QIP Course 13: Quantum Error Correction (this might be skipped)

Ryutaroh Matsumoto

Nagoya University

September 2019

Acknowledgment and Copyright

Error correction, in classical and quantum cases

A communication channel usually has noise, so error correction is necessary (e.g. audio CD, mobile phone, etc.).

Error correction of classical information

Adding redundancy helps a receiver to decode the original information from received signals.

Error correction of quantum information?

The quantum no-cloning theorem seemed to prevent adding redundancy, until 1995.

Simple repetition quantum error-correcting code

Hereafter quantum codes refer to quantum error-correcting codes.
Suppose that

- we want to send one qubit $\alpha|0\rangle + \beta|1\rangle$,
- each qubit transmitted can be multiplied by X or received without change,
- and errors on different qubits are statistically independent.

Encoder: $\alpha|0\rangle + \beta|1\rangle \mapsto \alpha|000\rangle + \beta|111\rangle$.
The above can actually be done by two steps.

1. Prepare two qubits to state $|00\rangle$ and attach it to $\alpha|0\rangle + \beta|1\rangle$, then get $(\alpha|0\rangle + \beta|1\rangle)|00\rangle$.
2. Apply a unitary matrix converting $|000\rangle$ to $|000\rangle$ and $|100\rangle$ to $|111\rangle$.

Decoder of the simple code

1. Measure $Z \otimes Z \otimes I$ and $I \otimes Z \otimes Z$. The order of two measurements does not matter.
2. Apply unitary matrices according to outcomes as below:

$Z \otimes Z \otimes I$	$I \otimes Z \otimes Z$	unitary
$+1$	$+1$	nothing
$+1$	-1	$I \otimes I \otimes X$
-1	$+1$	$X \otimes I \otimes I$
-1	-1	$I \otimes X \otimes I$

3. Perform the inverse of the encoding procedure.

The presented encoder and decoder reconstruct the original quantum state $\alpha|0\rangle + \beta|1\rangle$ **if** one or zero out of three qubits is affected by the X error. Demonstrate this on blackboard with the error $X \otimes I \otimes I$.

What happens if Z occurs

Suppose Z error occured at one of three qubits. The encoded state becomes

$$\alpha|000\rangle - \beta|111\rangle.$$

Measurement outcome of $Z \otimes Z \otimes I$ is $+1$ with probability 1, and that of $I \otimes Z \otimes Z$ is $+1$ with probability 1 (Verify this in Exercise 2).
Therefore, these errors cannot be distinguished from no error, and the error cannot be recognized. This example cannot correct Z errors.

Exercise

1. Suppose that X_2 error occured. Verify that measurement outcome of $Z_1 \otimes Z_2$ is -1 with probability 1, and that of $Z_2 \otimes Z_3$ is -1 with probability 1 and the state is not changed by measurement.
2. See page 6.

Fidelity – distance of quantum states

In order to decide whether quantum error correction is useful or not, we need a measure of distance between two quantum states, and we have to check whether quantum error correction decreases

- the distance between the original state and error corrected state
- from the distance between the original state and unprotected state with error.

A mixed state is a state represented by a density matrix. The fidelity between a pure state $|\varphi\rangle$ and a mixed state ρ is

$$\langle\varphi|\rho|\varphi\rangle.$$

We have $0 \leq \langle\varphi|\rho|\varphi\rangle \leq 1$, and larger fidelity means that two states are closer.

Meaning of the fidelity

Suppose that we check the state ρ is equal to $|\varphi\rangle$ by measuring the observable

$$M = |\varphi\rangle\langle\varphi| + 2(I - |\varphi\rangle\langle\varphi|).$$

Observe that M has eigenvalue $+1$ with projector $|\varphi\rangle\langle\varphi|$ and eigenvalue $+2$ with projector $(I - |\varphi\rangle\langle\varphi|)$. The probability of getting outcome $+1$ is equal to

$$\mathrm{Tr}[\rho|\varphi\rangle\langle\varphi|] = \langle\varphi|\rho|\varphi\rangle.$$

We also note that the fidelity can be generalized to two mixed states, and that $1 -$ fidelity satisfies the axiom of metric on the set of mixed states.

