Boulder Summer School 2023
“From topological to quantum LDPC codes”

Aleksander Kubica[1, 2]

[1]*AWS Center for Quantum Computing, Pasadena, CA, USA*
[2]*California Institute of Technology, Pasadena, CA, USA*
(Dated: July 17, 2023)

Plan for the lectures

1. Emphasis on quantum error correction. Split into three parts.
   (i) Topological codes: toric code, decoding problem.
   (ii) Limitations on topological codes: logical gates, code parameters.
   (iii) LDPC codes: classical and quantum code constructions, single-shot QEC.

Useful references

1. “Topological quantum memory” by Dennis et al., J. Math. Phys. 43, 4452-4505 (2002), `https://arxiv.org/abs/quant-ph/0110143`
2. “Topological codes” by Bombín, in “Quantum Error Correction”, edited by Lidar and Brun, Cambridge University Press (2013), `https://arxiv.org/abs/1311.0277`
3. “Classification of topologically protected gates for local stabilizer codes” by Bravyi and König, Phys. Rev. Lett. 110, 170503 (2013), `https://arxiv.org/abs/1206.1609`
4. “A no-go theorem for a two-dimensional self-correcting quantum memory based on stabilizer codes” by Bravyi and Terhal, New J. Phys. 11, 043029 (2009), `https://arxiv.org/abs/0810.1983`
5. “Quantum Low-Density Parity-Check Codes” by Breuckmann and Eberhardt, PRX Quantum 2, 040101 (2021), `https://arxiv.org/abs/2103.06309`
6. “Single-shot quantum error correction with the three-dimensional subsystem toric code” by Kubica and Vasmer, Nat. Commun. 13, 6272 (2022), `https://arxiv.org/abs/2106.02621`

Stabilizer codes

1. Hilbert space $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$ associated with n qubits. Quantum code is a subspace of $\mathcal{H}$.
2. Stabilizer code $\mathcal{C}$ is a subspace of $\mathcal{H}$ defined by the stabilizer group $\mathcal{S}$, which is an Abelian subgroup of n-qubit Pauli group $\mathcal{P}(n)$ which does not contain $-I$
$$\mathcal{C} = \{|\psi\rangle | \forall S \in \mathcal{S} : S|\psi\rangle = |\psi\rangle\} \tag{1}$$
3. The number of logical qubits k is given by $2^k = \dim \mathcal{C} = 2^{n-r}$, where r is the number of independent generators of the stabilizer group $\mathcal{S}$.
4. CSS stabilizer code $\mathcal{S} = \langle \mathcal{S}_X, \mathcal{S}_Z \rangle$. They can be constructed from classical codes specified by two parity check matrices H_X and H_Z satisfying $H_X H_Z^T = 0$. Note that a (binary linear) classical code C is defined as a subspace spanned by (binary) vectors that are in the kernel of the (binary) parity check matrix H, i.e., $C = \ker H$.
5. $\mathcal{N}(\mathcal{S})$ is defined as the group of all n-qubit Pauli operators that commute with all stabilizer operators
$$\mathcal{N}(\mathcal{S}) = \{L \in \mathcal{P}(n) | \forall S \in \mathcal{S} : LS = SL\}. \tag{2}$$
   Pauli logical operators correspond to different cosets $\mathcal{N}(\mathcal{S})/\mathcal{S}$, representatives of a logical Pauli operator correspond to different elements in the coset.

6. Code distance d is the weight of the minimum-weight nontrivial logical operator

$$d = \min_{L \in \mathcal{N}(\mathcal{S}) \setminus \mathcal{S}} |L|. \tag{3}$$

By definition, code with distance d allows to detect any Pauli error of weight at most $d-1$ and to correct any Pauli error of weight at most $\lfloor (d-1)/2 \rfloor$.

