ considered earlier. Thus both inner and outer cycles have the same length m . The two cycles are interconnected by m radial edges as shown in Figure 5 A). Radial edges are generated by the matrix B_3 , as one moves towards the center of the wheel. The wheel graph contains 4-cycles generated by tuples of edges (B_3, A_2, B_3^T, A_2^T) and (B_3^T, A_3, B_3, A_3^T) . Commutativity between A_i and B_j ensures that traversing any of these 4-cycles implements the identity matrix, that is, the graph is well defined. Clearly, the wheel graph is planar. Since G_A is a disjoint union of wheel graphs, G_A is planar. The same argument shows that G_B is planar: see Figure 5 B). \square

We empirically observed that quasi-cyclic codes reported in Table 3 have no weight-4 stabilizers. The presence of such stabilizers is known to have a negative impact on the performance of belief propagation decoders [34], which we

use here.

The definition of code $\text{QC}(A, B)$ does not guarantee that its Tanner graph is connected. Some choices of A and B lead to a code that is actually several separable code blocks. This manifests as a Tanner graph with several connected components. For instance, although all codes in Table 3 are connected, taking any of them with even ℓ and replacing every instance of x with x^2 creates a code with two connected components.

Lemma 3. *The Tanner graph of the code $\text{QC}(A, B)$ is connected if and only if $S = \{A_i A_j^T : i, j \in \{1, 2, 3\}\} \cup \{B_i B_j^T : i, j \in \{1, 2, 3\}\}$ generates the group \mathcal{M} . The number of connected components in the Tanner graph is $\ell m / |\langle S \rangle|$, and all components are graph isomorphic to one another.*

Proof. Figure 6 is helpful for following the arguments in this proof. We start by proving the reverse implication of the first statement. Note that there is a length 2 path in the Tanner graph from L qubit $\alpha \in \mathcal{M}$ to L qubit $A_i A_j^T \alpha$ and another length 2 path to L qubit $B_i B_j^T \alpha$. These travel through X and Z checks, respectively. Thus, because the $A_i A_j^T$ and $B_i B_j^T$ generate \mathcal{M} , there is some path from α to any other L qubit β . A similar argument shows existence of a path connecting any pair of R qubits. Since each X check and each Z check are connected to at least one L qubit and at least one R qubit, this implies that the entire Tanner graph is connected. The forward implication of the first statement follows after noticing that, for all $T \in \{L, R, X, Z\}$, the path from a type T node to any other T node is necessarily described as a product of elements from S . Connectivity of the Tanner graph implies the existence of all such paths, and so S must generate \mathcal{M} .

If S does not generate \mathcal{M} , it necessarily generates a subgroup $\langle S \rangle$ and nodes in connected components of the Tanner graph are labeled by elements of the cosets of this subgroup. This implies the theorem's second statement. \square

For the next part, we establish some terminology. A spanning sub-graph of a graph G is a sub-graph containing all the vertices of G . Also, the undirected Cayley graph of a finite Abelian group \mathcal{G} (with identity element 0) generated by set $S \subset \mathcal{G}$ is the graph with vertex set \mathcal{G} and undirected edges $(g, g + s)$ for all $g \in \mathcal{G}$ and all $s \in S, s \neq 0$. We say the Cayley graph of $\mathbb{Z}_a \times \mathbb{Z}_b$ when we mean the Cayley graph of $\mathbb{Z}_a \times \mathbb{Z}_b$ generated by $\{(1, 0), (0, 1)\}$. The order $\text{ord}(g)$ of an element g in a multiplicative group is the smallest positive integer such that $g^{\text{ord}(g)} = 1$.

Definition 1. *Code $\text{QC}(A, B)$ is said to have a toric layout if its Tanner graph has a spanning sub-graph isomorphic to the Cayley graph of $\mathbb{Z}_{2\mu} \times \mathbb{Z}_{2\lambda}$ for some integers μ and λ .*

Note that only codes with connected Tanner graphs can have a toric layout according to this definition. An example toric layout is depicted in Figure 2.

Lemma 4. *A code $\text{QC}(A, B)$ has a toric layout if there exist $i, j, g, h \in \{1, 2, 3\}$ such that*

$$(i) \langle A_i A_j^T, B_g B_h^T \rangle = \mathcal{M} \text{ and}$$

$$(ii) \text{ord}(A_i A_j^T) \text{ord}(B_g B_h^T) = \ell m.$$

Proof. We let $\mu = \text{ord}(A_i A_j^T)$ and $\lambda = \text{ord}(B_g B_h^T)$. We associate qubits and checks in the Tanner graph of $\text{QC}(A, B)$ with elements of $\mathcal{G} = \mathbb{Z}_{2\mu} \times \mathbb{Z}_{2\lambda}$. For L qubit with label $\alpha \in \mathcal{M}$, because of (i), there is $(a, b) \in \mathbb{Z}_\mu \times \mathbb{Z}_\lambda$ such that $\alpha = (A_i A_j^T)^a (B_g B_h^T)^b$. Because of (ii) and the pigeonhole principle, this choice of (a, b) is unique. We associate L qubit α with $(2a, 2b) \in \mathcal{G}$. Similarly, an R qubit with label $\alpha A_j^T B_g$ is associated with $(2a + 1, 2b + 1) \in \mathcal{G}$, X -check αA_j^T with $(2a + 1, 2b)$, and Z -check αB_g with $(2a, 2b + 1)$. Edges in the Tanner graph A_i, A_j^T, B_g , and B_h^T can now be drawn as in Figure 6 (B) and correspond to edges in the Cayley graph of \mathcal{G} . For instance, to get from $(2a + 1, 2b + 1)$, an R qubit, to $(2a + 2, 2b + 1)$, a Z check, we apply A_i , taking R qubit labeled $\alpha A_j^T B_g$ to the Z check labeled $(\alpha A_j^T B_g) A_i = \alpha (A_i A_j^T) B_g$. \square

Notation	Operation
CNOT $c \ t$	CNOT with control qubit c and target qubit t
InitX q	Initialize qubit q in the state $ +\rangle = (0\rangle + 1\rangle)/\sqrt{2}$
InitZ q	Initialize qubit q in the state $ 0\rangle$
MeasX q	Measure qubit q in the X -basis $ +\rangle, -\rangle$
MeasZ q	Measure qubit q in the Z -basis $ 0\rangle, 1\rangle$
Idle q	Identity gate on qubit q

Table 4: Elementary operations used for syndrome measurements.

All codes in Table 3 have a toric layout with $\mu = m$ and $\lambda = \ell$. Indeed, they all satisfy Lemma 4 with $i = g = 2$ and $j = h = 3$.

However, we also note two interesting cases. First, there are codes with connected Tanner graphs that do not satisfy the conditions for a toric layout given in Lemma 4. One example of such a code is $\text{QC}(A, B)$ with $\ell, m = 28, 14$, $A = x^{26} + y^6 + y^8$, and $B = y^7 + x^9 + x^{20}$ which has parameters $[[784, 24, \leq 24]]$. Second, for a code satisfying the conditions of Lemma 4, it need not be the case that the set $\{\text{ord}(A_i A_j^T), \text{ord}(B_g B_h^T)\}$ and the set $\{\ell, m\}$ are equal. For example, the $[[432, 4, \leq 22]]$ code with $\ell, m = 18, 12$ and $A = x + y^{11} + y^3$, $B = y^2 + x^{15} + x$ only satisfies Lemma 4 with $\mu, \lambda = 36, 6$ (take $i = g = 1$ and $j = h = 2$ for instance).

5 Syndrome measurement circuit

The next step is to furnish the code $\text{QC}(A, B)$ with a syndrome measurement (SM) circuit that repeatedly measures the syndrome of each check operator. Here we describe a SM circuit that requires $2n$ physical qubits in total: n data qubits and n ancillary check qubits used to record the measured syndromes. The circuit only applies CNOTs to pairs of qubits that are connected in the Tanner graph.

The SM circuit is defined as a periodically repeated sequence of *syndrome cycles* (SC). A single SC is responsible for measuring syndromes of all n check operators of the code. Let N_c be the number of syndrome cycles. We envision that $N_c > 1$. The circuit begins and ends with a special initialization and measurement cycle responsible for initializing logical qubits in a suitable initial state and measuring logical qubits in a suitable basis. Here we focus on the optimization of the SC circuit. Logical initialization and measurements are discussed in Section 8.

The SC circuit is divided into N_r rounds such that each round is a depth-1 circuit composed of CNOTs and single-qubit operations. The latter include initializing a qubit in the X or Z basis and measuring a qubit in the X or Z basis. CNOTs can be applied only to pairs of qubits which are nearest neighbors in the Tanner graph. Some qubits remain idle during some rounds, although we try to minimize such occurrences by squeezing more useful computations in as little time as possible. Our notations are summarized in Table 4.

Below we describe a SC circuit with effectively $N_r = 8$ rounds². Ignoring single-qubit initialization and measurement operations, the SC circuit is a depth-7 CNOT circuit. By designing the circuit for an explicit family of LDPC codes we are able to leverage the symmetries and reduce computational depth to 7 from what otherwise would be $14 = 2 \cdot 6 + 2$, as shown by previous authors [29, Theorem 1]. Our notations are as follows. We divide n data qubits into the left and the right registers $q(L)$ and $q(R)$ of size $n/2$ each. Each check operator acts on three data qubits from $q(L)$ and three data qubits from $q(R)$. The SM circuit uses $2n$ physical qubits in total: n data qubits and n ancillary check qubits

²The operator $\text{InitZ } q(Z, i)$ must be executed before the first application of this SC circuit, raising the depth of the first stage to 9. However, each following syndrome cycle takes Z-check initialization from the previous round. Last syndrome cycle needs not apply the Z-check state initialization. Total SM circuit depth with N_c syndrome cycles is thus $8N_c + 1$.

Round	Circuit	Round	Circuit
1	for $i = 1$ to $n/2$ do InitX $q(X, i)$ CNOT $q(R, A_1^T(i))$ $q(Z, i)$ Idle $q(L, i)$ end for	5	for $i = 1$ to $n/2$ do CNOT $q(X, i)$ $q(R, B_3(i))$ CNOT $q(L, B_3^T(i))$ $q(Z, i)$ end for
2	for $i = 1$ to $n/2$ do CNOT $q(X, i)$ $q(L, A_2(i))$ CNOT $q(R, A_3^T(i))$ $q(Z, i)$ end for	6	for $i = 1$ to $n/2$ do CNOT $q(X, i)$ $q(L, A_1(i))$ CNOT $q(R, A_2^T(i))$ $q(Z, i)$ end for
3	for $i = 1$ to $n/2$ do CNOT $q(X, i)$ $q(R, B_2(i))$ CNOT $q(L, B_1^T(i))$ $q(Z, i)$ end for	7	for $i = 1$ to $n/2$ do CNOT $q(X, i)$ $q(L, A_3(i))$ MeasZ $q(Z, i)$ Idle $q(R, i)$ end for
4	for $i = 1$ to $n/2$ do CNOT $q(X, i)$ $q(R, B_1(i))$ CNOT $q(L, B_2^T(i))$ $q(Z, i)$ end for	8	for $i = 1$ to $n/2$ do MeasX $q(X, i)$ InitZ $q(Z, i)$ Idle $q(L, i)$ Idle $q(R, i)$ end for

Table 5: Depth-8 syndrome measurement cycle circuit.

that record the syndrome of each check operator. Let $q(X)$ and $q(Z)$ be the ancillary registers of size $n/2$ that span X -check and Z -check qubits respectively. Thus the physical qubits are partitioned into four registers, $q(X)$, $q(L)$, $q(R)$, and $q(Z)$, of size $n/2$ each. Label qubits in each register by integers $i = 1, 2, \dots, n/2$. We write $q(X, i)$ for the i -th qubit of the register $q(X)$ with similar notations for $q(L)$, $q(R)$, and $q(Z)$. Each permutation matrix A_p and B_q from Eq. (1) defines a one-to-one map from the set $\{1, 2, \dots, n/2\}$ onto itself. We identify a permutation matrix and the corresponding one-to-one map. For example, we write $j = A_1(i)$ if the matrix A_1 has a one at row i and column j (this is well defined since A_1 is a permutation matrix). Likewise, we write $j = A_1^T(i)$ if the transposed matrix A_1^T has a one at the row i and column j . In this notation, the i -th X -check operator acts on data qubits $q(L, A_p(i))$ and $q(R, B_p(i))$ with $p = 1, 2, 3$. The i -th Z -check operator acts on data qubits $q(L, B_p^T(i))$ and $q(R, A_p^T(i))$ with $p = 1, 2, 3$.

Our depth-8 SC circuit is described in Table 5 and illustrated in Figure 7. Note that within each round all operations act over non-overlapping sets of qubits. In particular, each round applies at most one layer of CNOT gates between $q(X)$ and $q(L)$ registers (Rounds 2, 6, and 7), at most one layer of CNOTs between $q(X)$ and $q(R)$ registers (Rounds 3, 4, and 5), at most one layer of CNOTs between $q(Z)$ and $q(L)$ registers (Rounds 3, 4, and 5), and at most one layer of CNOTs between $q(Z)$ and $q(R)$ registers (Rounds 1, 2, and 6). Qubits from $q(Z)$ are always targets for CNOTs. Accordingly, X -type errors propagate from data qubits to check qubits in $q(Z)$. The latter are measured in the Z -basis in Round 7 revealing the syndrome of X -type errors. Qubits from $q(X)$ are always controls for CNOTs.