We also note that sometimes $\sqrt{\langle\varphi|\rho|\varphi\rangle}$ is meant by the word "fidelity".

Fidelity increases by error correction

Suppose that the X error occurs at each qubit with probability p. If an error correcting code is not used, the original state

$$\alpha|0\rangle + \beta|1\rangle$$

becomes

$$\begin{aligned} \rho &= (1-p)(\alpha|0\rangle + \beta|1\rangle)(\alpha\langle 0| + \beta\langle 1|) + \\ & \quad p(\alpha|1\rangle + \beta|0\rangle)(\alpha\langle 1| + \beta\langle 0|) \end{aligned}$$

We want to consider the worst case, so assume $\alpha = 1$ and $\beta = 0$. In this case

$$\rho = (1-p)|0\rangle\langle 0| + p|1\rangle\langle 1|$$

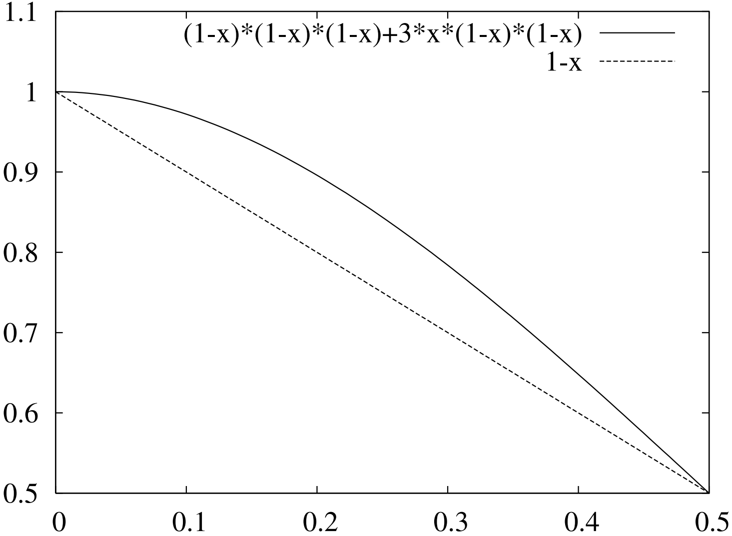
and the fidelity between ρ and $|0\rangle$ is p.

If we use the error correction, the original state is preserved when the number of errors ≤ 1, whose probability is $(1-p)^3 + 3p(1-p)^2$. The density matrix after error correction can be written as

$$\begin{aligned} \rho' &= \{(1-p)^3 + 3p(1-p)^2\}(\alpha|0\rangle + \beta|1\rangle)(\alpha\langle 0| + \beta\langle 1|) \\ &\quad +\{1-(1-p)^3 - 3p(1-p)^2\}\rho'' \end{aligned}$$

for some mixed state ρ''. Therefore the fidelity between $\alpha|0\rangle + \beta|1\rangle$ and ρ' is at least $(1-p)^3 + 3p(1-p)^2$, which is larger than $1-p$ if p is small.

Graph of fidelity



The Shor code

The first quantum error-correcting code was proposed by Peter Shor. It encodes 1 qubit to 9 qubits and can correct an *arbitrary* error acting on a single qubit.

$$
\begin{aligned}
|0\rangle &\mapsto \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} \\
|1\rangle &\mapsto \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}
\end{aligned}
$$

X_i: the X matrix acting on the i-th qubit
Z_i: the Z matrix acting on the i-th qubit

Correction of the X error

We measure $Z_1 \otimes Z_2, Z_2 \otimes Z_3, Z_4 \otimes Z_5, Z_5 \otimes Z_6, Z_7 \otimes Z_8, Z_8 \otimes Z_9$.
Observe that each triple of qubits is the same as the error correcting code explained in the previous lecture. Each triple refers to 1st, 2nd and 3rd qubits, or 4th, 5th and 6th qubits, or 7th, 8th and 9th qubits.
We can correct single X error by the same error-correcting process.