Toric code

1. Toric code on the $L \times L$ square lattice with periodic boundary conditions. Stabilizer operators associated with faces F and vertices V of the lattice. Check that they commute.
2. Parameters of the square lattice $V = L^2$, $E = 2L^2$ and $F = L^2$. The number of qubits $n = E$ and the number of independent stabilizer generators $r_X = V - 1$, $r_Z = F - 1$.
3. Number of logical qubits $k = n - r_X - r_Z = E - V - F + 2 = 2g$, where we use Euler's characteristic $V - E + F = 2(1-g)$ for genus g manifold. Note that $g = 0$ for a sphere and $g = 1$ for a torus.
4. Note that k does not depend on L or the details of the tessellation, but depends on the topology of the manifold.
5. One can consider $\mathbb{R}^2$, $\mathbb{RP}^2$, hyperbolic spaces—the number of qubits may depend on the ambient space.
6. Pauli logical operators form non-contractible strings. They can be deformed. For every hole of the manifold, there is a pair of logical qubits—in agreement with the formula $k = 2g$.
7. Consider the following state

$$|\overline{++}\rangle \propto \sum_{S \in \mathcal{S}_Z} S|+\rangle^{\otimes n}, \tag{4}$$

which is as a superposition of all contractible loops. Check that it is indeed a codeword of the toric code, as it is an eigenvectors of all stabilizer generators.

8. Other logical states can be obtained by applying logical Pauli Z operators, e.g., $|\overline{-+}\rangle = \overline{Z_1}|\overline{++}\rangle$. Interpretation: a non-contractible loop is inserted.

Toric code on a lattice with a boundary

1. Realization of the toric code on a torus may be difficult.
2. The $L \times L$ quare lattice with open boundary conditions: example for $L = 3$ has $n = 13$ qubits, six X-type stabilizers and six Z-type stabilizers and $k = 1$ logical qubit. Logical operators connect opposite boundaries (also referred to as rough and smooth boundaries).
3. Often, people refer to it as the surface code. A more qubit-efficient realization is referred to as the rotated surface code. The naming is quite unfortunate.

Topological quantum codes

1. Defining features of topological/geometrically-local quantum codes
   (i) qubits placed on a manifold (possibly with boundary),
   (ii) finite density of qubits,
   (iii) stabilizer generators are geometrically local, whereas logical operators non-local (growing distance).
2. Examples: toric code, color code, Haah's cubic code.
3. (i) and (ii) are not really a restriction, but rather a visualization/realization.
4. If (iii) is replaced by (iii) stabilizer generators have weight upper bounded by some constant and every qubit is in support of only a constant number of stabilizer generators, then we have quantum low-density parity-check (LDPC) codes.

Quantum error correction

1. Information encoded into a stabilizer code. Measure stabilizers to: (i) discretize errors, (ii) gain classical information for recovery. Errors can be diagnosed by measuring stabilizers, e.g.,

$$SP_i|\psi\rangle = \pm P_i S|\psi\rangle = \pm P_i|\psi\rangle, \tag{5}$$

   where P_i is a Pauli P error acting on qubit i and the sign depends on whether S and P commute or anticommute. Note that the corrupted state $P_i|\psi\rangle$ is still an eigenstate of S. The error syndrome comprises all the measurement outcomes that return -1.

2. We assume that we know noise model. Typically, we focus on the iid noise, where each qubit independently affected. Popular noise models:
   - bit-flip and phase-flip noise: Pauli X error with probability p_X, Pauli Z error with probability p_Z.
   - depolarizing noise: Pauli X, Y or Z error with probability $p/3$.

3. For CSS codes, we can split correction: Z-type stabilizers used for Pauli X errors.

4. Pauli noise is probabilistic and incoherent, but it can include correlations. It can be efficiently simulated (due to the Gottesman-Knill theorem, as error correction with stabilizer codes uses Clifford circuits).

5. Coherent noise, e.g., a small unitary rotation on every qubit, is difficult to simulate (typically requires time and memory exponential in the number of qubits). Also, there could be large differences between average-case and worst-case fidelities.

Decoding problem for the toric code

1. Interpretation of errors in the toric code: string-like operators that create point-like excitations at their ends. (Note that we can think of the toric code codespace as the ground space of the Hamiltonian that is the sum of all stabilizer generators, i.e., $H_{TC} = -\sum_v X_v - \sum_f Z_f$.)

2. Decoding problem: given the syndrome we want to find an error (and we do not need to find it exactly but rather up to some stabilizer). We are pairing up excitations (there is always an even number of them).