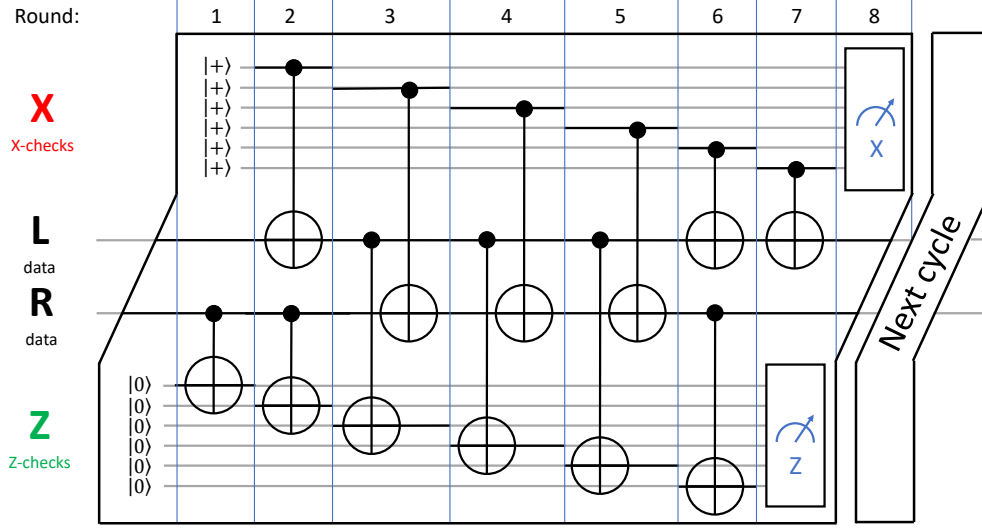


Figure 7: Depth-8 syndrome measurement cycle circuit.

Accordingly, Z -type errors propagate from data qubits to check qubits in $q(X)$. The latter are measured in the X -basis in Round 8 revealing the syndrome of Z -type errors. We envision that the syndrome cycles are repeated periodically. This justifies applying CNOTs to $q(Z)$ at Round 1 even though $q(Z)$ is initialized only at Round 8. Indeed, Round 8 of the previous syndrome cycle goes immediately before Round 1 of the current cycle. Thus $q(Z)$ has been already initialized at the beginning of Round 1. We were not able to find a depth-8 (or smaller depth) syndrome cycle in which X -check and Z -check qubits are initialized and measured synchronously.

Let us now prove that the above SC circuit has the desired functionality. Since the circuit involves only Clifford operations, its action can be compactly described using stabilizer tableau [49]. We track how the tableau changes as each layer of CNOTs in the circuit is applied. Since the CNOT gates do not mix Pauli X and Z operators, one may consider tableau describing the action of the circuit on X -type and Z -type Pauli operators separately.

Let us begin with X -type Pauli. The corresponding tableau T is a binary matrix of size $n \times 2n$ such that each row of T defines an X -type stabilizer of the underlying quantum state. We partition columns of T into four blocks that represent qubit registers $q(X)$, $q(L)$, $q(R)$, and $q(Z)$. We partition rows of T into two blocks such that initially the top $n/2$ rows represent weight-1 check operators on qubits of the register $q(X)$ initialized in the state $|+\rangle$ while the bottom $n/2$ rows represent weight-6 check operators on data qubits associated with the chosen code $\text{QC}(A, B)$. Thus, at the beginning of Round 1, when all check qubits in the register $q(X)$ have been initialized in the state $|+\rangle$, while data qubits are in some logical state of the code $\text{QC}(A, B)$, the binary matrix is

$$\begin{pmatrix} I & 0 & 0 & 0 \\ 0 & A & B & 0 \end{pmatrix}.$$

Here $I \equiv I_{n/2}$ is the identity matrix. The SC circuit (ignoring qubit initialization and measurements) enacts the transformation

$$\begin{pmatrix} I & 0 & 0 & 0 \\ 0 & A & B & 0 \end{pmatrix} \xrightarrow{\text{SC circuit}} \begin{pmatrix} I & A & B & 0 \\ 0 & A & B & 0 \end{pmatrix}.$$

Indeed, the circuit must map a single-qubit X stabilizer X_j on a check qubit $j \in q(X)$ to a product of X_j and the j -th X -type check operator on the data qubits determined by the j -th row of $H^X = [A|B]$. The eigenvalue measurement of X_j at the final round then reveals the syndrome of the j -th check operator. The bottom $n/2$ rows must be unchanged since the check operators of the code must be the same before and after the syndrome measurement.

Let us verify that the circuit defined in Table 5 enacts the desired transformation. To accomplish this, we rewrite the SC circuit by removing notations irrelevant to showing the correctness of X -checks. Specifically, we write each CNOT in Table 5 as $\text{CNOT}_M(a, b)$, where $a, b \in \{1, 2, 3, 4\} = \{q(X), q(L), q(R), q(Z)\}$, and $M \in \{A_1, A_2, A_3, B_1, B_2, B_3\}$. Note that the CNOT instructions where the matrix M^T is used instead of M can be written using matrix M by performing the variable renaming $i \leftarrow M(i)$ in the corresponding for loop in Table 5.

Using the above compact notation, the unitary part of the SC circuit becomes:

$$\begin{aligned}
&\text{Round 1:} && \text{CNOT}_{A_1}(3, 4) \\
&\text{Round 2:} && \text{CNOT}_{A_2}(1, 2), \text{CNOT}_{A_3}(3, 4) \\
&\text{Round 3:} && \text{CNOT}_{B_2}(1, 3), \text{CNOT}_{B_1}(2, 4) \\
&\text{Round 4:} && \text{CNOT}_{B_1}(1, 3), \text{CNOT}_{B_2}(2, 4) \\
&\text{Round 5:} && \text{CNOT}_{B_3}(1, 3), \text{CNOT}_{B_3}(2, 4) \\
&\text{Round 6:} && \text{CNOT}_{A_1}(1, 2), \text{CNOT}_{A_2}(3, 4) \\
&\text{Round 7:} && \text{CNOT}_{A_3}(1, 2)
\end{aligned} \tag{9}$$

In the following we apply all seven unitary rounds to verify the correctness of the performed transformation:

$$\begin{aligned}
&\text{Round 1: } \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & A & B & 0 \end{pmatrix} \xrightarrow{\text{CNOT}_{A_1}(3,4)} \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & A & B & A_1B \end{pmatrix} \\
&\text{Round 2: } \xrightarrow{\text{CNOT}_{A_2}(1,2)} \begin{pmatrix} I & A_2 & 0 & 0 \\ 0 & A & B & A_1B \end{pmatrix} \xrightarrow{\text{CNOT}_{A_3}(3,4)} \begin{pmatrix} I & A_2 & 0 & 0 \\ 0 & A & B & (A_1+A_3)B \end{pmatrix} \\
&\text{Round 3: } \xrightarrow{\text{CNOT}_{B_2}(1,3)} \begin{pmatrix} I & A_2 & B_2 & 0 \\ 0 & A & B & (A_1+A_3)B \end{pmatrix} \xrightarrow{\text{CNOT}_{B_1}(2,4)} \begin{pmatrix} I & A_2 & B_2 & A_2B_1 \\ 0 & A & B & (A_1+A_3)B + AB_1 \end{pmatrix} \\
&\text{Round 4: } \xrightarrow{\text{CNOT}_{B_1}(1,3)} \begin{pmatrix} I & A_2 & B_1+B_2 & A_2B_1 \\ 0 & A & B & (A_1+A_3)B + AB_1 \end{pmatrix} \\
&\xrightarrow{\text{CNOT}_{B_2}(2,4)} \begin{pmatrix} I & A_2 & B_1+B_2 & A_2(B_1+B_2) \\ 0 & A & B & (A_1+A_3)B + A(B_1+B_2) \end{pmatrix} = \begin{pmatrix} I & A_2 & B_1+B_2 & A_2(B_1+B_2) \\ 0 & A & B & A_2B + AB_3 \end{pmatrix}
\end{aligned}$$

Here, we use the identity $(A_1+A_3)B + A(B_1+B_2) = A_2B + AB_3$, which holds since the sum of first summands and second summands on both sides of the equation gives AB , and $AB + AB = 0$.

$$\begin{aligned}
&\text{Round 5: } \xrightarrow{\text{CNOT}_{B_3}(1,3)} \begin{pmatrix} I & A_2 & B & A_2(B_1+B_2) \\ 0 & A & B & A_2B + AB_3 \end{pmatrix} \xrightarrow{\text{CNOT}_{B_3}(2,4)} \begin{pmatrix} I & A_2 & B & A_2B \\ 0 & A & B & A_2B \end{pmatrix} \\
&\text{Round 6: } \xrightarrow{\text{CNOT}_{A_1}(1,2)} \begin{pmatrix} I & A_1+A_2 & B & A_2B \\ 0 & A & B & A_2B \end{pmatrix} \xrightarrow{\text{CNOT}_{A_2}(3,4)} \begin{pmatrix} I & A_1+A_2 & B & 0 \\ 0 & A & B & 0 \end{pmatrix} \\
&\text{Round 7: } \xrightarrow{\text{CNOT}_{A_3}(1,2)} \begin{pmatrix} I & A & B & 0 \\ 0 & A & B & 0 \end{pmatrix}.
\end{aligned}$$

This is the desired transformation.

So far, we have not considered the action of the SC circuit on the logical qubits of the code. Let us show that this action is trivial. Indeed, consider some X -type logical operator $X(v)$, where $v \in \mathbb{F}_2^n$. Write $v = (u, w)$ where u and w are restrictions of v onto the registers 2 and 3 respectively. Commutativity between $X(v)$ and any Z -type check operator implies

$$uB + wA = 0.$$

Here we consider u and w as row vectors. Extending v by zeroes on registers 1 and 4 gives the row vector $(0 \ u \ w \ 0)$, where 0 stands for the all-zero row vector of length $n/2$. Let us follow the same chain of transformations as above starting from the initial vector $(0 \ u \ w \ 0)$. All CNOT s controlled by the register 1, such as $\text{CNOT}_{A_2}(1, 2)$ or $\text{CNOT}_{B_2}(1, 3)$ in Eq. (9), have trivial action on the vector $(0 \ u \ w \ 0)$ since all qubits of the control register are zeroes. Such CNOT s can be omitted. The remaining CNOT s in Eq. (9) such as $\text{CNOT}_{A_1}(3, 4)$ or $\text{CNOT}_{B_1}(2, 4)$ map the initial vector $(0 \ u \ w \ 0)$ to $(0 \ u \ w \ t)$ for some vector t since the registers 2 and 3 always serve as the controls and the register 4 always serves as the target. Rounds 1, 2, and 6 in Eq. (9) are equivalent to XORing vectors wA_1 , wA_3 , and wA_2 respectively to the register 4. Rounds 3, 4, and 5 in Eq. (9) are equivalent to XORing vectors uB_1 , uB_2 , and uB_3 respectively to the register 4. Thus

$$t = w(A_1 + A_2 + A_3) + u(B_1 + B_2 + B_3) = wA + uB = 0.$$

We have shown that the SC circuit maps the vector $(0 \ u \ w \ 0)$ to itself. Hence the circuit acts trivially on logical X -type operators.

To prove the correctness of Z -checks, observe that Z -checks can be mapped into X -checks by conjugation with Hadamards. When the unitary circuit in Figure 7 is conjugated with Hadamards, this flips controls and targets of all CNOT gates. Thus, to verify Z -checks, it suffices to perform a very similar calculation to the one already shown for X -checks. We omit this calculation here.

The SC circuit shown in Table 5 is not unique in the following sense: we found 935 depth-7 alternatives to the unitary part of the SC circuit via a computer search. These alternatives are obtained from the circuit defined in Eq. (9) by applying the gate layers CNOT_{A_i} and CNOT_{B_j} in a different order. In the special case of the $[[144, 12, 12]]$ code, numerical simulations show that all 936 variants of the syndrome cycle give rise to syndrome measurement circuits with distance $d_{\text{circ}} \leq 10$ explaining our focus on a specific circuit Eq. (9) which we conjecture to have distance $d_{\text{circ}} = 10$. The short depth of the single cycle, relying on only seven computational stages, helps to keep the spread of errors under control. Details of calculating upper bounds on the circuit-level distance are provided in Section 6.

6 Decoder for the circuit-based noise model

So far we assumed that the SM circuit is noiseless. As shown in Section 5, in this case all measured syndromes are zero and the circuit implements the logical identity gate. Consider now what happens when each operation in the circuit including CNOT gates, qubit initializations, measurements, and idle qubits is subject to noise. To enable efficient decoding and numerical simulations, we use the standard circuit-based depolarizing noise model [22]. It assumes that each operation in the circuit is ideal or faulty with the probability $1 - p$ or p respectively. Here p is a model parameter called the error rate. Faults on different operations occur independently. We define faulty operations as follows. A faulty CNOT is an ideal CNOT followed by one of 15 non-identity Pauli errors on the control and the target qubits picked uniformly at random. A faulty initialization prepares a single-qubit state orthogonal to the correct one. A faulty measurement is an ideal measurement followed by a classical bit-flip error applied to the measurement outcome. A faulty idle qubit suffers from a Pauli error X or Y or Z picked uniformly at random.

