MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Department of Physics, EECS, and Department of Applied Math

MIT 6.443J / 8.371J / 18.409 / MAS.865

Quantum Information Science

March 18, 2008

Problem Set #3 Solutions

Problems:

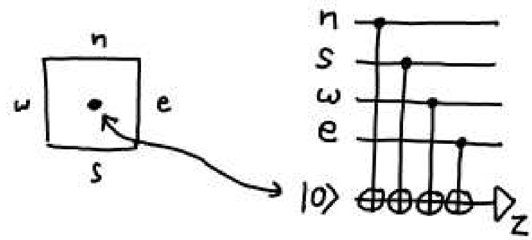
P1: (**Toric code**) **(a)** The Hilbert space decomposes into joint eigenspaces of $S = \langle A_p, B_s \rangle$ labeled by the eigenvalues of $2\ell^2 - 2$ independent generators. Hence, each eigenspace is 4-dimensional. Each of these eigenspaces is also an eigenspace of the Hamiltonian H with energy $-2\ell^2 + 2N$ where N is the number of pairs of site or plaquette operators with -1 eigenvalues. The lowest energy state is achieved when N is zero, so the joint $+1$ eigenspace, i.e. the code space, corresponds to the ground state manifold.

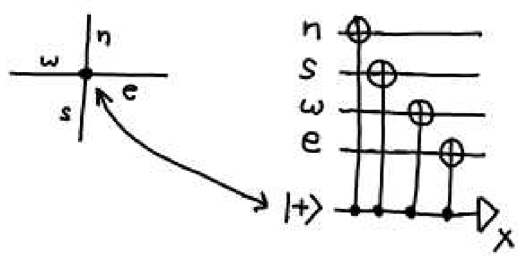
(b) A pair of charges is the boundary of a connected chain of Z errors and a pair of vortices is the boundary of a connected chain of X errors. If one half of such a pair tunnels around a nontrivial cycle before fusing with the other half of the pair, an element of $N(S) - S$ is applied since the resulting chain has no boundary and cannot be deformed to a point. This element is a nontrivial rotation of the code space, so it is a nontrivial rotation in the ground state manifold. A charge tranversing the nontrivial cycle around the hole corresponds to $\bar{Z}_1$ while a flux traversing the nontrivial cycle through the hole corresponds to $\bar{X}_1$, and $\bar{Z}_1 \bar{X}_1 \bar{Z}_1 \bar{X}_1 = -1$.

(c) The perturbation $V = \sum_e C_e$ is a sum of single qubit operators. Suppose that P projects from the unperturbed states to the perturbed states at the kth order of perturbation theory, so the kth order shifts of the ground states are the eigenvalues of the matrix HP evalulated in the ground state manifold*. The first order shift has $P = P_0$ and is simply $\langle \psi | V | \psi \rangle$ for an unperturbed ground state $|\psi\rangle$. The correction is zero since ground states can only be connected by operators of weight ℓ and higher. This is the main point. At order $k \geq 2$, each shift is a sum of terms proportional to $\langle \psi_i | (SV)^k S | \psi_j \rangle$ where each S is replaced by either $-P_0$ or $Q_0 = I - P_0$ and $\{|\psi_i\rangle\}$ is a basis for the ground state. Again, the shifts are zero and the splitting is zero as well since V^k can be written as a sum of Pauli operators of weight k or less. The degeneracy is not reduced until the ℓth order, when these terms begin to have nonzero contributions to the energy.

(d) The circuit shown below measures the site and plaquette operators using only nearest-neighbor interactions. The CNOT gates can be staggered so that the measurements can be done in parallel. There is an excellent paper by Dennis, Kitaev, Landahl, and Preskill entitled "Topological quantum memory" that explains why these circuits are fault-tolerant if ℓ is large enough, so that a quantum state can be stored by repeatedly measuring the syndrome and keeping track of the most likely chains of errors.

