Introduction to quantum information and quantum cryptography: Lecture 7

WANTED

DEAD & ALIVE

Schrödinger's cat

$$\frac{1}{\sqrt{2}}(|\mathrm{DEAD}\rangle + |\mathrm{ALIVE}\rangle)$$

Quantum error correction

Quantum error correction

Today we study how quantum entanglement is used in error correction processes. Due to the noisy quantum channels[a], error correction is required in the field of quantum communication protocols.

[a] Naturally there are several other phenomena which can cause errors in quantum information protocols, for instance faulty gates, measurements, preparations

First of all, we have to clarify the reason why we use the quantum entanglement as a tool in error correction, instead of using redundancy as we saw in the case of classical information systems.

Quantum error correction

The answer is very trivial, if we recall what we learned about quantum cloning.

Being an impossible quantum map, quantum cloning can not be used to create one or several clones of a qubit which is in an unknown quantum state, hence redundancy can not be applied if we handle quantum bits.

Quantum error correction

Fortunately, using a highly entangled state of several qubits, we have a possibility to spread the information carried by a single qubit onto the entangled state.

Peter Shor suggested a method where the information of one qubit is stored in the highly entangled state of nine qubits.

Quantum error correction

Classical error correcting codes generally use a syndrome measurement to detect which error appears in an encoded state. After this, applying a corresponsive operation based on the detected syndrome we can correct the error.

Also in quantum error correction protocols syndrome measurements are used. Making a multi-qubit measurement, we do not disturb the information stored in the encoded state, however we retrieve information about the error.

Quantum error correction

Besides diagnosing if a qubit has been corrupted, we can also find out which qubit was affected, if we use syndrome measurements.

In addition, the outcome of a syndrome measurement bespeaks us the way how the qubit was corrupted (bit flip, sign flip or both).

Quantum error correction

It is natural to ask: how can the effect of the noise be one of a few possibilities, when the noise itself can be arbitrary?

In most of the codes, this effect can be either a bit flip, or a sign flip, or both (corresponding to the Pauli matrices X, Z, and Y). It is important to keep in mind that syndrome-measurements are projective measurements[a], hence though the noise can be arbitrary, it can be built as a superposition of basis operations.

[a] just like any of the quantum measurements (except when POVM is made, but this kind of measurement is not discussed in this semester)

Quantum error correction

The syndrome-measurement makes the qubit to choose one of the Pauli errors to have happened[a], and the syndrome bespeaks us which error was choosen.

[a] it is said to be "Pauli error" because of the kinds of errors, for instance bit flip, sign flip, or both

Hence we can apply the same Pauli operator on the corrupted qubit and in this way the effect of the error can be reverted. Unfortunately syndrome-measurements tell nothing about the value stored in the logical qubit

The bit flip code

Quantum error correction

As we know, repetition code can not be used in case of a quantum channel, because of the no-cloning theorem. Fortunately there is a solution of this problem, namely the three-qubit bit flip code.

In this method syndrome-measurement and entanglement are applied and this "protocol" is as effective as the repitition code was in classical cases.

Quantum error correction

Let suppose we want to transmit a qubit $|\psi\rangle$ through a noisy channel C. We know that this channel either flips the state of the qubit, with probability p, or leaves it untouched.

Hence, if we have a general qubit ρ as an input state of the channel C, the action of the channel on the qubit can be written as

$$C(\rho) = (1 - p)\rho + p X \rho X.$$

Quantum error correction

In our case, we want to transmit the following state: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Without applying any error correcting protocol, the state will be correctly transmitted with a probability of $1 - p$.

Naturally this number can be improved, if we encode the state into a greater number of qubits. In this way we can detect and correct errors in the corresponding logical qubits.

Quantum error correction

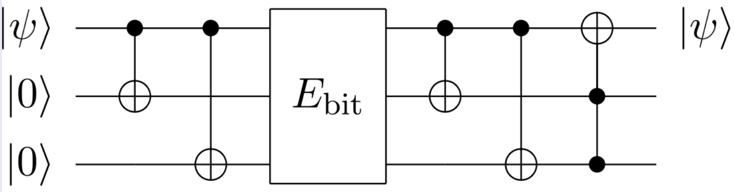
In the case of the simple three-qubit repetition code, the encoding means the following mappings:

$$|0\rangle \rightarrow |0_L\rangle \equiv |000\rangle \quad \text{and} \quad |1\rangle \rightarrow |1_L\rangle \equiv |111\rangle.$$

The input state $|\psi\rangle$ is encoded into the state $|\psi'\rangle = \alpha|000\rangle + \beta|111\rangle$. This mapping can be realized in case we apply two CNOT gates to entangle the system with two ancillary qubits initialized in the state $|0\rangle$. Hence, the encoded state $|\psi'\rangle$ is sent through the noisy channel.

Quantum error correction

Quantum circuit of the bit flip code



The channel can have an effect on $|\psi'\rangle$, because it can flip some subset of the qubits of the state. There is no qubit flip with a probability of $(1-p)^3$, one of the qubits is flipped with a probability of $3p(1-p)^2$, two of them are flipped with a probability of $3p^2(1-p)$ and all of them are flipped with a probability of p^3.

Let us realize that there is an additional assumption about the channel, namely: we assume that the effects of C on each qubit of $|\psi'\rangle$ are independent and equal.

Thus our problem is how to detect and correct such errors, without corrupting the state to be transmitted.

Quantum error correction

For the sake of simplicity, let us suppose that p is very small, thus the probability of more than one qubit is flipped is negligible.