3. Useful to introduce some terminology. A chain complex

$$C_2 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0 \tag{6}$$

   which is a sequence of $\mathbb{F}_2$-linear vector spaces C_i and linear maps ∂_i between them. For C_i, the set of all i-cells is a basis. Vectors in C_i can be interpreted as subsets of i-cells. The linear map ∂_i is called a boundary operator. A composition of two consecutive boundary operators is zero, i.e., $\partial_1 \circ \partial_2 = 0$.

4. The toric code is defined by associating Z-type stabilizers with C_2, qubits with C_1 and the syndrome for Pauli Z errors with C_0. If boundary operators viewed as binary matrices, then $\partial_2 = H_Z^T$ and $\partial_1 = H_X$, where H_Z and H_X are parity check matrices that describe Z- and X-type stabilizer generators, respectively.

5. By definition, any stabilizer generator $\omega \in C_2$ has a trivial syndrome, i.e., $\partial_1(\partial_2\omega) = 0$.

6. $\ker \partial_1$ are cycles (Pauli Z logical operators) and $\operatorname{im} \partial_2$ are boundaries (Z-type stabilizers). Every boundary is a cycle, i.e., $\operatorname{im} \partial_2 \subseteq \ker \partial_1$. First homology group $H_1 = \ker \partial_1 / \operatorname{im} \partial_2$ is the equivalence classes of cycles (differing by boundaries).

7. Decoding problem rephrased: unknown Pauli Z error $\epsilon \in C_1$, we know its syndrome $\sigma = \partial_1 \epsilon$, we want to find $\phi \in C_1$ such that $\partial_1 \phi = \sigma$. We succeed if $\epsilon + \phi \in \operatorname{im} \partial_2$ (contractible loop) and fail if $\epsilon + \phi \in \ker \partial_1 \setminus \operatorname{im} \partial_2$ (non-contractible loop).

Solutions to the decoding problem

1. Minimum-Weight Perfect Matching (MWPM) algorithm finds the most likely error.

2. For iid noise with error probability p we have

$$\mathrm{pr}(\epsilon) = p^{|\epsilon|}(1-p)^{n-|\epsilon|} = (1-p)^n \left(\frac{p}{1-p}\right)^{|\epsilon|}. \tag{7}$$

The most likely error

$$\phi = \arg \max_{\epsilon:\partial_1 \epsilon = \sigma} \mathrm{pr}(\epsilon) = \arg\max \log \mathrm{pr}(\epsilon) = \arg\min |\epsilon| \tag{8}$$

corresponds to finding the pairing with the shortest total length.

3. The error rate does not have to be the same. If p_i is the error rate on qubit on the edge i of the square lattice, then we need to properly weigh it, i.e., $w_i = \log \frac{1-p_i}{p_i}$.

4. Renormalization group algorithm tries to remove excitations by lumping them together. Two strategies: hard decisions vs. soft decisions. The performance may differ.

5. Neural network decoder: we can phrase the decoding problem as a classification problem (where logical Pauli operators are the labels). We use a naive decoder to get back to the code space, and then apply an appropriate logical Pauli operator to finish the recovery.

Thresholds

1. We expect to get better performance if the error rate goes down. But how about scaling up the code?

2. Needed: a family of codes of growing distance d (e.g., the toric code), decoding algorithm (e.g., the MWPM algorithm), noise model (e.g, iid noise with error rate p).

3. Threshold theorem: there exists $p^* > 0$, such that for any $p < p^*$, the probability of successful correction goes to one as d goes to infinity.

4. Having a nonzero threshold is a nontrivial property. For instance, with the toric code we can successfully correct, on average, $np \propto d^2 p$ errors, but from the code distance d we are guaranteed to correct only at most $\lfloor (d-1)/2 \rfloor$ errors.

5. One can prove lower bounds on the threshold. For instance, for the toric code on the square lattice, the MWPM algorithm and the phase-flip noise, we have $p_{\mathrm{th}} > .0373$.

6. Analytical bounds can be orders of magnitude smaller than the actual thresholds. Thus, we often resort to numerical estimates of thresholds.