*Messiah, Quantum Mechanics, Ch. 16





P2: (**Accuracy threshold for quantum error-correction**) **(a)** Contrary to the notation in the problem set, I will put bars over elements of the normalizer so they are not confused with single qubit Pauli operators X_i or Z_i acting on the ith qubit. Modulo $S = \langle g_1, g_2, g_3, g_4 \rangle$, $\bar{X}_5 = X_1 X_2 X_3$ and $\bar{Z}_5 = Z_1 Z_4 Z_7$ and these are the lowest weight representatives. Therefore, all single qubit errors can be corrected. The code is a CSS code, so it corrects X and Z errors independently, therefore all two qubit ZX-mixed errors can be corrected as well. The stabilizer does not have any weight two operators. Since we may neglect errors in the gauge group $G = \langle \bar{Z}_1, \ldots, \bar{Z}_4, \bar{X}_1, \ldots, \bar{X}_4, S \rangle$, all two qubit errors in G may be "corrected" because they only act on $\mathcal{H}_S$. Using the notation $Z_{(i,j)}$ for a Z in row i and column j, where the indices are modulo 3, the complete set of correctable two qubit errors is $\{Z_{(i,j)} Z_{(i,j+1)}, X_{(i,j)} X_{(i+1,j)}\}$. Any two qubit errors that are not in the gauge group and are not of ZX-mixed type will not be properly corrected, by inspection. For example, $Z_1 Z_4$ has the same syndrome as Z_7.

(b) The stabilizer operators are products of operators in the gauge group. Consider the Z-type stabilizer operators since the procedure for the X-type stabilizer operators is analogous (but rotated by 90 degrees). We can find the following set of two qubit operators in the gauge group: $Z_1 Z_2 = \bar{Z}_1$, $Z_2 Z_3 = \bar{Z}_2$, $Z_1 Z_3 = \bar{Z}_1 \bar{Z}_2$, $Z_4 Z_5 = \bar{Z}_3$, $Z_5 Z_6 = \bar{Z}_4$, $Z_4 Z_6 = \bar{Z}_3 \bar{Z}_4$, $Z_7 Z_8 = g_3 \bar{Z}_1 \bar{Z}_3$, $Z_8 Z_9 = g_4 \bar{Z}_2 \bar{Z}_4$, and $Z_7 Z_9 = g_3 g_4 \bar{Z}_1 \bar{Z}_2 \bar{Z}_3 \bar{Z}_4$. The product of $Z_1 Z_2$, $Z_4 Z_5$, and $Z_7 Z_8$ is g_3 and the product of $Z_2 Z_3$, $Z_5 Z_6$, and $Z_8 Z_9$ is g_4. Therefore, we can correct X errors with the following procedure.

(i) Measure the 6 operators $Z_1 Z_2$, $Z_4 Z_5$, $Z_7 Z_8$, $Z_2 Z_3$, $Z_5 Z_6$, $Z_8 Z_9$ to obtain respective outcomes m_1, m_2, …, m_6 in $\{0, 1\}$ where 0 corresponds to $+1$ and 1 corresponds to -1.

(ii) Compute the syndromes $s_3 = m_1 \oplus m_2 \oplus m_3$ and $s_4 = m_4 \oplus m_5 \oplus m_6$ corresponding to generators g_3 and g_4.

(iii) There are four possible outcomes for the pair (s_3, s_4): $(0, 0)$ is the no error case, $(1, 0)$ indicates an X error in the first column, $(0, 1)$ indicates an X in the third column, and $(1, 1)$ indicates an X error in the second column.

(iv) If the syndrome is nontrivial, correct the top qubit of the indicated column j. If some other qubit in the ith row of column j was actually in error, the resulting operator $X_{(1,j)}X_{(i,j)}$ is in the gauge group and only acts nontrivally on $\mathcal{H}_S$.

(c) The measurement circuits are given in the following figures.

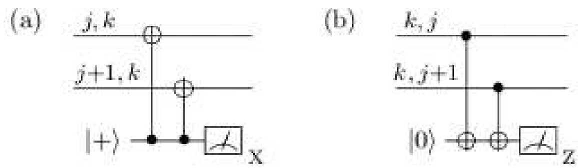
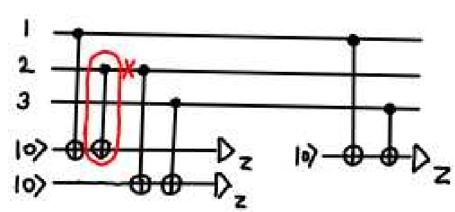


FIG. 2: (a) A circuit for measuring the operator $X_{j,k}X_{j+1,k}$ using one ancillary qubit. (b) A similar circuit for measuring $Z_{k,j}Z_{k,j+1}$. $|+\rangle \propto |0\rangle + |1\rangle$ is the $+1$ eigenstate of X.

When the input is in the code space, a necessary condition for fault-tolerance is that a single fault in the circuit does not lead to uncorrectable errors propagating to the data qubits. In these circuits, the worst cases occur when a CNOT gate fails, but all of these cases leave residual single qubit errors or residual two qubit errors in the gauge group or of ZX-mixed type. The ZX-mixed error occurs when the first CNOT of figure (a) fails and leaves an XZ on control and target respectively.