To perform error correction one needs a decoder — a classical algorithm that takes as input the measured error syndrome and outputs a guess of the final Pauli error on the data qubits resulting from all faults in the SM circuit. The error syndrome may itself be faulty due to measurement errors. The decoder succeeds if the guessed Pauli error

coincides with the actual error up to a product of check operators. In this case the guessed and the actual error have the same action on any logical state.

Let us show how to adapt Belief Propagation with an Ordered Statistics postprocessing step Decoder (BP-OSD) proposed in [34, 44] to the circuit-based noise model. The decoder consists of two stages. The first stage takes as input a quasi-cyclic code $QC(A, B)$ equipped with a SM circuit \mathcal{U} and an error rate p . It outputs a certain linearized noise model that ignores possible cancellations between errors generated by two or more faulty operations in \mathcal{U} . This stage is analogous to computing the decoding graph in error correction algorithms based on the surface code [50, 51]. The second (online) stage of the decoder takes as input an error syndrome measured in the experiment and outputs a guess of the final error on the data qubits. This stage decodes the linearized noise model using BP-OSD method [34, 44].

We begin by describing the offline stage. Consider a quasi-cyclic code with parameters $[[n, k, d]]$ and let \mathcal{U} be the SM circuit constructed in Section 5 with N_c syndrome cycles. The circuit \mathcal{U} contains $6nN_c$ CNOTs, nN_c initializations and measurements, and $2nN_c$ idle qubit locations. Let $\mathcal{U}_1, \mathcal{U}_2, \dots, \mathcal{U}_M$ be the list of all possible faulty realizations of \mathcal{U} with exactly one faulty operation. If the faulty operation happens to be CNOT or an idle qubit, one of the admissible Pauli errors for this operation is specified. A simple counting shows that $M = 98nN_c$, where $98 = 15 \cdot 6 + 1 + 1 + 3 \cdot 2$ accounts for 15 noisy realizations of each CNOT, 3 realizations of memory errors on idle qubits, noisy initializations and measurements. By definition, the list $\mathcal{U}_1, \mathcal{U}_2, \dots, \mathcal{U}_M$ includes all realizations of \mathcal{U} that can occur with the probability $O(p)$ in the limit $p \rightarrow 0$. We simulate each circuit \mathcal{U}_j by propagating the chosen Pauli error towards the final time step taking into account qubit initialization and measurement errors (if any). This simulation can be performed efficiently using the stabilizer formalism. Let $s_j^U \in \{0, 1\}^{nN_c}$ be the full measured syndrome of \mathcal{U}_j and E_j be the final n -qubit Pauli error on the data qubits generated by \mathcal{U}_j . Let $s_j^F \in \{0, 1\}^n$ be the syndrome of the final error E_j . In other words, if we write $E_j = X(\alpha_j)Z(\beta_j)$ for some vectors $\alpha_j, \beta_j \in \{0, 1\}^n$, then

$$s_j^F = \begin{bmatrix} H^Z \alpha_j \\ H^X \beta_j \end{bmatrix}.$$

Here H^X and H^Z are the check matrices of the chosen code. Finally, let $s_j^L \in \{0, 1\}^{2k}$ be a *logical syndrome* of the final error E_j defined as follows. Fix some basis set of logical Pauli operators $\bar{P}_1, \bar{P}_2, \dots, \bar{P}_{2k}$ for the chosen code. For example, $\bar{P}_1, \bar{P}_2, \dots, \bar{P}_k$ could be logical X -type operators and $\bar{P}_{k+1}, \bar{P}_{k+2}, \dots, \bar{P}_{2k}$ could be logical Z -type operators. The i -th bit of s_j^L is defined as

$$(s_j^L)_i = \begin{cases} 1 & \text{if } E_j \bar{P}_i = -\bar{P}_i E_j, \\ 0 & \text{if } E_j \bar{P}_i = \bar{P}_i E_j, \end{cases}$$

for $i = 1, \dots, 2k$. Note that the pair of syndromes s_j^F, s_j^L uniquely determines the final error E_j modulo check operators. Define a pair of *decoding matrices* D and D^L of size $(nN_c + n) \times M$ and $2k \times M$ respectively such that the j -th column of D is

$$\begin{bmatrix} s_j^U \\ s_j^F \end{bmatrix}$$

and the j -th column of D^L is s_j^L . Let p_j be the probability of a Pauli error that occurred in the circuit \mathcal{U}_j . We have $p_j = p/15$ if \mathcal{U}_j contains a faulty CNOT, $p_j = p/3$ if \mathcal{U}_j contains a faulty idle qubit, and $p_j = p$ if \mathcal{U}_j contains a faulty qubit initialization or measurement. Suppose $I \subseteq \{1, 2, \dots, M\}$ is a subset of columns of D such that triples of syndromes (s_j^U, s_j^F, s_j^L) are the same for all $j \in I$. We merge all columns in I to a single column and assign the value $\sum_{j \in I} p_j$ to the bit-flip error probability associated with the merged column. Let M be the number of columns of D after the merging step and p_1, p_2, \dots, p_M be the respective error probabilities.

Next, the decoding matrix D is converted to a sparse form. To this end consider a faulty circuit \mathcal{U}_j and a sequence of syndromes measured by \mathcal{U}_j on some check operator. Let this sequence be $m = (m_1, m_2, \dots, m_{N_c}) \in \{0, 1\}^{N_c}$. Since \mathcal{U}_j contains a single fault, the sequence m has only a few locations where the measured syndromes differ at two consecutive cycles. For example, if \mathcal{U}_j contains a Pauli error on some idle data qubit between two syndrome cycles,

the m -sequence may look as $(0, 0, \dots, 0, 1, 1, \dots, 1)$. Such sequence can be made sparse if we represent it by a binary vector

$$m' = (m_1, m_2 \oplus m_1, m_3 \oplus m_2, \dots, m_{N_c} \oplus m_{N_c-1}) \in \{0, 1\}^{N_c}.$$

In other words, m' stores changes in the measured syndrome at a given check operators at each cycle. We convert the matrix D to a sparse form by applying the map $m \rightarrow m'$ to the syndromes measured by each check operator for each faulty circuit \mathcal{U}_j .

Let $\xi_1, \xi_2, \dots, \xi_M \in \{0, 1\}$ be independent random variables such that ξ_j takes values 0 and 1 with the probability $1 - p_j$ and p_j respectively. Define a linearized noise model that outputs a random triple (s^U, s^F, E) , where

$$E = \prod_{j=1}^M (E_j)^{\xi_j}$$

is an n -qubit Pauli error and

$$\begin{bmatrix} s^U \\ s^F \end{bmatrix} = \sum_{j=1}^M \xi_j \begin{bmatrix} s_j^U \\ s_j^F \end{bmatrix} \pmod{2}$$

is a binary vector that represents the error syndrome. The linearized model is a simplified version of the circuit-based noise that ignores possible cancellations among errors generated by two or more faulty operations in \mathcal{U} . Note that such errors occur with the probability only $O(p^2)$. The decoder attempts to guess the final error E acting on the data qubits based on the syndrome s^U measured in the experiment making a simplifying assumption that that the pair (s^U, E) was generated using the linearized noise model. We additionally assume that the decoder knows the syndrome s^F of the final error E . This syndrome can be acquired by adding one noiseless cycle at the end of the syndrome measurement circuit, which is a common practice in numerical simulations of error correction. By definition, we have

$$D\xi = \begin{bmatrix} s^U \\ s^F \end{bmatrix}.$$

Here $\xi = (\xi_1, \xi_2, \dots, \xi_M)$ is a column vector and matrix-vector multiplication is modulo two. Define a minimum weight error $\xi^* = \xi^*(s) \in \{0, 1\}^M$ as a solution of an optimization problem

$$\xi^* = \arg \min_{\xi \in \{0, 1\}^M} \sum_{j=1}^M \log(1/p_j) \xi_j \quad \text{subject to} \quad D\xi = \begin{bmatrix} s^U \\ s^F \end{bmatrix}. \quad (10)$$

This problem is equivalent to the minimum weight decoding for a length- M linear code with the check matrix D , bit-flip error probabilities p_1, p_2, \dots, p_M , and noiseless syndromes. Our guess of the unknown logical syndrome is

$$s^L = D^L \xi^*.$$

Let E^* be any n -qubit Pauli operator with the syndrome s^F and the logical syndrome s^L . Note that E^* is defined uniquely modulo multiplication by check operators. The Pauli E^* is our guess of the final error on the data qubits. Let E be the actual final error on the data qubits generated by a noisy realization of \mathcal{U} without making any simplifications of the noise model. By definition, Pauli operators E and E^* have the same syndrome but they may differ by a logical Pauli operator. We declare a logical error if E and E^* differ by any non-identity logical operator (there are $4^k - 1$ choices of this logical operator). Otherwise the decoding is deemed successful.

It remains to explain how to solve the optimization problem Eq. (10). Since the minimum weight decoding for a linear code is known to be NP-hard problem [52], finding the exact solution of Eq. (10) might be practically impossible for problem instances with several thousand variables that we have to deal with. Furthermore, estimation of the

logical error probability p_L by the Monte Carlo method requires solving $O(1/p_L)$ instances of the problem Eq. (10). This number can be quite large since p_L is a small parameter. To address these challenges, we employ the BP-OSD algorithm [34, 44]. Recall that belief propagation (BP) is a heuristic message passing algorithm aimed at computing single-bit marginals of a probability distribution

$$P(\xi|\sigma) = \begin{cases} \frac{1}{\mathcal{Z}} \prod_{j=1}^M (1-p_j)^{1-\xi_j} p_j^{\xi_j} & \text{if } D\xi = \sigma, \\ 0 & \text{otherwise.} \end{cases}$$

Here $\xi \in \{0,1\}^M$ and \mathcal{Z} is a normalization factor chosen such that $\sum_{\xi \in \{0,1\}^M} P(\xi|\sigma) = 1$. In our case ξ represents an unknown error in the linearized noise model, D is the decoding matrix constructed above, and $\sigma = \begin{bmatrix} s^U \\ s^F \end{bmatrix}$ is the measured error syndrome. Let $q_j \in [0,1]$ be an estimate of the marginal probability $\Pr[\xi_j = 1]$ obtained by the belief propagation method with some fixed number of message passing iterations. The ordered statistics post-processing step examines *information sets* which are subsets of bits $I \subseteq [M]$ such that the linear system $D\xi = \sigma$ has a unique solution ξ supported on I , that is, $\xi_j = 0$ for all $j \notin I$. Information sets are ranked according to their *reliability* which is defined as

$$\rho(I) = \prod_{j \in I} \max(q_j, 1 - q_j).$$

BP-OSD finds an information set I with the largest reliability using a greedy algorithm [34]. The final output of BP-OSD is a solution of the system $D\xi = \sigma$ supported on the most reliable information set I . We replace the minimum weight error ξ^* in Eq. (10) by the solution ξ proposed by BP-OSD.

Since quasi-cyclic LDPC codes are of CSS-type, it is natural to decode X -type and Z -type errors independently. Accordingly, we solve the minimum weight decoding problem Eq. (10) twice with a pair of decoding matrices D_X and D_Z constructed as above but including only the syndromes of X -type and Z -type check operators respectively. This results in guessed X -type and Z -type errors E_X^* and E_Z^* . The guessed final error is $E^* = E_X^* E_Z^*$. We empirically observed that the resulting decoding matrices D_X and D_Z are $(6, 35)$ -sparse for any quasi-cyclic code, meaning that there are at most 6 nonzeros in each column and at most 35 nonzeros in each row of D_X and D_Z . The number of columns scales as $O(nN_c)$ where the constant coefficient depends on a particular code. For example, decoding matrices D_X and D_Z describing the code $[[144, 12, 12]]$ with $N_c = 12$ syndrome cycles have 8857 and 8785 columns respectively.

We also employed BP-OSD to compute an upper bound on the code distance d . Consider a CSS-type LDPC code $[[n, k, d]]$ with check matrices H^X and H^Z . Assume for simplicity that this code has the same distance for X - and Z -type errors (this assumption is satisfied for quasi-cyclic LDPC codes due to Lemma 1). Suppose $Z(\xi)$ is a minimum weight logical Z -type operator. Then $\xi \in \ker(H^X)$ and $\xi \notin \text{rs}(H^Z)$. Let $X(\eta)$ be any logical X -type operator. Here $\eta \in \ker(H^Z) \setminus \text{rs}(H^X)$. Consider the following optimization problem:

$$d(\eta) = \min_{\xi \in \ker(H^X)} \sum_{j=1}^n \xi_j \quad \text{subject to} \quad \eta^T \xi = 1. \quad (11)$$

Then $d(\eta) \geq d$ for any logical operator $X(\eta)$ and $d(\eta) = d$ if $X(\eta)$ anti-commutes with some minimum-weight logical operator $Z(\xi)$. The latter event occurs with the probability $1/2$ if one picks $\eta \in \ker(H^Z)$ uniformly at random. In this case $d(\eta) = d$ with the probability at least $1/2$ and $d(\eta) \geq d$ with certainty. Let $d^{\text{BP}}(\eta)$ be an upper bound on $d(\eta)$ obtained by solving the optimization problem Eq. (11) using BP-OSD method with a parity check matrix $\begin{bmatrix} H^X \\ \eta^T \end{bmatrix}$ and a syndrome $(0, 0, \dots, 0, 1)^T$. We have $d^{\text{BP}}(\eta) \geq d$ with certainty and $d^{\text{BP}}(\eta) = d$ with the probability $1/2$ whenever BP-OSD finds the optimal solution. Choose the number trials $T \gg 1$ and pick vectors $\eta^1, \eta^2, \dots, \eta^T \in \ker(H^Z) \setminus \text{rs}(H^X)$ uniformly at random. Then

$$d^{\text{BP}} := \min_{a=1,2,\dots,T} d^{\text{BP}}(\eta^a)$$

is an upper bound on the distance d that can be systematically improved by increasing the number of trials T .