Correction of the Z error

After (or before) correcting an X error, we correct a Z error.
We measure $X_1 \otimes X_2 \otimes \cdots \otimes X_6$ and $X_4 \otimes X_5 \otimes \cdots \otimes X_9$.
$(|000\rangle \pm |111\rangle)(|000\rangle \pm |111\rangle)$ belongs to the eigenvalue $+1$ of $X_1 \otimes X_2 \otimes \cdots \otimes X_6$ if the two $\pm$ are the same, otherwise it belongs to -1.

Z errors changes the sign $\pm$:
$Z_1 \otimes I \otimes I(|000\rangle \pm |111\rangle) = I \otimes Z_2 \otimes I(|000\rangle \pm |111\rangle) = I \otimes I \otimes Z_3(|000\rangle \pm |111\rangle) = |000\rangle \mp |111\rangle$. Observe that different errors have the same effect.

Relation between errors and measurement outcomes

observable	no error	Z_1 or Z_2 or Z_3	Z_4 or Z_5 or Z_6	Z_7 or Z_8 or Z_9
$X_1 \otimes \cdots X_6$	+1	-1	-1	+1
$X_4 \otimes \cdots \otimes X_9$	+1	+1	-1	-1

Correction of the XZ error

If an XZ error occurs on some qubit, it can be corrected by doing the X error correction and the Z error correction sequentially (Exercise).

Correction of an arbitrary error 1

Let U be a 2×2 unitary matrix. Suppose that the error U occured at the first qubit. Since I, X, Z, and XZ is a basis for 2×2 matrices, we can write

$$U = a_I I + a_X X + a_Z Z + a_{XZ} XZ.$$

Suppose that the state of 9 qubits was $|\varphi\rangle$ (an encoded state of the Shor code) before error. Specifically

$$\alpha \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}$$
$$+\beta \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}.$$

After error, the state is

$$\begin{aligned} & (U \otimes I^{\otimes 8})|\varphi\rangle & (1) \\ = \;& a_I(I \otimes I^{\otimes 8})|\varphi\rangle + a_X(X \otimes I^{\otimes 8})|\varphi\rangle & (2) \\ & + a_Z(Z \otimes I^{\otimes 8})|\varphi\rangle + a_{XZ}(XZ \otimes I^{\otimes 8})|\varphi\rangle. & (3) \end{aligned}$$

Correction of an arbitrary error 2

Recall that

1. The state after a single error X, Z, or XZ is an eigenstate of the observable for error correction.
2. Different errors cause different measurement outcomes, or have the same effect on the state. Otherwise one cannot correct errors.

Thus, the each term in Eq. (3) belongs to different eigenvalues. After measurement, one out of four terms in Eq. (3) remains, whose error can be regarded as I, X, XZ, or Z.

Noisy channel

Study of diginal communications expresses a noisy channel as a conditional probability of output given input.

Noisy quantum channel can be considered in a similar way. Suppose that output σ_i (density matrix) is output with a probability p_i when the input is ρ (density matrix).
But, the output can be expressed as

$$\sum_i p_i \sigma_i.$$

It is more natural to express a noisy quantum channel as a mapping from density matrices to density matrices.

Which conditions are necessary for noisy quantum channel

$\mathcal{S}_{\mathrm{in}}$: the set of density matrices on some linear space.
$\mathcal{S}_{\mathrm{out}}$: the set of density matrices on another linear space.
$\Gamma : \mathcal{S}_{\mathrm{in}} \to \mathcal{S}_{\mathrm{out}}$.
Γ should have the following three properties:

Linearlity Because Γ must preserve the ratio of probabilistic mixtures.