The measurement circuits from the figure can be composed in series to measure the syndrome of a Bacon-Shor code. We have already shown that single faults in these circuits cannot produce uncorrectable errors in the data. However, if two or more circuits are composed in series, a fault in an earlier circuit may produce an error E that modifies the measurement outcomes of the later circuits. If the measurement outcomes give a syndrome that decodes to the error $E' \neq E$, the product EE' of the actual error and the correction may not be correctable.

Consider the circuit to measure Z_1Z_2 and Z_2Z_3 on qubits 1, 2, and 3, shown below. A single fault at the marked location leads us to infer that the 3rd column is in error when actually the 2nd column contains the error. By inspection, this is the only case where our interpretation of the measurement outcomes is incorrect. Therefore, adding an additional measurement of Z_1Z_3 allows us to detect this case and interpret the measurement outcomes correctly.



The other circuits can be constructed analogously.

(d) The circuit to measure the gauge operators along a single row or column contains 12 possible fault locations, so a single EC contains $6 \times 12 = 72$ locations. A simple lower bound on the threshold for FTEC (for stochastic noise) is $\gamma_{th} \geq \binom{2\times 72}{2}^{-1}$ or 9.7×10^{-5}. In fact, 1.26×10^{-4} is a lower bound for the threshold for computation with this code.

P3: (**Codeword stabilized codes**) **(a)** First, any stabilizer state can be mapped by a Pauli operator to a new stabilizer state whose phases are all $+1$. Let $S = \langle g_i \rangle$ stabilize a state $|S\rangle$. There is a unitary U that maps the state $|00\ldots0\rangle$ to $|S\rangle$. Since these states are both binary stabilizer states, U may be chosen to be in the Clifford group. Therefore, $\bar{g}_i := UX_iU^\dagger$ is a Pauli operator that anticommutes with g_i and commutes with g_j for all $j \neq i$ (since the all zero state is stabilized by all products of Z). Hence, we may apply some product P of the $\bar{g}_i$ to $|S\rangle$ so that the resulting state $P|S\rangle$ is stabilized by $S' := \langle g_i' \rangle$ where $g_i' = \pm g_i$ and all g_i' have $+1$ phase.

Second, there is a map ϕ from the Pauli group G_n to binary strings of length $2n$ given by $\phi(I) = [0|0]$, $\phi(X) = [1|0]$, $\phi(Z) = [0|1]$, and $\phi(Y) = [1|1]$ and $\phi(P_1 \otimes P_2) = (\phi(P_1), \phi(P_2))$. For example $\phi(XZYI) = [1010|0110]$. The map is a homomorphism, meaning $\phi(P_1P_2) = \phi(P_1) + \phi(P_2)$, i.e. matrix multiplication becomes addition modulo 2. The phases of Pauli elements are dropped, so we can write $\phi(X^{\mathbf{a}}Z^{\mathbf{b}}) = [\mathbf{a}|\mathbf{b}]$ where "|" just separates the two halves of the binary string. $X^{\mathbf{a}}Z^{\mathbf{b}}$ and $X^{\mathbf{a}'}Z^{\mathbf{b}'}$ commute iff $(\mathbf{a}|\mathbf{b}) \odot (\mathbf{a}'|\mathbf{b}') := \mathbf{a}\mathbf{b}' + \mathbf{b}\mathbf{a}' = 0$. The single qubit Clifford gates are generated by

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \text{ and } S = \text{diag}(1, i). \tag{1}$$

Acting on coordinate $i \in \{1, 2, \ldots, n\}$ of $[\mathbf{a}|\mathbf{b}]$, Hadamard swaps a_i and b_i and Phase maps b_i to $a_i + b_i$.

These observations reduce the problem to a potentially simpler one. Show that any $n \times 2n$ matrix $[A|B]$ whose rows pairwise satisfy $(\mathbf{a}|\mathbf{b}) \odot (\mathbf{a}'|\mathbf{b}') = 0$ can be mapped to $[I|\Lambda]$, where Λ is an adjacency matrix, by the following operations:

(i) replacing row j by the sum of row j and another row j'