Using the quantity d^{BP} as an efficiently computable proxy for the code distance enabled us to search over a large number of candidate quasi-cyclic codes with $n = O(100)$ qubits. The vast majority of these candidates was discarded due to an insufficiently large upper bound d^{BP} . This left only a few viable candidates with a sufficiently large value of d^{BP} . The actual distance of each candidate code was computed using the integer linear programming method [48].

We similarly computed an upper bound on the circuit-level distance d_{circ} . Since the SM circuit can break the symmetry between X - and Z -type errors, the circuit-level distance has to be computed for both types of errors. For concreteness, let us discuss the circuit-level distance d_{circ}^Z for Z -type errors. The latter is defined as the minimum number of faulty operations in the SM circuit that can generate an undetectable Z -type logical error. The optimization problem Eq. (11) is replaced by

$$d_{\text{circ}}^Z(\eta) = \min_{\xi \in \ker(D_X)} \sum_{j=1}^M \xi_j \quad \text{subject to} \quad \eta^T \xi = 1, \quad (12)$$

where D_X is the decoding matrix constructed above and $\eta \in \{0, 1\}^M$ is a random linear combination of rows of D_X and rows of D_L that represent logical X -type operators. Then $d_{\text{circ}}(\eta) \geq d_{\text{circ}}^Z$ with certainty and $d_{\text{circ}}(\eta) = d_{\text{circ}}^Z$ with the probability at least $1/2$. Solving the optimization problem Eq. (12) using BP-OSD method for many random choices of the vector η and taking the minimum value of $d_{\text{circ}}^Z(\eta)$ provides an upper bound on d_{circ}^Z . One can similarly compute an upper bound on the circuit-level distance d_{circ}^X for X -type errors. This provides an upper bound on $d_{\text{circ}} = \min(d_{\text{circ}}^X, d_{\text{circ}}^Z)$.

7 Numerical simulation details

Data reported in Figure 3 was generated using BP-OSD software developed by Roffe et al. [44, 53]. The decoder was extended to the circuit-based noise model as described in Section 6. The simulations were performed using MIN-SUM belief propagation with the limit of 10,000 iterations and combination sweep version of OSD, as described in [44]. All data points except for those with the smallest error rate accumulated at least 100 logical errors to estimate the logical error rate p_L with the error bars $\approx p_L/10$. The fitting formula $p_L(p) = p^{d_{\text{circ}}/2} e^{c_0 + c_1 p + c_2 p^2}$ with fitting parameters c_0, c_1, c_2 was proposed in [54] in the context of surface code simulations. We observed that the same fitting formula works well for quasi-cyclic LDPC codes. The fitting parameters c_i of the considered codes are provided in Table 6.

Surface code data reported in Figure 4 was generated using software developed by one of the authors and Alexander Vargo in [54]. The simulation was performed for the rotated surface code with parameters $[[d^2, 1, d]]$, where $d \in \{11, 13, 15\}$, and the standard SM circuit [22]. Let $P_{L,1}$ be the logical error probability for the surface code encoding one logical qubit and SM circuit with $N_c = d$ syndrome cycles. Encoding $k = 12$ logical qubits into 12 separate patches of the surface code results in a logical error probability

$$P_{L,12} = 1 - (1 - P_{L,1})^{12}.$$

Figure 4 shows the logical error rate p_L defined as the logical error probability per syndrome cycle,

$$p_L = 1 - (1 - P_{L,12})^{1/N_c} = 1 - (1 - P_{L,1})^{12/d}.$$

8 Logical memory capabilities

In this section we give evidence that quasi-cyclic LDPC codes have the required features for an effective quantum memory or storage unit. Although there are few ways of performing computations on stored qubits, there are fault

$[[n, k, d]]$	c_0	c_1	c_2
$[[72, 12, 6]]$	10.00	431.9	-19970
$[[90, 8, 10]]$	13.86	497.5	-12430
$[[108, 8, 10]]$	13.19	478	98.33
$[[144, 12, 12]]$	16.46	1076	-54422
$[[288, 12, 18]]$	35.46	734.6	-8038

Table 6: Parameters c_0, c_1, c_2 in the fitting formula $p_L(p) = p^{d/2} e^{c_0 + c_1 p + c_2 p^2}$ for quasi-cyclic LDPC codes shown in Table 1.

tolerant operations for initialization and measurement of individual qubits, and most importantly transfer of data into and out of the code via quantum teleportation. These capabilities are based on a combination of two different techniques. First, we follow [55] to derive fault tolerant unitary operations that require only the connectivity already necessary to perform syndrome measurements. Second, we give low-overhead extensions of the Tanner graph based on work by [46] which enable measurement of a single logical operator while preserving the thickness-2 implementability criterion. Together, these capabilities allow us to address any logical qubit.

A conceptual representation of the logical operators is shown in Figure 8. We first derive logical Pauli operators for quasi-cyclic LDPC codes, and find that the logical qubits divide into an “unprimed” and a “primed” block with equal size and symmetrical structure. We visualize the primed and unprimed block as two sheets featuring a 2D grid of logical operators. Some of these grid cells contain one of the $k/2$ logical qubits per sheet.

Next, we show that there exists a set of fault tolerant depth-four circuits that implement a small family of commuting logical CNOT circuits. These gates are based on automorphisms of the code: permutations of the data qubits that commute with the stabilizer. Based on their group structure we can think of the automorphism gates as translations of 2D grid of operators within each of the primed and unprimed blocks. Furthermore, we follow [55] to derive a fault tolerant operation based on a ZX-duality that also allows us to swap the two blocks while also applying Hadamard gates to all qubits.

Finally, we show how to leverage techniques from [46] to extend the Tanner graph to a larger Tanner graph defining a code whose stabilizer group contains one logical X operator of the original code. This construction acts as a “probe” that gives us access to one of the logical qubits. Measurements of logical X or Z operators on any qubit can be realized by conjugating this measurement by gates based on automorphisms and the ZX-duality. We can think of this as shifting any desired qubit to be the target of the probe using translation and exchange of the two blocks.

Logical X or Z measurement of any logical qubit also enables transfer of data into and out of the code using a teleportation circuit. This teleportation can be realized through a product measurement of the logical Pauli in the quasi-cyclic code, and a logical Pauli in another quantum error correction code. While the Tanner graph of the quasi-cyclic code demands thickness-2, we show how the ancilla system corresponding to logical measurement can be implemented in an “effectively planar” Tanner graph. This makes it possible to connect two such ancilla systems, one for each error correction code, within a thickness-2 implementation. This capability indicates the suitability of quasi-cyclic LDPC codes as a fault tolerant quantum memory.

8.1 Logical Pauli Operators

In this section we derive that the logical Pauli matrices of quasi-cyclic LDPC codes split into a “primed” and an “unprimed” block with $|\mathcal{M}| = \ell m$ many X operators and Z operators each. Operators in the primed block commute with operators in the unprimed block, and the two blocks have identical commutation structure.

We begin by introducing some new notation for Pauli matrices acting on the data qubits. We denote with $\mathbb{F}_2^{\mathcal{M}}$ the

set of polynomials over \mathbb{F}_2 with monomials from \mathcal{M} . This is equivalent to the quotient ring obtained from $\mathbb{F}_2[x, y]$ by identifying $x^\ell = y^m = 1$. With $x = S_m \otimes I$ and $y = I \otimes S_\ell$, the elements of $\mathbb{F}_2^{\mathcal{M}}$ have natural matrix representations, and can also be interpreted as sets since the coefficient on any particular $x \in \mathcal{M}$ is either 0 or 1.

For $P, Q \in \mathbb{F}_2^{\mathcal{M}}$, we can consider the set of qubits $q(L, \alpha)$ for $\alpha \in P$ and $q(R, \beta)$ for $\beta \in Q$. We write $X(P, Q)$ to denote a Pauli matrix acting as X on this collection of qubits, and identity elsewhere. Similarly, $Z(P, Q)$ denotes Z acting on $q(L, \alpha)$ for $\alpha \in P$ and $q(R, \beta)$ for $\beta \in Q$. For example, we can recall that $q(L, \beta)$ is connected to $q(X, \alpha)$ whenever $\beta \in A\alpha$, and see that the stabilizer corresponding to $q(X, \alpha)$ becomes $X(\alpha A, \alpha B)$. Similarly, the stabilizer corresponding to $q(Z, \alpha)$ can be written as $Z(\alpha B^T, \alpha A^T)$. There is also the following useful fact:

Lemma 5. $X(P, Q)$ anticommutes with $Z(\bar{P}, \bar{Q})$ if and only if $1 \in P\bar{P}^T + Q\bar{Q}^T$.

Proof. Write

$$P = \sum_{\alpha \in \mathcal{M}} p_\alpha \alpha, \quad \bar{P} = \sum_{\alpha \in \mathcal{M}} \bar{p}_\alpha \alpha, \quad Q = \sum_{\alpha \in \mathcal{M}} q_\alpha \alpha, \quad \bar{Q} = \sum_{\alpha \in \mathcal{M}} \bar{q}_\alpha \alpha,$$

where $p_\alpha, \bar{p}_\alpha, q_\alpha, \bar{q}_\alpha \in \mathbb{F}_2$ are coefficients. Pauli operators $X(P, Q)$ and $Z(\bar{P}, \bar{Q})$ overlap on a qubit $q(L, \alpha)$ iff $p_\alpha \bar{p}_\alpha = 1$ and overlap on a qubit $q(R, \alpha)$ iff $q_\alpha \bar{q}_\alpha = 1$. Thus $X(P, Q)$ and $Z(\bar{P}, \bar{Q})$ anti-commute iff $\sum_{\alpha \in \mathcal{M}} p_\alpha \bar{p}_\alpha + q_\alpha \bar{q}_\alpha$ is odd. We have

$$P\bar{P}^T = \sum_{\alpha \in \mathcal{M}} p_\alpha \bar{p}_\alpha 1 + \dots \quad \text{and} \quad Q\bar{Q}^T = \sum_{\alpha \in \mathcal{M}} q_\alpha \bar{q}_\alpha 1 + \dots$$

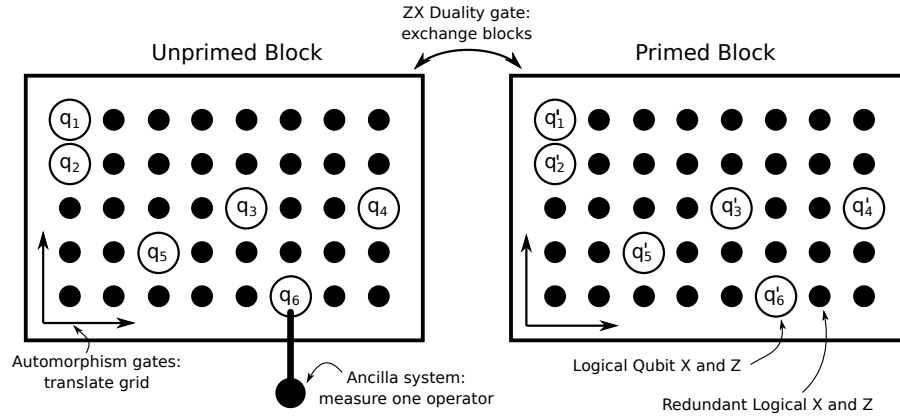


Figure 8: Conceptual diagram depicting the manner by which logical operators can be loaded into and out of a quasi-cyclic LDPC code. In Subsection 8.1 we derive that there are two blocks of logical Pauli operators corresponding to a 2d grid. Some subset of these grid elements can be chosen as logical qubits (large dots) and the other elements correspond to various Pauli products (small dots). In Subsection 8.2 we show that there are fault tolerant logical gates based on automorphisms that translate the grid of operators within each block, and in Subsection 8.3 we give a fault tolerant gate based on a ZX-duality [55] that swaps the two blocks. Finally, in Subsection 8.4 we show that there exists an ancilla system based on [46] that can measure one logical X operator. We can think of this system as a probe that can access one logical qubit. Together, these operations allow external access of every logical qubit and many of their products.

where dots represent all monomials different from 1. By linearity,

$$P\bar{P}^T + Q\bar{Q}^T = \sum_{\alpha \in \mathcal{M}} (p_\alpha \bar{p}_\alpha + q_\alpha \bar{q}_\alpha) 1 + \dots$$

Thus $X(P, Q)$ and $Z(\bar{P}, \bar{Q})$ anti-commute iff $P\bar{P}^T + Q\bar{Q}^T$ contains the monomial 1. \square

Without loss of generality, we can express logical Pauli matrices as either $X(P, Q)$ or $Z(Q^T, P^T)$ via a choice of $P, Q \in \mathbb{F}_2^M$. The operator $X(P, Q)$ commutes with the stabilizer $Z(\alpha B^T, \alpha A^T)$ whenever $1 \notin P(\alpha B^T)^T + Q(\alpha A^T)^T = \alpha^T(PB + QA)$. This is equivalent to $\alpha \notin PB + QA$. Since we must have $\alpha \notin PB + QA$ for all α , we see that $X(P, Q)$ commutes with the stabilizer whenever $PB + QA$ vanishes. Similarly we can derive that $Z(Q^T, P^T)$ commutes with the stabilizer when $PB + QA = 0$.

