Problem Set #5

CO 639: Quantum Error Correction
Instructor: Daniel Gottesman

Due Tues., Mar. 23

Problem 1. Fault-tolerance in higher dimensions

For d-dimensional qudits, recall that we can define an analogue of the Pauli group generated by X and Z, where $X|j\rangle = |j+1\rangle$ (modulo d) and $Z|j\rangle = \omega^j|j\rangle$ (where $\omega = e^{2\pi i/d}$). We can also define a d-dimensional Clifford group as operators which conjugate this generalized Pauli group into itself.

For this problem, only consider the case where $d \geq 3$ is prime.

a) For $d = 3$, consider the 3-qudit code with stabilizer generated by $X \otimes X \otimes X$ and $Z \otimes Z \otimes Z$. Of the following gates, which give transversal gates for this code? What logical gate do they perform? (You may choose any suitable operators for $\overline{X}$ and $\overline{Z}$.)

$$\begin{aligned} F : |j\rangle &\mapsto \sum_{k=0}^{d-1} \omega^{jk}|k\rangle && (1)\\ P : |j\rangle &\mapsto \omega^{j(j+1)/2}|j\rangle && (2)\\ S_c : |j\rangle &\mapsto |cj\rangle \quad (c \text{ a constant}) && (3)\\ \mathrm{SUM} : |j\rangle|k\rangle &\mapsto |j\rangle|j+k\rangle. && (4) \end{aligned}$$

(All arithmetic is modulo d.)

b) We can define a higher-dimensional analogue of a CSS code (at least for d prime) as a code whose stabilizer can be generated by operators that are either all powers of X (including $I = X^d$) or all powers of Z (again including $I = Z^d$). Of the same set of gates, which can be performed transversally on any higher-dimensional CSS code?

c) As with qubits, the qudit Clifford group (at least for d prime) corresponds to all automorphisms of the Pauli group. That is, for any two Pauli operations A and B, $AB = \omega^{\alpha(A,B)}BA$ for some power α of the dth root of unity. The Clifford group then performs any invertible mapping on the Pauli group preserving α, so $A \mapsto A'$, $B \mapsto B'$, with $\alpha(A,B) = \alpha(A',B')$. Can you find a minimal set of generators for the 1-qudit Pauli group?

Problem 2. Quantum MDS Codes

Let $p \geq 3$ be a prime and let $\alpha \in \mathrm{GF(p)} \setminus \{0\}$. For $1 \leq \mu \leq p-1$ let $C^{p,\mu}$ be the classical code defined by the generator matrix

$$G^{(p,\mu)} := \begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ \alpha^0 & \alpha^1 & \alpha^2 & \dots & \alpha^{p-2} & 0 \\ \alpha^0 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(p-2)} & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha^0 & \alpha^\mu & \alpha^{2\mu} & \dots & \alpha^{\mu(p-2)} & 0 \end{pmatrix}. \qquad (5)$$

Note that the rth row of this generator matrix can be considered to be the values of the polynomial x^{r-1} evaluated at the p points $1, \alpha, \alpha^2, \dots, \alpha^{p-2}, 0$ of the field GF(p). The code $C^{p,\mu}$ is therefore the set of all polynomials of degree μ evaluated at the p points of the field.

a) Show that $C^{p,\mu}$ can correct μ erasure errors and is thus a code with parameters $[p, \mu+1, p-\mu]_p$, meaning it is a classical MDS code (one that saturates the classical Singleton bound $n \geq k + d - 1$).

b) Show that the dual of $C^{p,\mu}$ is $C^{p,p-\mu-2}$.

c) Use two copies of this code $C^{p,\mu}$ to construct a QECC via the CSS construction. What are the parameters of the QECC? What is the allowed range of values of μ?

d) Recall that a (classical) code has distance d iff in its parity check matrix, all sets of $d-1$ columns are linearly independent (but some set of d is not). Use this fact to show that the dual of any classical MDS code (parameters $[n, k, n-k+1]$) is also an MDS code.

e) Show that given any MDS code, we can create a QECC using the CSS construction. Give the parameters of the QECC.

Problem 3. Threshold with Local Gates

In this problem, we will show that there still exists a threshold for fault-tolerant quantum computation even if we are only allowed to perform gates locally, say between nearest-neighbor gates when the qubits are arranged on a cubic lattice in two or more physical dimensions.

a) Suppose we can physically arrange all the ancillas required to perform a single level of quantum error correction within a distance D of the data block of a QECC. Show that we can arrange all the ancillas required to do L levels of concatenated quantum error correction within a distance D^L.

b) Suppose we can physically move qubits around the lattice, but that moving a qubit a distance R causes an error on it with probability Rp, where p is the error rate from a single gate. Show that the recursion relation for the effective error rate for blocks at L levels of concatenation is at worst $P_L = C(4D)^L P_{L-1}^2$ when we use a code that corrects one error, and when $P_L = CP_{L-1}^2$ is a bound on the recursion relation without the locality assumption. (Assume that we are given a computation to perform on the logical qubits which only involves gates between nearest-neighbor encoded qubits.)

c) Show that the recursion relation $P_L = C(4D)^L P_{L-1}^2$ admits a threshold value P_c such that if $P_0 < P_c$, then $P_L \to 0$ as $L \to \infty$, and calculate P_c in terms of D and C.

d) Suppose we only have nearest neighbor gates; we can still move qubits around by performing the SWAP gate between nearest neighbors. Argue that this creates a problem for fault-tolerance, and show that it can be solved in two or more physical dimensions.

e) Suppose the qubits are arranged on a one-dimensional lattice, and we only have nearest-neighbor gates. Do we still have a fault-tolerant threshold?