Trace-Preserving

Complete Positivity Let I_n be the identity mapping from the space of $n \times n$ matrices to itself. For all n, $\Gamma \otimes I_n$ sends positive semidefinite matrices to positive semidefinite matrices.

The second and the third conditions are **necessary** to convert density matrices to density matrices.

Three conditions are also **sufficient**

Suppose that Γ satisfies the three conditions. Then there exists a linear space $\mathcal{H}_{\mathrm{env}}$, its pure state $|0_E\rangle$ and the unitary matrix acting on $\mathcal{H}_{\mathrm{env}}$ and the input of Γ, such that

$$\Gamma(\rho) = \mathrm{Tr}_{\mathcal{H}_{\mathrm{env}}}[U(\rho \otimes |0_E\rangle\langle 0_E|)U^*]. \tag{4}$$

Draw its physical meaning on the black board.
The existence of such U and $|0_E\rangle$ shows that the three conditions are also sufficient.

A map with the three conditions is called

- quantum operation, or
- CPTP (completely positive trace-preserving) map.

Criticism on the usual error model in QECC

In the beginning of research in quantum error correction, it was assumed that a finite set of unitary matrices can occur as a channel error. It does not seem reasonable because

- There are infinitely many unitary matrices, and
- The noisy state evolution comes from interaction with the surrounding environment, and such an interaction cannot be written as a uniatry matrix on the transmitted quantum information.

But the original assumption can be justified (explained later).

When an error is considered to be corrected

When the receiver reconstructs the original transmitted quantum state perfectly, the error is considered to be corrected. But this is too restrictive, because

1. quantum information is "analog", and
2. a small difference between the original state and the decoded state is acceptable.

Small difference between two states results in a small difference in probability distributions under the same measurement. This also justifies allowing a small difference the transmitted and the decoded states.

Then, how one quantifies the difference? There are several ways (see Chapter 12 of Nielsen&Chuang). One way is to use the fidelity introduced earlier in this course.

Memoryless assumption

In digital communications, additive noise can often be seen as independently and identically distributed (i.i.d.). For example, the additive noise often comes from random motion of electrons in receive circuit, which has the same probability distribution and statistically independent among different time instances. A channel with the i.i.d. assumption is called **memoryless**.

Suppose that n quantum systems are transmitted and the channels is denoted by a CPTP map Γ_n. Under some assumtions (e.g., each quantum system interacts with a different environment during transmission), then Γ_n satisfies the i.i.d. assumption, i.e.,

$$\Gamma_n = \Gamma_1 \otimes \Gamma_1 \otimes \cdots \otimes \Gamma_1,$$

where Γ_1 is a CPTP map acting on a single system. Such a quantum channel is called **memoryless**.

Memoryless assumption justifies finite errors

Assume that

- n quantum systems are transmitted, and
- the quantum channel is memoryless.

Let B be a basis of matrices on a single system, and B is assumed to have the identity matrix.
When a transmitter and a receiver

- assume only errors in $B^{\otimes n}$ occur,
- define the number of errors to be non-identity component in the error matrix,
- and corrects errors if the number of errors is not large,

then the decoded mixed state has high fidelity with the original pure state.
Reference: R. Matsumoto, Fidelity of a t-error correcting quantum code with more than t errors, Phys. Rev. A, vol. 64, no. 2, 022314, Aug. 2001 (see also its erratum).

Exercise

1. Suppose that the XZ error occured at the 5th qubit of the Shor code. Describe the changes of the state in the error correction process step by step.
2. Verify that I, X, Z, and XZ form a basis for the linear space of 2×2 matrices.
3. Suppose that the H error occured at the 5th qubit of the Shor code, where

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Describe the changes of the state in the error correction process step by step.
4. Show that the fidelity between $\alpha|0\rangle + \beta|1\rangle$ and ρ' in page 11 is at least $(1-p)^3 + 3p(1-p)^2$.
5. Show that $0 \leq \langle\varphi|\rho|\varphi\rangle \leq 1$.