We aim to construct a family of solutions to $PB + QA = 0$ which give rise to a basis of logical qubits defined by a set of operators $\{\bar{X}_1, \bar{X}_2, \dots, \bar{Z}_1, \bar{Z}_2, \dots\}$ with the correct commutation relations. To do so, let us make some observations about Pauli operators defined via solutions to $PB + QA = 0$. First, if P, Q are a solution, then so are $\alpha P, \alpha Q$ for any $\alpha \in \mathcal{M}$, so each P, Q immediately gives rise to a family of $|\mathcal{M}| = lm$ logical operators for both X and Z . Second, consider using the same P, Q to define both $X(\alpha P, \alpha Q)$ and $Z(\beta Q^T, \beta P^T)$. Then these operators always commute because $\beta \alpha^T \in PQ + QP = 0$ never holds. So we require at least two solutions to $PB + QA = 0$ to define a set of operators with nontrivial commutation relations.

For reasons described later in Subsection 8.4, we would like a logical X operator with no support on $q(R)$. To this end, we select $f, g, h \in \mathbb{F}_2^M$ that satisfy $Bf = 0$ and $gB + hA = 0$, yielding two solutions to the equation $PB + QA = 0$ with $P, Q = f, 0$ and $P, Q = g, h$. These yield the following family of logical operators for all $\alpha \in \mathcal{M}$:

$$\begin{aligned} \bar{X}_\alpha &:= X(\alpha f, 0) & \bar{Z}_\alpha &:= Z(\alpha h^T, \alpha g^T) \\ \bar{X}'_\alpha &:= X(\alpha g, \alpha h) & \bar{Z}'_\alpha &:= Z(0, \alpha f^T) \end{aligned} \tag{13}$$

For all α, β , we see that $\bar{X}_\alpha, \bar{Z}'_\beta$ always commute because $f0^T + 0f^T = 0$, and $\bar{X}'_\beta, \bar{Z}_\alpha$ always commute because $gh + hg = 0$. Furthermore, $\bar{X}_\alpha, \bar{Z}_\beta$ and $\bar{X}'_\alpha, \bar{Z}'_\beta$ form anticommuting pairs when $\alpha^T \beta \in fh$. We see that we have constructed two independent blocks of logical operators with symmetrical structure. It follows that each of these blocks must contain a set of operators that define $k/2$ qubits. We name these the “unprimed” and “primed” logical blocks with $\bar{X}_\alpha, \bar{Z}_\beta$ and $\bar{X}'_\alpha, \bar{Z}'_\beta$ respectively.

Not all choices of f, g, h span all k logical qubits, but valid choices are readily enumerated in software. Solutions to $Bf = 0$ and $gB + hA = 0$ correspond to null spaces of B and $\begin{bmatrix} B \\ A \end{bmatrix}$ respectively, which can be constructed by Gaussian elimination. Gaussian elimination can also be used to check if the operators $\bar{X}_\alpha, \bar{Z}_\alpha, \bar{X}'_\alpha, \bar{Z}'_\alpha$ together span k qubits up to the stabilizer. We find all codes in Table 3 admit several such choices of f, g, h , although for the $[[756, 16, \leq 34]]$ code the choice of f has many terms, making $X(f, 0)$ have prohibitively high weight. In Table 7 we show choices of f that also either achieve the minimum weight or something close to it.

To identify logical qubits we can enumerate choices of monomials $\{n_1, n_2, \dots, n_{k/2}\}$ and $\{m_1, m_2, \dots, m_{k/2}\}$ such that $n_i^T m_j \in fh$ exactly when $i = j$. That way $\bar{X}_i := \bar{X}_{n_i}$ and $\bar{Z}_i := \bar{Z}_{m_i}$, as well as $\bar{X}'_i := \bar{X}'_{n_i}$ and $\bar{Z}'_i := \bar{Z}'_{m_i}$ form a choice of logical qubits \bar{X}_i, \bar{Z}_i . A brute force search readily finds choices of $\{n_i\}, \{m_i\}$.

8.2 Logical Gates based on Automorphisms

An automorphism of an error correction code is a permutation of the physical qubits that is equivalent to a permutation of the checks (more generally, an automorphism can map a check operator to a product of check operators). We focus on permutations that are implementable using fault tolerant circuits within the connectivity already required for syndrome measurements.

[[72, 12, 6]] (Cost: 15)	[[90, 8, 10]] (Cost: 25)	[[108, 8, 10]] (Cost: 30)
[[144, 12, 12]] (Cost: 30)	[[288, 12, 18]] (Cost: 45)	[[360, 12, ≤ 24]] (Cost: 75)

Table 7: Choices of polynomials f such that $\bar{X}_\alpha := X(\alpha f, 0)$ as defined in equation 13 are logical Pauli operators. These choices of \bar{X}_α have no support on the $q(R)$ block which simplifies the construction of the ancilla system described in Subsection 8.4. They also achieve either ensure that $X(f, 0)$ is a minimum weight operator or something not much higher weight, which reduces the size of the ancilla system. The dots in the figures denote the monomials $x^i y^j$ contained in the polynomial f in question. The ‘Cost’ figure denotes the number of qubits per layer in an ancilla system capable of measuring $X(f, 0)$ - see Subsection 8.4 for details.

The existing connectivity admits some natural fault tolerant circuits implementing a particular family of permutations on the data qubits. Quasi-cyclic LDPC codes feature two data registers $q(L), q(R)$ and two check registers $q(X), q(Z)$. We consider circuits that transfer the qubits from the data registers to the ancilla registers, and back again on a different path. The adjacency matrices describing the connectivity between the data and the ancilla registers are given by A and B , which are the sum of three monomials A_1, A_2, A_3 and B_1, B_2, B_3 in \mathcal{M} . Each monomial is a permutation and thus describes a vertex-disjoint set of edges between the data and ancilla block. Hence, all swaps along these edges can be parallelized. In a single circuit we can either swap along the edges defined by A which are $q(L) \leftrightarrow q(X)$ and $q(R) \leftrightarrow q(Z)$, or along edges defined by B which are $q(L) \leftrightarrow q(Z)$ and $q(R) \leftrightarrow q(X)$. See also Figure 6 A).

The monomial defining the particular set of edges in each of these sets of swaps can be chosen independently for each stage of the permutation (data \rightarrow ancilla or ancilla \rightarrow data), and on each side of the Tanner graph. For example, we can select any $A_j, A_k, A_{j'}, A_{k'}$ and move $q(L) \rightarrow_{A_j^T} q(X) \rightarrow_{A_k} q(L)$ and simultaneously move $q(R) \rightarrow_{A_{k'}} q(Z) \rightarrow_{A_{j'}^T} q(R)$. However, we will see later that it is necessary to select $A_j = A_{j'}$ and $A_k = A_{k'}$. Furthermore, these swaps admit a standard optimization: if we initialize the check registers $q(X), q(Z)$ to the $|0\rangle$ state, then circuits implementing these permutations have CNOT depth four. If we also reset qubits to the $|0\rangle$ state in between the swaps wherever possible, we obtain circuits whose errors cannot propagate between physical qubits, and are hence fault tolerant. See Table 8.

We now verify that the permutations implemented by the circuits described above are indeed automorphisms. After having applied an ‘A’ type permutation based on A_j, A_k , the qubits are permuted by $q(L, \alpha) \leftrightarrow q(L, A_k^T A_j \alpha)$ and $q(R, \alpha) \leftrightarrow q(R, A_k^T A_j \alpha)$. We see that this transforms a Pauli matrix by $X(P, Q) \rightarrow X(A_j A_k^T P, A_j A_k^T Q)$. Consequently, the stabilizers are transformed as $X(\alpha A, \alpha B) \rightarrow X(\alpha A_j A_k^T A, \alpha A_j A_k^T B)$, which is the same as permuting the X checks by $\alpha \rightarrow \alpha A_j A_k^T$. The Z stabilizers are also permuted by $\alpha \rightarrow \alpha A_j A_k^T$, so the described circuit indeed implements an automorphism. Notice also that this only works because the $q(L)$ and $q(R)$ blocks were transformed by the same $A_j A_k^T$. The ‘B’ type permutations can be verified to be automorphisms in the same manner, permuting the checks by some $B_j B_k^T$.

These automorphisms allow us to fault tolerantly implement a subgroup of the Clifford gates. As we saw in Section 4, specifically Lemma 3, shifts of the form $A_j A_k^T$ or $B_j B_k^T$ generate the entire group \mathcal{M} whenever the Tanner graph is connected. Therefore, by leveraging these permutations as generators, we can perform all translations of the tori containing $q(L), q(R)$ using fault tolerant circuits of varying depth. An automorphism defined by an element $s \in \mathcal{M}$ transforms $\bar{X}_{n_i} \rightarrow \bar{X}_{sn_i}, \bar{Z}_{m_i} \rightarrow \bar{Z}_{sm_i}$ and similarly for the primed logical Pauli matrices. This capability is critical for addressing all logical qubits.

We can also comment on the nature of these operations as logical gates, although they are less useful in this sense. There is one such operation per element in \mathcal{M} , and since \mathcal{M} is Abelian the subgroup of Clifford gates implemented by these automorphisms must be Abelian as well. A transformation of this form cannot act like the logical identity so all of these gates (except $s = 1$) are nontrivial. Since automorphism operations take \bar{X} to \bar{X} and \bar{Z} to \bar{Z} , and they must hence be logical CNOT circuits up to a logical Pauli correction. While it is not clear how to use these CNOT circuits to facilitate useful computations, they may make for interesting test cases in an implementation.

8.3 Accessing the Primed Block via a ZX-duality

A ZX-duality is a permutation of the logical qubits that commutes with the stabilizer, except that it turns X checks into Z checks and Z checks into X checks. A physical circuit implementing this permutation and then applying Hadamard to all data qubits always acts as a logical gate [55]. In this section we focus on the implementation of a particular ZX-duality with applications for readout. We leave discovery and implementation of other ZX-dualities for future work. In particular, we derive a general method for constructing fault tolerant circuits for implementing a particular ZX-duality that is present in all quasi-cyclic LDPC codes. While the circuits from this construction are generally quite expensive, they may be amenable to further optimization and can be used sparingly in practice.

‘A’ type automorphism based on any A_j, A_k

<pre> for $\alpha \in \mathcal{M}$ do InitZ $q(X, \alpha)$ CNOT $q(L, A_j \alpha)$ $q(X, \alpha)$ CNOT $q(X, \alpha)$ $q(L, A_j \alpha)$ InitZ $q(L, A_k^T \alpha)$ CNOT $q(X, \alpha)$ $q(L, A_k \alpha)$ CNOT $q(L, A_k \alpha)$ $q(X, \alpha)$ end for </pre>	<pre> for $\alpha \in \mathcal{M}$ do InitZ $q(Z, \alpha)$ CNOT $q(R, \alpha)$ $q(Z, A_j \alpha)$ CNOT $q(Z, A_j \alpha)$ $q(R, \alpha)$ InitZ $q(R, A_k \alpha)$ CNOT $q(Z, A_k \alpha)$ $q(R, \alpha)$ CNOT $q(R, \alpha)$ $q(Z, A_k \alpha)$ end for </pre>
--	--

‘B’ type automorphism based on any B_j, B_k

<pre> for $\alpha \in \mathcal{M}$ do InitZ $q(X, \alpha)$ CNOT $q(R, B_j \alpha)$ $q(X, \alpha)$ CNOT $q(X, \alpha)$ $q(R, B_j \alpha)$ InitZ $q(R, B_k^T \alpha)$ CNOT $q(X, \alpha)$ $q(R, B_k \alpha)$ CNOT $q(R, B_k \alpha)$ $q(X, \alpha)$ end for </pre>	<pre> for $\alpha \in \mathcal{M}$ do InitZ $q(Z, \alpha)$ CNOT $q(L, \alpha)$ $q(Z, B_j \alpha)$ CNOT $q(Z, B_j \alpha)$ $q(L, \alpha)$ InitZ $q(L, B_k \alpha)$ CNOT $q(Z, B_k \alpha)$ $q(L, \alpha)$ CNOT $q(L, \alpha)$ $q(Z, B_k \alpha)$ end for </pre>
--	--

Table 8: Circuits implementing automorphisms of a quasi-cyclic LDPC code within the connectivity already present for syndrome checks. These circuits are fault tolerant and have CNOT depth four. If $s = A_j A_k^T$ or $s = B_j B_k^T$, then the logical gate implemented by these automorphisms performs the transformation $\bar{X}_\alpha, \bar{Z}_\alpha, \bar{X}'_\alpha, \bar{Z}'_\alpha \rightarrow \bar{X}_{s\alpha}, \bar{Z}_{s\alpha}, \bar{X}'_{s\alpha}, \bar{Z}'_{s\alpha}$.