Problem 4. Ancilla Purification for Toffoli Gates

Recall that to perform a universal set of gates fault-tolerantly, we needed some ancillas that were not stabilizer states. These special ancillas allow us to perform gates such as the Toffoli gate. The ancilla I showed you in class for the Toffoli gate used 6 qubits, but using ideas from Problem 5 of the last problem set, you can show that the following 3-qubit ancilla is sufficient:

$$|\Psi_{000}\rangle = \sum_{ijk} (-1)^{ijk} |ijk\rangle \tag{6}$$

That is, all kets have phase $+1$ except for $|111\rangle$, which has phase -1. (Actually, this state will let you directly perform the CC-Z gate, which is related to the Toffoli gate by Hadamards on the last qubit.)

Unfortunately, the problem with these special ancilla states is that a straightforward fault-tolerant construction of them gives a rather high error rate. In this problem, we will see how a non-fault-tolerant construction can be made fault-tolerant and how the error rates on the states can be substantially decreased.

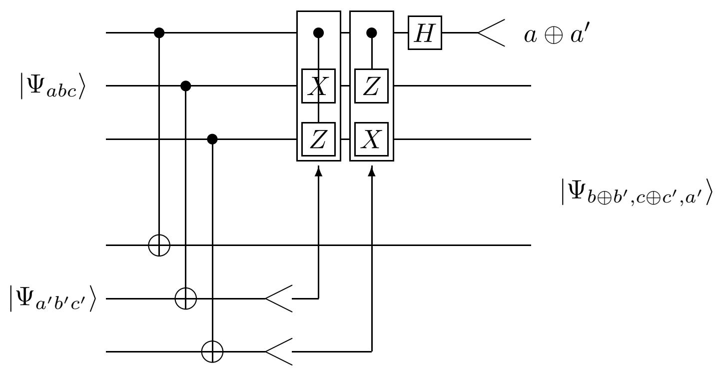
a) Show that the state $|\Psi_{000}\rangle$ is a $+1$ eigenstate of the operator $M_1 = X \otimes$ C-Z and its two cyclic permutations M_2 and M_3. Show that the 8 states

$$|\Psi_{abc}\rangle = Z^a \otimes Z^b \otimes Z^c |\Psi_{000}\rangle \tag{7}$$

are all eigenstates of M_1, M_2, and M_3, and give their eigenvalues. Show that the states $|\Psi_{abc}\rangle$ form a basis for the Hilbert space of 3 qubits.

b) Suppose we are given an arbitrary state and perform each of M_1, M_2, and M_3 with probability 1/2 independently (so, for instance, there is a probability 1/8 that we perform M_1 and M_2, but not M_3). Show that the resulting density matrix, averaged over the possible operations, is a mixture of the states $|\Psi_{abc}\rangle$.

c) Suppose we take two states, one of which is $|\Psi_{abc}\rangle$, and the other of which is $|\Psi_{a'b'c'}\rangle$, and we perform CNOTs transversally between them (from the ith qubit of the first state to the ith qubit of the second state). Then for the second state we leave the 1st qubit alone and measure the other two qubits in the Z basis. If measuring the jth qubit of the second state results in $|1\rangle$, we perform X on the jth qubit of the first state, and C-Z on the other two qubits of the first state; if measuring the jth qubit of the second state results in $|0\rangle$, we do nothing. Finally, measure the 1st qubit of the first state in X basis. We are left with three qubits, the 1st qubit of the second state and the 2nd and 3rd qubits from the first state. Show that together, they form the state $|\Psi_{b\oplus b', c\oplus c', a'}\rangle$, and that the X basis measurement of the 1st qubit of the first state has an outcome equal to $a \oplus a'$.



d) Imagine that we start with two states both of which are mixtures of various $|\Psi_{abc}\rangle$ with independent probabilities (p_a, p_b, p_c) of $a = 1$, $b = 1$, $c = 1$, respectively. Let us perform the operation from the previous part, and reject the state if the measurement shows that $a \oplus a' = 1$. Show that the new state, conditioned on $a \oplus a' = 0$, has independent probabilities (p'_a, p'_b, p'_c) and calculate them in terms of the old probabilities.

e) Show that if we perform the operation repeatedly, the probabilities approach 0 provided all the initial probabilities are below some threshold value, assuming all measurements and Clifford group operations can be done without error. Calculate the threshold value. Can you improve it by rearranging the qubits before each test?

f) What happens if we introduce some small error rate into each of the measurements and Clifford group operations?