7. How to find the threshold numerically? Data collapse with a rescaled variable $x = (p - p_{\mathrm{th}})d^{\alpha}$ and fitting to a quadratic approximation of the scaling function.

Erasure noise

1. Erasure noise: with some probability e the state is replaced by some fixed state $|\perp\rangle$ that is orthogonal to the qubit subspace. We know when this happens.

2. We can think about replacing the state with the maximally mixed state, i.e.,

$$\rho \mapsto \mathbf{1} = \frac{1}{4} \sum_P P \rho P^{\dagger}. \tag{9}$$

Thus, we can treat an erasure as the bit-flip noise with error rate $p = 0.5$ and the phase-flip noise with error rate $p = 0.5$ applied at the known location.

3. Decoding algorithm: (i) find connected components of erased qubits, (ii) for each connected component, choose one vertex and move all excitations to that vertex.

4. For erasure noise, the QEC threshold for the toric code can be related to the bond percolation threshold. For the square lattice we have $p_{\mathrm{th}} = 0.5$.

5. We can consider noise comprising Pauli errors with probability p and erasures with probability e. We can use the MWPM decoder to correct this noise if we choose the edge weights appropriately. We obtain the correctable region in the (e, p) phase space.

6. This is the basic idea behind erasure qubits, which recently has gained a lot of interest (culminating in a few experimental demonstrations).

Optimal decoding

1. Assume iid noise with error rate p. Given the syndrome σ, we are not interested in any particular error ϵ (not even the most likely one) consistent with the syndrome, i.e., $\partial_1 \epsilon = \sigma$, but rather the most likely equivalent class

$$\mathrm{pr}(\overline{\epsilon}) = \sum_{\omega \in C_2} \mathrm{pr}(\epsilon + \partial_2 \omega) = (1-p)^n \left(\frac{p}{1-p}\right)^{|\epsilon + \partial_2 \omega|}. \tag{10}$$

2. Maximum-likelihood decoding: given σ, find any ϵ satisfying $\partial_1 \epsilon = \sigma$, pick the most likely equivalence class among $\mathrm{pr}(\overline{\epsilon})$, $\mathrm{pr}(\overline{\epsilon + \lambda_{01}})$, $\mathrm{pr}(\overline{\epsilon + \lambda_{10}})$ and $\mathrm{pr}(\overline{\epsilon + \lambda_{01} + \lambda_{10}})$. Correction $\phi = \epsilon + \arg\max_{\lambda \in H_1} \mathrm{pr}(\overline{\epsilon + \lambda})$.

3. Intuition: $\mathrm{pr}(\text{success}) \to 1$ if with high probability $\mathrm{pr}(\overline{\epsilon}) > \mathrm{pr}(\overline{\epsilon + \lambda})$ for any $0 \neq \lambda \in H_1$.

4. There is a challenge in evaluating $\mathrm{pr}(\overline{\epsilon})$, as the number of terms is $|C_2| = 2^{L^2}$. However, it can be efficiently evaluated, either exactly (the bit-flip noise) or approximately (the depolarizing noise), by contracting a two-dimensional tensor network.

Statistical-mechanical connection

1. Classical spin model on the square lattice with spins on faces and (anti)ferromagnetic interactions between neighboring spins

$$H_\epsilon(\{s_i\}) = -\sum_{\langle i,j \rangle} \kappa_{i,j} s_i s_j, \tag{11}$$

where $\epsilon \in C_1$ and $\kappa_{i,j} = -1$ iff the edge between s_i and s_j is in ϵ, otherwise $\kappa_{i,j} = 1$. Two parameters: temperature T and disorder rate p.

2. Consider some configuration of spins $\{s_i\}$ and let $\omega \in C_2$ correspond to -1 spins. Then we have

$$H_\epsilon(\{s_i\}) = H_{\epsilon + \partial_2 \omega}(\{s_i = +1\}) = -|E| + 2|\epsilon + \partial_2 \omega|. \tag{12}$$

and the partition function

$$Z_\epsilon = \sum_{\{s_i\}} e^{-\beta H_\epsilon(\{s_i\})} = \sum_{\omega \in C_2} e^{\beta(|E| - 2|\epsilon + \partial_2 \omega|)} = e^{\beta |E|} \sum_{\omega \in C_2} (e^{-2\beta})^{|\epsilon + \partial_2 \omega|}. \tag{13}$$

3. Note that $\mathrm{pr}(\overline{\epsilon}) \propto Z_\epsilon$ if $e^{-2\beta} = p/(1-p)$ (which is known as the Nishimori condition).