Consider a permutation of data qubits that swaps $q(L, \alpha)$ with $q(R, \alpha^T)$ for all $\alpha \in \mathcal{M}$. A check qubit $q(X, \beta)$ which previously implemented the stabilizer $X(\beta A, \beta B)$ now is connected to the qubits $q(L, (\beta B)^T)$ and $q(R, (\beta A)^T)$ instead, corresponding to the check $Z(\beta^T B^T, \beta^T A^T)$. We see that this permutation switches the stabilizer implemented by $q(X, \beta)$ with the stabilizer implemented by $q(Z, \beta^T)$, so this permutation is indeed a ZX-duality.

We can also see that implementing this permutation and applying Hadamard to all qubits takes logical Pauli matrices to logical Pauli matrices. In particular, the operation swaps $\bar{X}_\alpha = X(\alpha f, 0)$ with $\bar{Z}'_{\alpha^T} = Z(0, \alpha^T f^T)$, as well as $\bar{Z}_\alpha = Z(\alpha h^T, \alpha g^T)$ with $\bar{X}'_{\alpha^T} := X(\alpha^T g, \alpha^T h)$. This operation swaps the primed and unprimed logical blocks, transposes the grid of operators, and applies logical Hadamard to all qubits. Since we can measure logical X for all qubits in the unprimed block using the ancilla system described in Subsection 8.4, we can use this operation to measure logical Z for qubits in the primed block.

For the rest of this section we describe a fault tolerant method for implementing this operation. We begin with exchanging $q(L)$ and $q(R)$: since these blocks are connected by pairs of edges in $q(X)$ and $q(Z)$, for any $A_i \in A$ and $B_j \in B$ there exists a loop connecting the qubits $q(L, \alpha) \rightarrow q(X, A_i^T \alpha) \rightarrow q(R, B_j A_i^T \alpha) \rightarrow q(Z, B_j \alpha) \rightarrow q(L, \alpha)$. A circuit identical in shape to those in Table 8 hence performs a fault tolerant exchange of $q(L, \alpha)$ and $q(R, B_j A_i^T \alpha)$ for all α . The additional shift of $B_j A_i^T$ can be removed via an additional automorphism gate. It remains to exchange $q(L, \alpha) \leftrightarrow q(L, \alpha^T)$, as well as $q(R, \alpha) \leftrightarrow q(R, \alpha^T)$ for all α , which is significantly more complicated. We focus on $q(L, \alpha) \leftrightarrow q(L, \alpha^T)$ in our discussion but it will be clear the exact same transformations are implementable on $q(R)$ in parallel with those on $q(L)$.

Fault tolerant implementation of the permutation $q(L, \alpha) \leftrightarrow q(L, \alpha^T)$ can be achieved using a more sophisticated

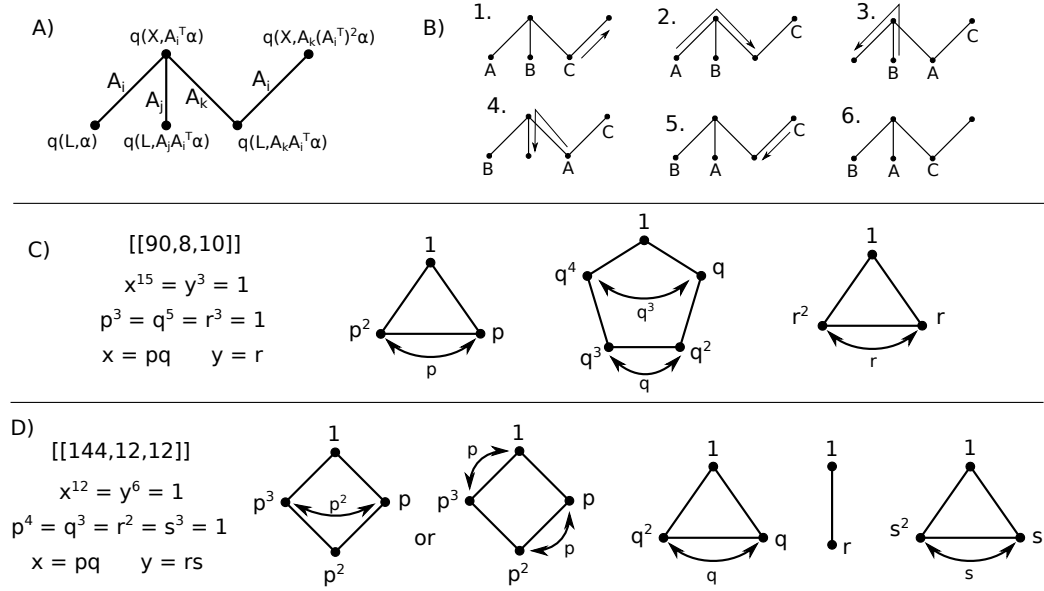


Figure 9: Diagrams for the description of the implementation of the ZX-duality permutation. A) A subgraph of the Tanner graph providing enough connectivity to fault tolerantly swap $q(L, \alpha)$ and $q(L, A_j A_i^T \alpha)$. B) A sequence of shifts of the data on the qubits in the $q(L)$ block that performs the desired exchange without interacting qubits directly. A naive implementation of this sequence has CNOT depth 12. C) D) Decomposition of the generators of \mathcal{M} via the classification of finite Abelian groups for two different codes. Drawing the Cayley graph of the subgroup for each generator reveals the ratios defining pairs of qubits that must be exchanged to implement the permutation $q(L, \alpha) \leftrightarrow q(L, \alpha^T)$.

version of the fault tolerant circuits in Table 8 used for implementing automorphisms. These circuits relied on the existence of a connected loop of alternating check and data qubits, enabling a short depth fault tolerant circuit implementing a cyclic permutation of the data qubits therein. The same connectivity can be leveraged to implement a fault tolerant nearest neighbor swap of two data qubits connected by a check qubit. The fault tolerance of these circuits relies on the same principle: while a swap gate acting on two qubits containing data is not fault tolerant, moving a data qubit onto a blank qubit is. Figure 9 A) shows a subgraph of the Tanner graph consisting of several connected qubits in the $q(L)$ and $q(X)$ block, and Figure 9 B) shows a sequence of operations where two data qubits can be exchanged without ever interacting directly. This gives us the following capability: whenever the circuits in Table 8 can implement the cyclic permutation $q(L, \alpha) \rightarrow q(L, s\alpha)$ for all α , there also exists a circuit that can swap $q(L, \alpha)$ and $q(L, s\alpha)$ for a particular α . Matching circuits exist for $q(R)$, and can be implemented simultaneously.

To decompose $q(L, \alpha) \leftrightarrow q(L, \alpha^T)$ into a sequence of swaps, it will be helpful to consider the group structure of \mathcal{M} . Consider for example the $[[90, 8, 10]]$ code with $x^{15} = y^3 = 1$. Following the classification of finite Abelian groups we see that $\mathcal{M} \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_3$. We can re-express elements of \mathcal{M} using generators p, q, r with $p^3 = q^5 = r^3 = 1$ where $x = pq$ and $y = r$. Transforming α to α^T amounts to decomposing α as $\alpha = p^i q^j r^k$ and exchanging the qubit with $\alpha^T = p^{-i} q^{-j} r^{-k}$.

This exchange $p^i q^j r^k \leftrightarrow p^{-i} q^{-j} r^{-k}$ can be split into a sequence of swaps that are implementable with the method described above using Figure 9 A) and B). It suffices to be able to exchange for any $\alpha = q^j r^k$ the qubits $q(L, p^i \alpha) \leftrightarrow q(L, \alpha p^{-i})$, as well as for any $\alpha = p^i r^k$ the qubits $q(L, q^j \alpha) \leftrightarrow q(L, \alpha q^{-j})$, and finally for any $\alpha = p^i q^j$

the qubits $q(L, r^k \alpha) \leftrightarrow q(L, \alpha r^{-k})$. This, for any i, j, k , creates a sequence of qubits $q(L, p^i q^j r^k) \leftrightarrow q(L, p^{-i} q^j r^k) \leftrightarrow q(L, p^{-i} q^{-j} r^k) \leftrightarrow q(L, p^{-i} q^{-j} r^{-k})$ where swaps are possible along each nearest neighbor. This is sufficient for swapping the first and last qubit in the chain. The implementation of the individual generators like $q(L, \alpha q^i) \leftrightarrow q(L, \alpha q^{-i})$ swaps may also involve additional intermediate qubits, but this only lengthens the chain and does not prohibit implementation.

The resources required for swapping $q(L, p^i \alpha) \leftrightarrow q(L, \alpha p^{-i})$ where $p^3 = 1$ and similarly for other generators depends on the order of the generator p as well as the ratios $A_i A_j^T$ that can be formed using terms $A_i, A_j \in A$ or similar ratios from B . See Figure 9 C). Plotting the Cayley graph of the cyclic subgroup spanned by p immediately reveals that since p is order three, only a single ratio $B_i B_j^T = p$ is needed in order to swap any qubits marked p^1 and p^2 , while leaving p^0 qubits in place. Indeed since $B = 1 + x^2 + x^7 = 1 + p^2 q^2 + p q^2$ we can implement $p = (p^2 q^2)(p q^2)^T$ in a single layer of transforms in Figure 9 B).

The exchange $q(L, \alpha q^i) \leftrightarrow q(L, \alpha q^{-i})$ with $q^5 = 1$ requires two such ratios q and q^2 , the minimal depth expression of which demands the chaining together of two such transforms each. In other codes, like the $[[144, 12, 12]]$ code, we encounter generators p, q, r, s of order $p^4 = q^3 = r^2 = s^3 = 1$. Elements of order two like r require no swaps at all, and elements of order four like p can be implemented either using the ratio p^2 or just p , as shown in Figure 9 D). Numerical searches can quickly compute the most efficient decompositions of the required swaps. We give the orders of the generators, the ratios defining the required swaps, and the number of transforms required to implement them in Table 9.

We emphasize that the swap $q(L, p^i \alpha) \leftrightarrow q(L, \alpha p^{-i})$ can be performed for all $\alpha = q^j r^k$ simultaneously in parallel. This stems from the structure of the exchange circuit in Figure 9 B). This circuit performs the swap $q(L, \alpha) \leftrightarrow q(L, A_j A_i^T \cdot \alpha)$ while using the qubit $q(L, A_k A_i^T \cdot \alpha)$ as scratch space. However, we can simultaneously want to swap $q(L, A_k A_i^T \cdot \alpha) \leftrightarrow q(L, A_j A_i^T \cdot A_k A_i^T \cdot \alpha)$ since the first step of the exchange circuit in Figure 9 B) is to move the data marked ‘A’ away from the qubit holding it, just as if it were a piece of data marked ‘C’ for a different exchange.

For clarity, we compute the total depth of the circuit for the $[[144, 12, 12]]$ code without any further optimization. The ratios p, q, s can be implemented using two ratios each via $p = x^{-3} y \cdot y^{-2} y$, $q = y^{-3} x^2 \cdot y^{-3} x^2$ and $s = y^{-2} y \cdot y^{-2} y$. This results in a chain $q(L, \alpha) \leftrightarrow q(L, \alpha') \leftrightarrow q(L, \alpha'') \dots \leftrightarrow q(L, \alpha^T)$ of length six (counting the number of \leftrightarrow s). We can swap the qubits at the ends of a chain of length n using $2n-1$ many nearest neighbor swaps. Each swap circuit of the form Figure 9 B) can be implemented in CNOT depth twelve, resulting in CNOT depth $(2 \cdot 6 - 1) \cdot 12 = 132$ to implement $q(L, \alpha) \leftrightarrow q(L, \alpha^T)$.

Despite its fault tolerance, the implementation of this logical operation is clearly significantly more expensive than that of the automorphisms. Since the intermediate permutations corresponding to each of the generators p, q, r are not ZX dualities in general, it will not be possible in general to perform error correction during this long operation. However, the significant overhead of this operation may be worth such a large cost, since it grants us the capability of accessing the primed block of qubits, effectively doubling the storage capacity of the code. This operation can also be used significantly more sparingly than the automorphism gates, and may be amenable to additional optimization.

8.4 Logical Measurements

In this section we describe how to leverage methods from [46] to implement a measurement of $\bar{X}_1 := X(f, 0)$. As described above, this capability suffices to measure X for all logical qubits in the unprimed block and logical Z for qubits in the primed block. We can also use this technique to measure various Pauli product operators by measuring \bar{X}_α for \bar{Z}'_α for α not corresponding to logical qubits.