(ii) swapping column i and column $i + n$

(iii) adding column i to column $i + n$

Therefore, we can use Gauss-Jordan steps (i) to put A into the form

$$\begin{pmatrix} I & A' \\ 0 & A'' \end{pmatrix}, \tag{2}$$

then we use Gauss-Jordan steps (i) to put B into the form

$$\begin{pmatrix} B' & 0 \\ B'' & I \end{pmatrix}. \tag{3}$$

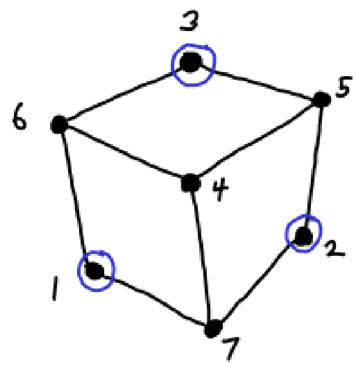
Now we use Hadamard gates (ii) to swap the right blocks of A and B to get

$$\left(\begin{array}{cc|cc} I & 0 & B' & A' \\ 0 & I & B'' & A'' \end{array} \right), \tag{4}$$

and, finally, we use Phase gates (iii) to clear the diagonal of B. The final form of B is an adjacency matrix because the rows of $[A|B]$ originally satisfied $(\mathbf{a}|\mathbf{b}) \odot (\mathbf{a}'|\mathbf{b}') = 0$, pairwise.

(b) The map $\text{classical}_G(E)$ takes any single qubit Pauli error to 10000_c, 11100_c, or 10100_c, where the subscript indicates that all cyclic shifts are included. All strings are nonzero, so the only condition to satisfy is that C detects these errors as a classical code, but this is obvious. By linearity, the code detects any single qubit error. On the other hand, the string 11010_c is produced by $ZIXII_c$, so the code is distance 2.

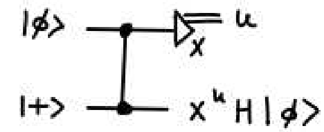
(c) Write the $[[7,1,3]]$ code as a CWS code with stabilizer $\langle S_{[[7,1,3]]}, \bar{X} = XXXXXXX\rangle$ and word operators $\{I, \bar{Z} = ZZZZZZZ\}$. Apply the procedure in part (a) to the stabilizer. The word operators transform by conjugation $UW|S\rangle = UWU^\dagger U|S\rangle$. The CWS standard form of the $[[7,1,3]]$ Steane code is

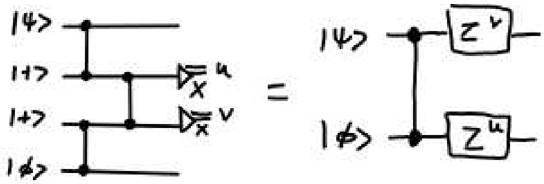


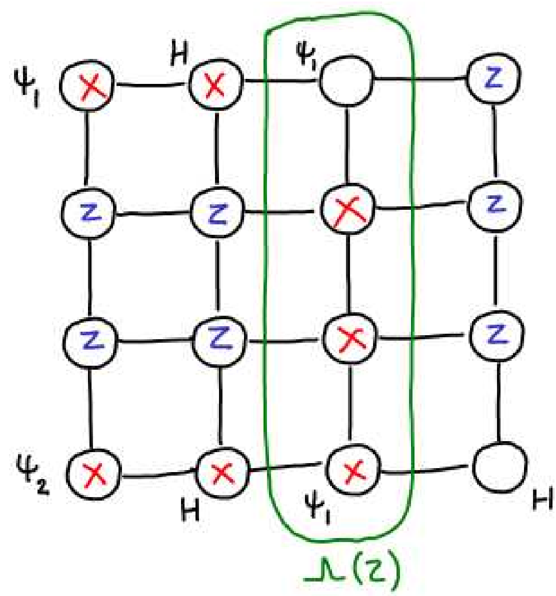
The circled vertices indicate where the $\bar{Z}$ word operator acts, so the classical code is $C = \{0000000, 1110000\}$. By inspection now, it is easy to see that the code has distance 3 since we cannot flip the bits at only the degree two vertices using one or two Pauli errors.

P4: (**Measurement-based computing with cluster states**) **(a)** By the convention in class, the input qubits are the left-most qubits that are measured in the X basis and the output qubits are the unmeasured qubits. The qubits measured in the Z basis are removed.

(b,c) This is a simple case where Pauli measurement bases do not depend on prior outcomes, so the circuit is a stabilizer circuit. Partition the cluster into regions and consider them separately. Suppose the top qubit begins in the state $|\psi_1\rangle$ and the bottom qubit in state $|\psi_2\rangle$. The first two columns teleport the inputs to positions $(1,3)$ and $(4,3)$ respectively.







The third column applies a controlled-Z gate between $|\psi_1\rangle$ and $|\psi_2\rangle$. Finally, the last row applies a Hadamard to the bottom qubit. The circuit is a controlled-Z gate followed by H_2. The initial cluster state preparation puts the inputs in $|+\rangle$, so the final state is a Bell pair $(|00\rangle + |11\rangle)/\sqrt{2}$.