4. Rather than considering individual systems described by H_ϵ, the random-bond Ising model is a statistical-mechanical model obtained by making the parameter ϵ a quenched random variable (which is not subject to thermal fluctuations). The (p, T) plane of the random-bond Ising model consists of an ordered region for low p and T, and a disordered one.

5. An order parameter: free energy cost of inserting a domain wall $\lambda \in H_1$ defined as

$$\Delta_\lambda(\epsilon) = -\beta \log Z_{\epsilon + \lambda} + \beta \log Z_\epsilon = \beta \log \frac{Z_\epsilon}{Z_{\epsilon + \lambda}} \tag{14}$$

In the ordered phase $\Delta_\lambda(\epsilon)$ diverges with high probability, whereas in the ordered phase $\Delta_\lambda(\epsilon)$ is finite with high probability.

6. A connection with maximum-likelihood decoding can be made rigorous. For other noise models, e.g., the depolarizing noise, we get different disordered models. This gives a useful tool to numerically benchmark the fundamental limitation on the performance (measured in terms of a QEC threshold) of QEC codes by using stat-mech methods.

Gates and Clifford hierarchy

1. So far we discussed QEC but we would like to implement gates. Useful for later discussion to introduce the notion of a group commutator $K(A,B) = ABA^\dagger B^\dagger$. Examples: $K(Z,X) = -I$, $K(S,X) = -iZ$, $K(R(\phi),X) = e^{i\phi}R(2\phi)$, where $R(\phi) = \mathrm{diag}(1, \exp(i\phi))$.
2. Clifford hierarchy defined recursively

$$\mathcal{C}_1 = n\text{-qubit Pauli group } \mathcal{P}(n) \tag{15}$$

$$\mathcal{C}_{l+1} = \{n\text{-qubit unitary operators } U | \forall P \in \mathcal{P}(n) : K(U,P) \in \mathcal{C}_l\} \tag{16}$$

The second level corresponds to the Clifford group that is generated by the Hadamard gate H, the CX gate (the CNOT gate), and the $S = R(\pi/2)$ gate. The third level is a set (not a group) and includes the $T = R(\pi/4)$ gate. The l-level includes the $R(\pi/2^{l-1})$ gate and the l-qubit controlled-Z gate $C^{l-1}Z$.
3. Universal gate set, e.g., $\{H, T, CX\}$. The Solovay-Kitaev theorem guarantees that any unitary U can be approximated up to operator norm error δ using a number of gates from the universal gate set that scales as $O(\log^c(1/\delta))$ for some constant c.
4. We want to implement logical gates on the encoded information while maintaining the protection given by the QEC code. A particularly appealing way of realizing logical gates is via transversal gates (or, more generally, constant-depth circuits), as they do not spread errors in an uncontrollable way.

Limitations on logical gates and code parameters of topological codes

1. The Eastin-Knill theorem rules out the existence of a QEC code with a universal set of transversal gates. There are analogous theorems for approximate QEC codes.
2. For any topological stabilizer code on a lattice in $D \geq 2$ dimensions, the Bravyi-König theorem limits logical gates implemented with constant-depth quantum circuits to the Dth level of the (logical) Clifford hierarchy. In particular, it is not possible to have any transversal non-Clifford gate in 2D.
3. Proof for the 2D toric code is intuitive and can be generalized to quantum circuits comprising geometrically non-local gates—the resulting bound relies on the code quantity called disjointness.
4. For a QEC code that corresponds to the common eigenspace of geometrically-local commuting projectors on a lattice in $D \geq 2$ dimensions, the Bravyi-Poulin-Terhal theorem restricts the QEC code parameters $[\![n,k,d]\!]$, namely

$$kd^{2/(D-1)} \leq O(n). \tag{17}$$

In particular, in 2D imposing the rate k/n to be constant implies that code distance $d = O(1)$.
5. The aforementioned limitations motivate the study of topological codes in $D \geq 3$ dimensions and quantum low-density parity-check (LDPC) codes. In particular, with 3D topological codes we can have transversal non-Clifford gates and there exist quantum LDPC codes with good parameters (for which both the number of logical qubits k and code distance d scale linearly in the number of physical qubits n).