In this case we can detect if a qubit was flipped, without also querying for the values being transmitted, by asking whether one of the qubits differs from the others.

Quantum error correction

This amounts to performing a measurement with four different outcomes, corresponding to the following four projective measurements:

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$

$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$

$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$

$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

We can do it, if we first measure $Z_1 Z_2$ and then $Z_2 Z_3$. This tells us which qubits are different from which others but does not yield any information of the state of the qubits.

In case we obtain the outcome which corresponds to P_0, there is no need to apply any of the corrections. On the other hand, in case of obtaining an outcome corresponding to P_i, we have to apply the Pauli X gate on the i-th qubit.

Quantum error correction

This procedure can be expressed by the following map (which has to be applied on the output of the channel):

$$C_{corr}(\rho) = P_0 \, \rho \, P_0 + \sum_{i=1}^{3} X_i P_i \, \rho \, P_i X_i .$$

It is important to know that this procedure does not work properly, if there are more the one qubit flipped by the channel.

The sign flip code

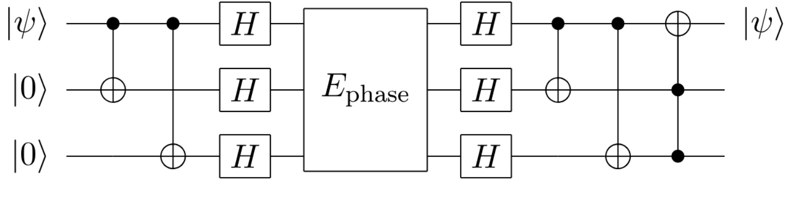
Quantum error correction

Although in classical case bit flip can be the only kind of error, using a quantum computer we have to face another kind of error, namely the sign flip.

This means that the relative sign between $|0\rangle$ and $|1\rangle$ can become inverted. For example a state like this $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ can change into the following state: $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, which is a sign flip.

Quantum error correction

Quantum circuit of the phase flip code



Quantum error correction

The original state to be transmitted is $|\psi\rangle = \alpha|+\rangle + \beta|-\rangle$, which will be altered into the following state:

$$|\psi'\rangle = \alpha|+++\rangle + \beta|---\rangle.$$

Expressing a state on the Hadamard base, a sign flip becomes bit flip and vice versa. In case C_{phase} is a quantum channel causing at most one bit flip, the bit flip code can recover $|\psi\rangle$ by transforming it into the Hadamard basis before and after transmission through C_{phase}.

The Shor code

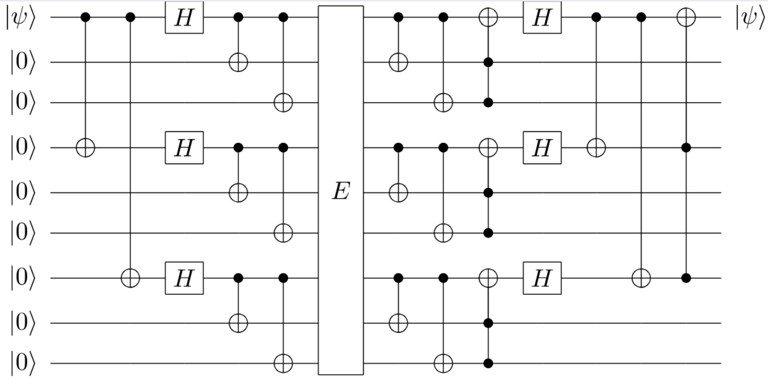
Quantum error correction

A noisy channel can cause sign flip, bit flip or both. Using the Shor code both types of errors can be corrected. Actually, arbitrary single-qubit errors can be fixed by applying the Shor code.

Let us suppose C is a quantum channel, which can corrupt a quantum bit in an arbitrary way. In our figure (below), the 1st, 4th and 7th are for the sign flip code and the three group of qubits (1,2,3), (4,5,6), (7,8,9) are designed for the bit flip code.

Quantum error correction

Quantum circuit of Shor code



Quantum error correction

Using the Shor code, we transform the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ into the product state of nine qubits $|\psi'\rangle = \alpha|0_S\rangle + \beta|1_S\rangle$, where

$$|0_S\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

and

$$|1_S\rangle = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle).$$

Quantum error correction

In case one of the qubits has a bit flip error, the syndrome analysis is performed on each set of states (1,2,3), (4,5,6), (7,8,9), and the error will be fixed.

If the three bit flip groups (1,2,3), (4,5,6), (7,8,9) are considered as three inputs, the Shor code circuit can be reduced as a sign flip code. In other words, the Shor code can also fix sign flip error for a single qubit.

Quantum error correction

Any arbitrary error can be corrected by the Shor code, in the case of a single qubit. Considering an error as a unitary transform U (acting on a qubit $|\psi\rangle$), it can be described by the following expression:

$$U = c_0\, I + c_1\, \sigma_x + c_2\, \sigma_y + c_3\, \sigma_z,$$

where c_0, c_1, c_2, c_3 are complex factors, I is the identity operator and there are the familiar Pauli matrices in the formula, namely:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

In case $U = 0$, there was no error. If $U = \sigma_x$, there was a bit flip. In the case of $U = \sigma_z$, there was a sign flip. And if $U = i\sigma_y$, there were both bit flip and sign flip. From the linearity, it follows that the Shor code can fix arbitrary one-qubit errors.

We remark there are other quantum error correcting protocols, but our present knowledge is not enough to understand how they work.