Lecture 23

First an answer to a question from last time:

If the syndrome measurement tells us that a phase flip has occurred on the ith block of three qubits, then correction can be done by applying three Zs to all qubits in that block or by applying Z to any *one* qubit in that block. (Note that the syndrome measurement is independent of which qubit in the block of three was affected by the phase flip.)

A more sophisticated view of Shor's code via stabilizers.

Lemma 15. *Let $|\psi\rangle$ is an n-qubit state, U an n-qubit unitary and P an n-qubit stabilizer. Then if $P|\psi\rangle = |\psi\rangle$ and $PU = \alpha UP$, where $\alpha \in \{-1, +1\}$. Then $PU|\psi\rangle = \alpha U|\psi\rangle$. So measuring P on $|\psi\rangle$ gives outcome α.*

If $PU = UP$, say U and P *commute*. If $PU = -UP$, say P and U *anticommute*.

Lemma 16. *If a set of d-dimensional observables pairwise commute, then they can be measured simultaneously, i.e., the order in which they are measured does not affect the distribution over measurement outcomes and the resulting states.*

Proof sketch. Suppose the observables are $O_1, \ldots, O_n$ and measurement is performed on a d-dimensional quantum state $|\psi\rangle$. By definition, they are Hermitian, so diagonalizable. Since they also pairwise commute, they are simultaneously diagonalizable. Let $P_{\lambda_1,\ldots,\lambda_n}$ be the projector onto the simultaneous eigenspace with eigenvalues $\lambda_1, \ldots, \lambda_n$ corresponding to $O_1, \ldots, O_n$, respectively. Then can directly verify that, whatever order the observables are measured in, the probability of getting outcome λ_i when measuring observable O_i for all i is $\|P_{\lambda_1,\ldots,\lambda_n}|\psi\rangle\|^2$ and, given this outcome, the resulting state is

$$\frac{P_{\lambda_1,\ldots,\lambda_n}|\psi\rangle}{\|P_{\lambda_1,\ldots,\lambda_n}|\psi\rangle\|}. \tag{165}$$

□

Then we discussed Shor's code and the five-qubit code from HW3 from a stabilizers perspective.

The stabilizers of Shor's code:

$$\begin{aligned}
&Z_1Z_2\\
&Z_2Z_3\\
&Z_4Z_5\\
&Z_5Z_6\\
&Z_7Z_8\\
&Z_8Z_9\\
&X_1X_2X_3X_4X_5X_6\\
&X_4X_5X_6X_7X_8X_9
\end{aligned}$$

The stabilizers of the five-qubit code are as in HW3.

Then we drew two tables, one for Shor's code and one for the five-qubit code with rows labelled by the stabilizers and columns labelled by I, X_i, Z_i, X_iZ_i for $i \in [9]$ and $i \in [5]$, respectively. In each cell, we noted whether the row label commutes or anti-commutes with the column label. We observed that the table for the five-qubit code contains all possible (2^4) sign patterns which implies that it could correct any possible single-qubit error. But note that containing all possible sign patterns in the table is a *sufficient* but not necessary condition for the code being able to correct any possible single-qubit error, as we saw from the table for Shor's code.

Remark 10. There's a lot more to quantum error correction and quantum fault tolerance. Some key points we haven't covered:

1. non-unitary errors: requires formalism of density matrices. But it turns out Shor's code protects against any single-qubit error even if non-unitary.

2. better codes, e.g., correct more error, uses less qubits, easier to apply gates on, easier to detect/correct? give a flavor of non-triviality: Hamming $(7, 4)$ code, which leads to Steane's code via the CSS construction. (There are now many families of codes: see quantum error correction zoo. Some of these led to new phases of matter in physics being discovered, e.g., Haah's code.)

3. how to implement elementary quantum gates (H,T,cNOT) and measurements fault-tolerantly? (Can think of what we did as implementing the identity fault tolerantly.)

4. quantum threshold theorem: if every operation of a quantum circuit can carry faults (including components purported to do the error correction) is it even possible to correct errors? (Who guards the guards question.) Answer: yes. Statement of threshold theorem: a quantum circuit on n qubits containing C operations (elementary quantum gates, state preparation, measurement) may be simulated with probability of error at most ϵ using $O(C \times \text{poly}(\log(C/\epsilon)))$ operations such that each operation is affected by error with probability at most p_e, provided p_e is less than some contant threshold $p_e < p_{\text{th}}$.

Brief introduction to quantum cryptography.

1. Quantum money [Wiesner, 70s]. Unclonable money. Classical banknotes can be cloned in principle: put it under a microscope find out all its constituent materials and remake using those materials. Quantum information allows a form of money that is not clonable even in principle. Bank knows classical info (serial number, basis, value); only serial number and quantum state corresponding to basis-value pairs is printed on banknote. Also works with $|+\rangle$ and $|0\rangle$ but doesn't work with $|0\rangle$ and $|1\rangle$ or $|+\rangle$ and $|-\rangle$.

2. BB84 quantum key distribution [Bennett-Brassard, 84]. Suppose Alice and Bob want to be able to communicate in secret but everyone sees what they are communicating? How can this be done? Classically: meetup beforehand and agree on a cipher, the most secure cipher is a one-time pad, i.e., a random string of bits. But what if they are not allowed to meet, maybe it's too dangerous if they're, say, spies? Can Alice and Bob share a random string of bits that only they know? Classically this would be impossible, because an eavesdropper can copy the information Alice and Bob are communicating and "play Bob" to get the key – it can play Bob because by assumption Alice and Bob don't have any private information if they don't meet up beforehand.

   (a) Alice send qubits in uniformly random BB84 states (recording which ones she sent) and Bob measures each qubit in a uniformly random basis (i.e., either do measurement $\{|+\rangle\langle+|, |-\rangle\langle-|\}$ –X-basis measurement – or measurement $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ – Z basis measurement).

   (b) Communicate all their basis information. (But not value information.)

   (c) Consistency check on some values where the basis agrees.

   (d) If consistency check passes, use remaining values where the basis agrees.