The measurement is facilitated by an ancilla system that extends the Tanner graph of the original code. The code defined by this extended Tanner graph contains the logical operator of interest as a stabilizer, enabling its fault tolerant measurement. A sketch of the structure of this ancilla system is given in Figure 10 C). For the logical operator $X(f, 0)$, we consider a subgraph of the Tanner graph consisting of $q(L, f)$ as well as $q(Z, \alpha)$ operators corresponding to checks with support on $q(L, f)$. This subgraph is copied several times, the qubits are given different roles, and the

Code	Base Order	Reduced Order	Required Ratios	Swap Chain Length
[[72, 12, 6]]	x^6, y^6	p^2, q^3, r^2, s^3	q, s	4
[[90, 8, 10]]	x^{15}, y^3	p^3, q^5, r^3	p, q, q^2, r	6
[[108, 8, 10]]	x^9, y^6	p^9, q^2, r^3	p, p^3, p^5, p^7, r	9
[[144, 12, 12]]	x^{12}, y^6	p^4, q^3, r^2, s^3	p, q, s	6
[[288, 12, 18]]	x^{12}, y^{12}	p^4, q^3, r^4, s^3	p, q, r, s	10
[[360, 12, ≤ 24]]	x^{30}, y^6	p^2, q^3, r^5, s^2, t^3	q, ps, psr^2, psr^3, t	11

Table 9: Table deriving the steps in the circuit implementing the $q(L, \alpha) \leftrightarrow q(L, \alpha^T)$, permutation for the ZX-duality for several codes. The generators of \mathcal{M} are decomposed into generators following the decomposition of finite Abelian groups. Following Figure 9 B) and C) these generators demand a set of ratios of terms in A or B which define fault tolerantly implementable exchanges of qubits with corresponding labels. The result is a decomposition of $q(L, \alpha) \leftrightarrow q(L, \alpha^T)$ into a chain $q(L, \alpha) \leftrightarrow q(L, \alpha') \leftrightarrow q(L, \alpha'') \leftrightarrow \dots \leftrightarrow q(L, \alpha^T)$ with length as shown (counting the number of arrows, \leftrightarrow). Note the special implementation of the ratios in the [[360, 12, ≤ 24]] code: the ratios r^2, r^3 are not implementable, but psr^2, psr^3 are. This is fine if we can also perform the ps ratio on its own to remove the additional transformation on some of the qubits.

copies are connected together as shown in the figure. With enough copies, the code defined by the extended Tanner graph has the same distance as the original code.

The main challenge of implementing this ancilla system, in addition to minimizing its size, is to show that the extended Tanner graph satisfies the thickness-2 constraint. If our goal is to leverage this ancilla system to measure a Pauli product measurement between two different error correction codes, then arguably a thickness-2 extension of the Tanner graph does not suffice since there is no way of connecting these two systems in the manner of Figure 3 of [46]. To this end, we show how to make the subgraph corresponding to the ancilla system “effectively planar”: while the graph has thickness-2, the planar graph in one plane consists entirely of connected components with two vertices. Given these properties of the embedding of a single ancilla system, a connection between two error correction codes may be facilitated by a construction that is thickness-2 overall.

Effectively planar embedding of the ancilla system relies on the fact that the logical operator $X(f, 0)$ has no support on the $q(R)$ block. An implementation of more general logical operators is possible, but would require a graph that renders many ancilla qubits inaccessible from the outside. Limiting ourselves to $X(f, 0)$ sometimes prohibits us from selecting a minimum-weight operator, but it is nonetheless possible to make the support of $X(f, 0)$ rather small compared to the code as a whole. We can also minimize the number of copies of $q(Z)$ qubits in the system by considering only a set of linearly dependent Z checks. Table 7 shows choices of polynomials f defining $X(f, 0)$, as well as the number of qubits in each layer of the resulting ancilla system.

Given that the ancilla is only supported on qubits of type $q(L)$ and $q(Z)$, we now show that an effectively planar embedding is possible. Our construction relies on the properties of the ‘wheel graphs’ we defined in Section 4 and showed in Figure 5 A) and B). The ‘B’ wheels of the original code may be arranged in such a way that the $q(L)$ and $q(Z)$ qubits are placed on the outside of the wheel - we will need this property to connect the ancilla system to the main code.

Let us now consider the structure of the wheel graphs for each layer of the ancilla system. The qubits in each layer take on a variety of different roles: the qubits alternately perform checks or store data depending on their role in the original Tanner graph. Thus, it is easier to refer to the qubits by their color: bLue and oRange for data, as well as red X checks and green Z checks. When the ‘B’ wheel graph is truncated to the qubits required by the Tanner graph, Figure 10 B) shows that the resulting graph merely consists of circles. This exposes the blue and green qubits on both the inside and outside of the circle. The main idea of the construction is to nest the ‘B’ wheels of the the

original Tanner graph inside several concentric circles corresponding to the layers of the ancilla system. Since the blue and green qubits are always exposed, connections in between the layers is possible within a single plane: see Figure 10 D). The structure of the connections within the ‘A’ wheels is particularly simple: looking at Figure 10 A), we see that the subgraph corresponding to connected blue and green qubits consists entirely of connected components with two qubits each.

Our construction achieves both favorable embedding properties allowing data transfer between codes, but also is close to minimizing the size of the ancilla system given the techniques of [46]. An advantage of the measurement method described by [46] is its applicability to a wide range of quantum error correction codes. It may be possible to measure logical qubits in a more efficient manner that is more tailored to this family of error correction codes.

9 Conclusion

In summary, we offered a new perspective on how a fault-tolerant quantum memory could be realized using near-term quantum processors with a small qubit overhead. Our approach complements a concatenation-based scheme by Pattison, Krishna, and Preskill [56] where each data qubit of a high-rate LDPC code is additionally encoded by the surface code. Although the concatenation approach makes use of the high error threshold of the surface code and its geometric locality to address quantum hardware limitations such as a relatively high noise rate and limited qubit connectivity, the additional surface code encoding incurs a significant qubit overhead, partially negating the advantages offered by LDPC codes. Here we have shown that the concatenation step can be avoided by introducing examples of high-rate LDPC codes which have nearly the same error threshold as the surface code itself. Although these LDPC codes are not geometrically local, qubit connectivity required for syndrome measurements is described by a thickness-two graph which can be implemented using two planar degree-3 layers of qubit couplers. This is a valid architectural solution for platforms based on superconducting qubits. Numerical simulations performed for the circuit-based noise model indicate that the proposed LDPC codes compare favorably with the surface code in the practically relevant range of error rates $p \geq 0.1\%$ offering the same level of error suppression with nearly 15x reduction in the qubit overhead.

The key hardware challenges to enable the new codes with superconducting qubits are:

1. the development of a low-loss second layer,
2. the development of qubits that can be coupled to 7 connections (6 buses and 1 control line), and
3. the development of long-range couplers.

These are all difficult to solve but not impossible. For the first challenge, we can imagine a small change to the packaging [47] which was developed for the IBM Quantum Eagle processor [57]. The simplest would be to place the extra buses on the opposite side of the qubit chip. This would require the development of high Q through substrate vias (TSV) which would be part of the coupling buses and as such would require intensive microwave simulation to make sure these TSVs could support microwave propagation while not introducing large unwanted crosstalk.

The second challenge is an extension of the number of couplers from the heavy hex lattice arrangement [58] which is 4 (3 couplers and 1 control) to 7. The implication of this is that the cross-resonance gate, which has been the core gate used in large quantum systems for the past few years, would not be the path forward. This is due to fact that the qubits in cross-resonance gate are not tunable and as such for a large device with a large number of connections the probability of a energy collisions (not just the qubit levels but also higher levels of the transmon) trends to one very fast [59]. This is because of frequency requirements for the gate to work properly and intrinsic device variability, which is fundamental to Josephson junction fabrication. However, with the tunable coupler [60, 61], which was used in the IBM Quantum Egret and now being developed for the IBM Quantum Heron, this problem no longer exists as the qubits can be designed to be further apart. This new gate is also similar to the gates used by Google Quantum AI

[62], which have shown that a square lattice arrangement is possible. Extending the coupling map to 7 connections will require significant microwave modeling; however, typical transmons have about 60fF of capacitance and each gate is around 5fF to get the appropriate coupling strengths to the buses, so it is fundamentally possible to develop this coupling map without changing the properties of the transmon qubits which have been shown to have larger coherence and are stable.

The final challenge is the most difficult. For the buses that are short enough so that the fundamental mode can be used the standard circuit QED model holds. However, to demonstrate the 144-qubit code some of the buses will be long enough that we will require frequency engineering. One way to achieve this is with filtering resonators, and a proof of principle experiment was demonstrated in Ref. [63].

Our work leaves several open questions concerning quasi-cyclic LDPC codes and their applications.

1. What are tradeoffs between the code parameters n, k, d and can one achieve a constant non-zero encoding rate and a growing distance?
2. Are there more general LDPC codes compatible with our syndrome measurement circuit(s)? We expect that the same circuit applies to any two-block LDPC code based on an Abelian group [35, 36]. However our circuit analysis breaks down for non-Abelian groups.
3. Our work gives a depth-7 syndrome measurement circuit, as measured by the number of CNOT layers. Is it possible to reduce the circuit depth? Numerical experiments performed for the code $[[72, 12, 6]]$ indicate that this code may have no depth-6 syndrome measurement (SM) circuit [64].
4. We observed that a depth-7 SM circuit is not unique. A natural next step is identifying a SM circuit that works best for a particular code. In addition, it may be possible to improve the circuit-level distance by using different SM circuits in different syndrome cycles. Even though some low-weight fault paths are not detectable by any single circuit, such fault paths may be detected if two circuits are used in tandem.
5. How much would the error threshold change for a noise biased towards measurement errors? Note that measurements are the dominant source of noise for superconducting qubits. Since the considered quasi-cyclic codes have a highly redundant set of check operators, one may expect that they offer an extra protection against measurement errors.
6. The general purpose BP-OSD decoder used here may not be fast enough to perform error correction in real time. Is there a faster decoder making use of the special structure of quasi-cyclic codes?
7. How to apply logical gates? While our work gives a fault-tolerant implementation of certain logical gates, these gates offer very limited computational power and are primarily useful for implementing memory capabilities.

Acknowledgements

The authors thank Ben Brown, Oliver Dial, Alexander Ivrii, Tomas Jochym-O'Connor, Yunseong Nam, Matthias Steffen, and Kevin Tien for stimulating discussions at various stages of this project. The authors acknowledge the IBM Research Cognitive Computing Cluster service for providing resources that have contributed to the research results reported within this paper.

References

- [1] Michael A. Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

- [2] Seth Lloyd. Universal quantum simulators. *Science*, 273(5278):1073–1078, 1996.
- [3] Hefeng Wang, Sabre Kais, Alán Aspuru-Guzik, and Mark R. Hoffmann. Quantum algorithm for obtaining the energy spectrum of molecular systems. *Physical Chemistry Chemical Physics*, 10(35):5388–5393, 2008.
- [4] Markus Reiher, Nathan Wiebe, Krysta M. Svore, Dave Wecker, and Matthias Troyer. Elucidating reaction mechanisms on quantum computers. *Proceedings of the National Academy of Sciences*, 114(29):7555–7560, 2017.
- [5] Yuri Alexeev, Dave Bacon, Kenneth R. Brown, Robert Calderbank, Lincoln D. Carr, Frederic T. Chong, Brian DeMarco, Dirk Englund, Edward Farhi, Bill Fefferman, et al. Quantum computer systems for scientific discovery. *PRX Quantum*, 2(1):017001, 2021.
- [6] Jay M. Gambetta, Jerry M. Chow, and Matthias Steffen. Building logical qubits in a superconducting quantum computing system. *npj Quantum Information*, 3(1):2, 2017.
- [7] Pranav S. Mundada, Aaron Barbosa, Smarak Maity, Yulun Wang, T. M. Stace, Thomas Merkh, Felicity Nielson, Andre R. R. Carvalho, Michael Hush, Michael J. Biercuk, and Yuval Baum. Experimental benchmarking of an automated deterministic error suppression workflow for quantum algorithms, 2023.
- [8] Nathalie P. De Leon, Kohei M. Itoh, Dohun Kim, Karan K. Mehta, Tracy E. Northup, Hanhee Paik, B.S. Palmer, Nitin Samarth, Sorawis Sangtawesin, and David W. Steuerman. Materials challenges and opportunities for quantum computing hardware. *Science*, 372(6539):eabb2823, 2021.
- [9] Antonio D. Córcoles, Jerry M. Chow, Jay M. Gambetta, Chad Rigetti, J. R. Rozen, George A. Keefe, Mary Beth Rothwell, Mark B. Ketchen, and M. Steffen. Protecting superconducting qubits from radiation. *Applied Physics Letters*, 99(18):181906, 11 2011.
- [10] Antti P. Vepsäläinen, Amir H. Karamlou, John L. Orrell, Akshunna S. Dogra, Ben Loer, Francisca Vasconcelos, David K. Kim, Alexander J. Melville, Bethany M. Niedzielski, Jonilyn L. Yoder, et al. Impact of ionizing radiation on superconducting qubit coherence. *Nature*, 584(7822):551–556, 2020.
- [11] Ted Thorbeck, Andrew Eddins, Isaac Lauer, Douglas T. McClure, and Malcolm Carroll. Two-level-system dynamics in a superconducting qubit due to background ionizing radiation. *PRX Quantum*, 4:020356, Jun 2023.
- [12] Yukai Wu, Sheng-Tao Wang, and L.-M. Duan. Noise analysis for high-fidelity quantum entangling gates in an anharmonic linear Paul trap. *Physical Review A*, 97(6):062325, 2018.
- [13] Matthew J. Boguslawski, Zachary J. Wall, Samuel R. Vizvary, Isam Daniel Moore, Michael Bareian, David T.C. Allcock, David J. Wineland, Eric R. Hudson, and Wesley C. Campbell. Raman scattering errors in stimulated-Raman-induced logic gates in Ba^{+} 133. *Physical Review Letters*, 131(6):063001, 2023.
- [14] A. A. Houck, J. A. Schreier, B. R. Johnson, J. M. Chow, Jens Koch, J. M. Gambetta, D. I. Schuster, L. Frunzio, M. H. Devoret, S. M. Girvin, and R. J. Schoelkopf. Controlling the spontaneous emission of a superconducting transmon qubit. *Physical Review Letters*, 101:080502, 2008.
- [15] Peter W. Shor. Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, 52(4):R2493, 1995.
- [16] Dorit Aharonov and Michael Ben-Or. Fault-tolerant quantum computation with constant error. In *Proceedings of the twenty-ninth Annual ACM Symposium on Theory of Computing*, pages 176–188, 1997.