Classical and quantum codes

1. Classical ($\mathbb{F}_2$-linear) code C is defined as the linear subspace spanned by binary vectors that are in the kernel of a binary matrix H, commonly referred to as a parity-check matrix, i.e., $C = \ker H$. We can visualize C via a Tanner graph.
2. Parameters of a classical code.

3. Given a classical code C, we can consider the following chain complex

$$C_1 \xrightarrow{H} C_0, \tag{18}$$

where C_1 and C_0 correspond to, respectively, bits and parity checks. If e is the subset of bits affected by bit-flip errors, then the corresponding error syndrome is $s = He$.

4. CSS construction combines two classical codes with parity check matrices H and H' satisfying $H(H')^T = 0$ in order to obtain a quantum code with the following chain complex

$$C_2 \xrightarrow{(H')^T} C_1 \xrightarrow{H} C_0, \tag{19}$$

where C_2, C_1 and C_0 correspond to, respectively, Z parity checks, qubits and X parity checks. H and H' denote the support of X and Z parity checks, and the condition $H(H')^T = 0$ guarantees that parity checks commute.

5. Parameters of a quantum code.

6. Good QEC codes exist, i.e, k and d scale linearly in n, however no guarantee on small weight of parity checks (which is equivalent to H and H' being sparse matrices).

Quantum LDPC codes

1. We are interested in quantum LDPC codes, which, by definition, have parity checks of constant weight. The requirement on parity checks is motivated from the perspective of fault tolerance.

2. Hypergraph/tensor/homological product codes are at the heart of recent progress in quantum LDPC codes. By taking a tensor product of a chain complex $A \xrightarrow{H} B$ (associated with a classical code) with itself, i.e.,

$$\begin{array}{ccc} A \otimes A & \xrightarrow{I \otimes H} & A \otimes B \\ \big\downarrow{\scriptstyle H \otimes I} & & \big\downarrow{\scriptstyle H \otimes I} \\ B \otimes A & \xrightarrow{I \otimes H} & B \otimes B \end{array}, \tag{20}$$

we can construct a quantum code associated with the following chain complex

$$A \otimes A \xrightarrow{\partial_2 = \begin{pmatrix} I \otimes H \\ H \otimes I \end{pmatrix}} A \otimes B \oplus B \otimes A \xrightarrow{\partial_1 = (H \otimes I, I \otimes H)} B \otimes B. \tag{21}$$

If we use a good classical LDPC code, then this construction results in a quantum LDPC code with parameters $k \sim n$ and $d \sim \sqrt{n}$.

3. Example how the toric code can be obtained from two classical repetition codes.

4. Recent constructions of quantum LDPC codes include: (i) quantum expander codes, (ii) fiber bundle codes, (iii) lifted product codes, (iv) balanced product codes, and (v) quantum Tanner codes. Importantly, constructions (iii)-(v) give rise to good quantum LDPC codes.

5. Connection with quantum many-body physics: the NLTS conjecture about the complexity of low-energy states of local commuting Hamiltonians.

Single-shot QEC

1. QEC itself is a noisy process. Typically, we need to repeat measurements in order to gain sufficient confidence in their outcomes to perform QEC.

2. In the presence of measurement errors, in order to implement reliable QEC with the toric code in 2D we either suffer from time overhead (which typically scales as code distance) or sacrifice geometric locality and constant weight of parity checks that we have to measure.

3. Alternative solution in the form of single-shot QEC. Reliable QEC possible in constant time.

4. The 3D subsystem toric code is the quintessential model illustrating single-shot QEC.

5. Good quantum LDPC codes, such as quantum Tanner codes, can also facilitate single-shot QEC.