- [17] A. Yu. Kitaev. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52(6):1191, 1997.
- [18] Panos Aliferis, Daniel Gottesman, and John Preskill. Quantum accuracy threshold for concatenated distance-3 codes. *arXiv preprint quant-ph/0504218*, 2005.
- [19] Alexei Kitaev. Fault-tolerant quantum computation by anyons. *arXiv preprint quant-ph/9707021*, 1997.
- [20] Sergey B. Bravyi and A. Yu. Kitaev. Quantum codes on a lattice with boundary. *arXiv preprint quant-ph/9811052*, 1998.
- [21] Eric Dennis, Alexei Kitaev, Andrew Landahl, and John Preskill. Topological quantum memory. *Journal of Mathematical Physics*, 43(9):4452–4505, 2002.
- [22] Austin G. Fowler, Ashley M. Stephens, and Peter Groszkowski. High-threshold universal quantum computation on the surface code. *Physical Review A*, 80(5):052312, 2009.
- [23] Maika Takita, Antonio D. Córcoles, Easwar Magesan, Baleegh Abdo, Markus Brink, Andrew Cross, Jerry M. Chow, and Jay M. Gambetta. Demonstration of weight-four parity measurements in the surface code architecture. *Physical Review Letters*, 117(21):210505, 2016.
- [24] J. F. Marques, B. M. Varbanov, M. S. Moreira, Hany Ali, Nandini Muthusubramanian, Christos Zachariadis, Francesco Battistel, Marc Beekman, Nadia Haider, Wouter Vlothuizen, et al. Logical-qubit operations in an error-detecting surface code. *Nature Physics*, 18(1):80–86, 2022.
- [25] Sebastian Krinner, Nathan Lacroix, Ants Remm, Agustin Di Paolo, Elie Genois, Catherine Leroux, Christoph Hellings, Stefania Lazar, Francois Swiadek, Johannes Herrmann, et al. Realizing repeated quantum error correction in a distance-three surface code. *Nature*, 605(7911):669–674, 2022.
- [26] Youwei Zhao, Yangsen Ye, He-Liang Huang, Yiming Zhang, Dachao Wu, Huijie Guan, Qingling Zhu, Zuolin Wei, Tan He, Sirui Cao, et al. Realization of an error-correcting surface code with superconducting qubits. *Physical Review Letters*, 129(3):030501, 2022.
- [27] Google Quantum AI. Suppressing quantum errors by scaling a surface code logical qubit. *Nature*, 614(7949):676–681, 2023.
- [28] Daniel Gottesman. Fault-tolerant quantum computation with constant overhead. *arXiv preprint arXiv:1310.2984*, 2013.
- [29] Maxime A. Tremblay, Nicolas Delfosse, and Michael E. Beverland. Constant-overhead quantum error correction with thin planar connectivity. *Physical Review Letters*, 129(5):050504, 2022.
- [30] Nikolas P. Breuckmann and Barbara M. Terhal. Constructions and noise threshold of hyperbolic surface codes. *IEEE Transactions on Information Theory*, 62(6):3731–3744, 2016.
- [31] Jean-Pierre Tillich and Gilles Zémor. Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength. *IEEE Transactions on Information Theory*, 60(2):1193–1202, 2013.
- [32] Nikolas P. Breuckmann and Jens N. Eberhardt. Balanced product quantum codes. *IEEE Transactions on Information Theory*, 67(10):6653–6674, 2021.
- [33] Alexey A. Kovalev and Leonid P. Pryadko. Quantum kronecker sum-product low-density parity-check codes with finite rate. *Physical Review A*, 88(1):012311, 2013.

- [34] Pavel Panteleev and Gleb Kalachev. Degenerate quantum LDPC codes with good finite length performance. *Quantum*, 5:585, 2021.
- [35] Hsiang-Ku Lin and Leonid P. Pryadko. Quantum two-block group algebra codes. *arXiv preprint arXiv:2306.16400*, 2023.
- [36] Renyu Wang, Hsiang-Ku Lin, and Leonid P. Pryadko. Abelian and non-Abelian quantum two-block codes. *arXiv preprint arXiv:2305.06890*, 2023.
- [37] Pavel Panteleev and Gleb Kalachev. Asymptotically good quantum and locally testable classical LDPC codes. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, pages 375–388, 2022.
- [38] Anthony Leverrier and Gilles Zémor. Quantum Tanner codes. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 872–883. IEEE, 2022.
- [39] Nouédy Baspin and Anirudh Krishna. Quantifying nonlocality: How outperforming local quantum codes is expensive. *Physical Review Letters*, 129(5):050505, 2022.
- [40] Sergey Bravyi, David Poulin, and Barbara Terhal. Tradeoffs for reliable quantum information storage in 2D systems. *Physical Review Letters*, 104(5):050503, 2010.
- [41] Petra Mutzel, Thomas Odenthal, and Mark Scharbrodt. The thickness of graphs: a survey. *Graphs and combinatorics*, 14:59–73, 1998.
- [42] Andrew Steane. Multiple-particle interference and quantum error correction. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 452(1954):2551–2577, 1996.
- [43] A. Robert Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098, 1996.
- [44] Joschka Roffe, David R. White, Simon Burton, and Earl Campbell. Decoding across the quantum low-density parity-check code landscape. *Physical Review Research*, 2(4):043423, 2020.
- [45] Peter Groszkowski, Austin Fowler, and Ashley M. Stephens. High-threshold surface code quantum computing: threshold calculation. In *APS March Meeting Abstracts*, pages W17–002, 2009.
- [46] Lawrence Z. Cohen, Isaac H. Kim, Stephen D. Bartlett, and Benjamin J. Brown. Low-overhead fault-tolerant quantum computing using long-range connectivity. *Science Advances*, 8(20), may 2022.
- [47] Sergey Bravyi, Oliver Dial, Jay M. Gambetta, Darío Gil, and Zaira Nazario. The future of quantum computing with superconducting qubits. *Journal of Applied Physics*, 132(16), 2022.
- [48] Andrew J. Landahl, Jonas T. Anderson, and Patrick R. Rice. Fault-tolerant quantum computing with color codes. *arXiv preprint arXiv:1108.5738*, 2011.
- [49] Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Physical Review A*, 70(5):052328, 2004.
- [50] Austin G. Fowler, Adam C. Whiteside, Angus L. McInnes, and Alimohammad Rabbani. Topological code auto-tune. *Physical Review X*, 2(4):041003, 2012.
- [51] Oscar Higgott and Craig Gidney. Sparse blossom: correcting a million errors per core second with minimum-weight matching. *arXiv preprint arXiv:2303.15933*, 2023.

- [52] Elwyn Berlekamp, Robert McEliece, and Henk Van Tilborg. On the inherent intractability of certain coding problems (corresp.). *IEEE Transactions on Information Theory*, 24(3):384–386, 1978.
- [53] Joschka Roffe. LDPC: Python tools for low density parity check codes, 2022.
- [54] Sergey Bravyi and Alexander Vargo. Simulation of rare events in quantum error correction. *Physical Review A*, 88(6):062308, 2013.
- [55] Nikolas P. Breuckmann and Simon Burton. Fold-transversal Clifford gates for quantum codes, 2022.
- [56] Christopher A. Pattison, Anirudh Krishna, and John Preskill. Hierarchical memories: Simulating quantum LDPC codes with local gates. *arXiv preprint arXiv:2303.04798*, 2023.
- [57] Jerry Chow, Oliver Dial, and Jay Gambetta. IBM Quantum breaks the 100-qubit processor barrier, 2021.
- [58] Paul Nation, Hanhee Paik, Andrew Cross, and Zaira Nazario. The IBM Quantum heavy hex lattice, 2021.
- [59] Jared B. Hertzberg, Eric J. Zhang, Sami Rosenblatt, Easwar Magesan, John A. Smolin, Jeng-Bang Yau, Vivekananda P. Adiga, Martin Sandberg, Markus Brink, Jerry M. Chow, and Jason S. Orcutt. Laser-annealing josephson junctions for yielding scaled-up superconducting quantum processors. *npj Quantum Information*, 7:129, 2021.
- [60] David C. McKay, Stefan Filipp, Antonio Mezzacapo, Easwar Magesan, Jerry M. Chow, and Jay M. Gambetta. Universal gate for fixed-frequency qubits via a tunable bus. *Physical Review Applied*, 6:064007, Dec 2016.
- [61] J. Stehlik, D. M. Zajac, D. L. Underwood, T. Phung, J. Blair, S. Carnevale, D. Klaus, G. A. Keefe, A. Carniol, M. Kumph, Matthias Steffen, and O. E. Dial. Tunable coupling architecture for fixed-frequency transmon superconducting qubits. *Physical Review Letters*, 127:080505, Aug 2021.
- [62] F. Arute, K. Arya, R. Babbush, and et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574:505–510, 2019.
- [63] David C. McKay, Ravi Naik, Philip Reinhold, Lev S. Bishop, and David I. Schuster. High-contrast qubit interactions using multimode cavity qed. *Physical Review Letters*, 114:080501, 2015.
- [64] Alexander Ivrii. Private communication, 2023.

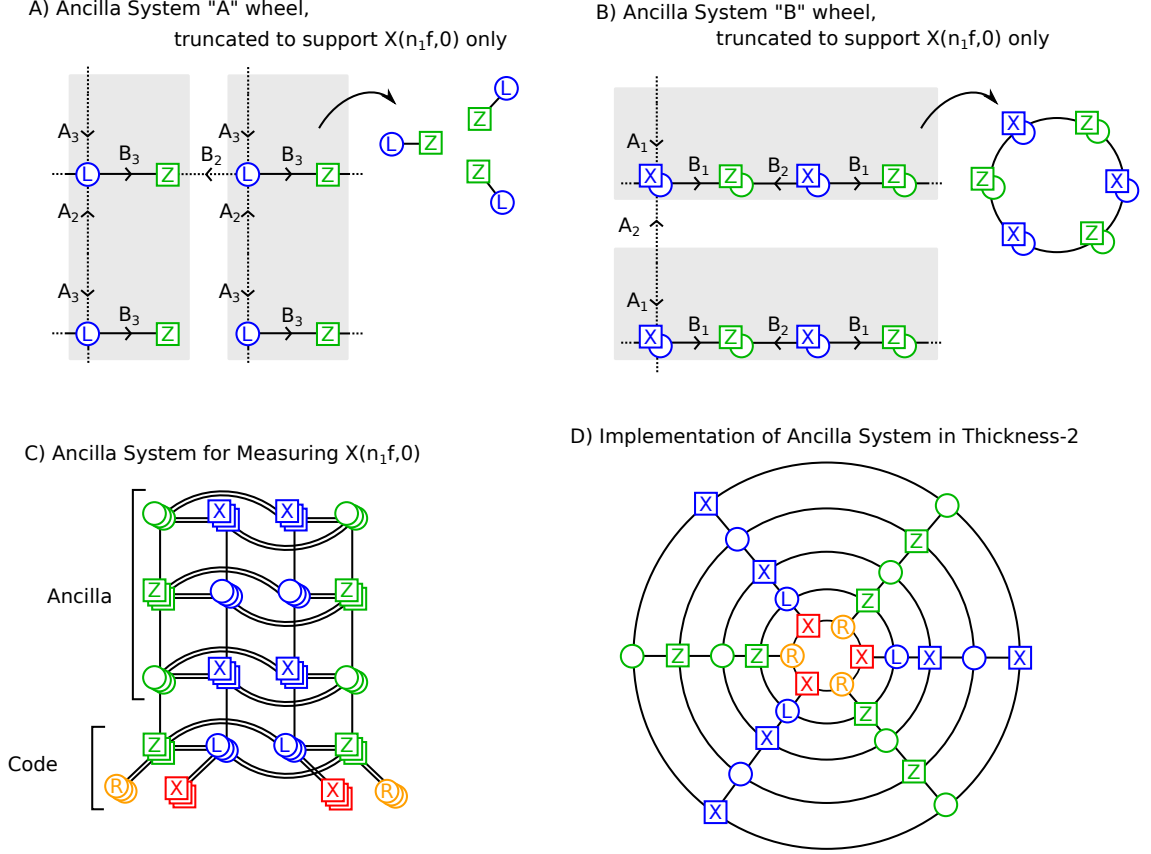


Figure 10: Visual proof of the thickness-2 property of the Tanner graph of quasi-cyclic LDPC codes. A) B) Planar embedding of each layer of the ancilla system from C) via truncating the 'A' and 'B' wheels. C) Conceptual representation of the Tanner graph extension for measuring one logical operator, described in Figure 2 of [46]. D) Implementation of the graph from C) via an effectively planar extension of the 'B' wheels of the original code.