How well can you copy a qubit?

Piotr Deuar

Supervisors: Peter Drummond
Bill Munro

Outline

- The No-cloning theorem
- Fidelity measures of copying efficiency
- Information measures of copying efficiency
- Finding maximum transmitted information into the copies.
- Results
- Comparison of Fidelity and Information measures
- Unfinished business

No-cloning Theorem

W.K.Wootters & W.H.Zurek *Nature* **299** 802 (1982)

Perfect copies of arbitrary quantum states cannot be made by any unitary process

if $\langle + | - \rangle = 0$, $|q\rangle$ is some state, and

$$\begin{cases} |+\rangle\,|q\rangle & \rightarrow |+\rangle\,|+\rangle \\ |-\rangle\,|q\rangle & \rightarrow |-\rangle\,|-\rangle \end{cases}$$

then if

$$|\theta\rangle = \cos\theta\,|+\rangle + \sin\theta\,|-\rangle$$

$$|\theta\rangle\,|q\rangle \rightarrow \sin\theta\,|+\rangle\,|+\rangle + \cos\theta\,|-\rangle\,|-\rangle$$

but a perfect copier would produce

$$\begin{aligned} |\theta\rangle\,|\theta\rangle = {} & \sin^2\theta\,|+\rangle\,|+\rangle + \cos^2\theta\,|-\rangle\,|-\rangle \\ & + \cos\theta\sin\theta\,(|+\rangle\,|-\rangle + |-\rangle\,|+\rangle) \end{aligned}$$

So if we can't have perfect copiers,
How well can we do?

relevant to many fields

- Quantum Cryptography
- State Preparation
- Teleportation
- Others

Says something about quantum behaviour in general.

Fidelity measures

The fidelity between two states ρ_1 and ρ_2 is

$$F = \mathrm{Tr}\left[\rho_1 \rho_2\right]$$

for pure states it is the *overlap squared* between the states.

When characterising quantum copying in the literature, usually the fidelity between the actual output states, and "ideal copies" is evaluated.

Some similar, related measures, such as the Hilbert-Schmidt norm of the difference between ρ_1 and ρ_2:

$$\sqrt{\mathrm{Tr}\left[\|\rho_1 - \rho_2\|^2\right]}$$

are also used.

Fidelity is easy to calculate (certainly a plus!), but:

- Experiments don't measure fidelity.
- For copying: Fidelity between what?
- Its meaning varies depending on the system.
- For copying: not robust to transformations done on the copies after all copying has been completed.
- Can be very high, even though copies are useless.

examples

Coherent states:

$$\langle \alpha | \, \alpha + 1 \rangle = \frac{1}{e}$$

a constant.

But if $|\alpha|$ is small, the states $|\alpha\rangle$ and $|\alpha + 1\rangle$ are very different, whereas if $|\alpha|$ is large, they are almost identical.

examples

Relabeling of copy states:

Suppose you send a message in a binary alphabet of orthogonal states $|0\rangle$,$|1\rangle$ through a lossless communication channel that swaps the states

$$\begin{cases} |0\rangle & \to |1\rangle \\ |1\rangle & \to |0\rangle \end{cases}$$

then the fidelity of the transmitted state with respect to the sent one is *zero*.

But the message can still be perfectly reconstructed!

Conversely: If you encode a message using very nonorthogonal states, $|a\rangle$,$|b\rangle$ but the channel always transmits the same state $|a\rangle$.

$$\begin{cases} |a\rangle & \to |a\rangle \\ |b\rangle & \to |a\rangle \end{cases}$$

then the average fidelity is still high, although the transmitted message is useless.

Mutual Information

If we have two observers A and B who make some measurements. Then the amount of information (per measurement) each has about the results of the other's measurements is the *Mutual Information*. This is given by

$$
\begin{aligned}
I_{\text{mutual}} &= -\sum_i P_i \log_2 P_i \\
&\quad -\sum_j P_j \log_2 P_j \\
&\quad +\sum_{i,j} P_{i,j} \log_2 P_{i,j}
\end{aligned}
$$

where $P_{i,j}$ are the probabilities that A will get the ith measurement result, and B will get the jth result. P_i and P_j are the marginal probabilities.

Often easy to get in an experiment, and avoids the pitfalls of Fidelity, but is harder to calculate.

In quantum copying, we really want to know how much information can be transmitted between A who encodes a sequence of states, and B who gets one of the copies. Not how close mathematically the states are.

Not interested in a “dumb” B, but in how much a “smart” B can get out of the copies. Optimising B’s measurements can be difficult.

Information limits on copiers

Will consider a basic message encoded by observer A as a binary sequence of quantum states.

1. Two signal states $|s_1\rangle$, $|s_2\rangle$
2. Signal states are pure
   $\rightarrow$ output states also.
3. Signal states have an overlap of
   $\langle s_1 | s_2 \rangle = z$
4. Sent with equal probability.
5. Hilbert space of states is 2d $\rightarrow$ qubits.

Consider copiers which:

1. are unitary transformations

2. are $1 \to 2$

3. are symmetric.

4. do not use additional states

Observer B considers one copied symbol at a time.

These conditions define the basic copying transformations underlying more complicated ($\to$ harder to implement) schemes.

How not to waste your states

Observer B gets one of two states ρ_1, ρ_2 depending on what A sent. Want to distinguish them with maximum confidence.

Make projective measurements on the states in the basis which diagonalises the difference between them.

So this is what a "smart" B is going to do with the copy.

Outline of the calculations

There are two arbitrary input qubits $|s_1\rangle$ and $|s_2\rangle$, and two corresponding states $|\psi_1\rangle$ and $|\psi_2\rangle$ consisting of both copies (possibly entangled). At first glance: 24 real variables.

Fortunately you can discard 21 as irrelevant before you start calculating.

Input states: Form irrelevant. Occur with equal probability. Their overlap is a parameter, and can be made real without loss of generality.

Output states: One phase in each state is unphysical. Since B is "smart", we can let the basis in one of the copy subsystems be whatever we like, to reduce the number of variables without affecting the generality of the calculation. So, there are 11 left

$$
\begin{aligned}
|\psi_1\rangle &= a_1|{+}{+}\rangle + a_2 e^{i\theta_2}|{+}{-}\rangle + a_4|{-}{-}\rangle \\
|\psi_2\rangle &= b_{++}|{+}{+}\rangle + b_{+-} e^{i\theta_{+-}}|{+}{-}\rangle + b_{-+} e^{i\theta_{-+}}|{-}{+}\rangle + b_{=} e^{i\theta_{=}}|{-}{-}\rangle
\end{aligned}
$$

Now,
B is only interested in one copy $\rightarrow$ trace over the other
Copier is symmetric.
Transformation is unitary.

Three free parameters left.

Stetes received by B are:

$$\rho_1^B = \begin{pmatrix} a_1^2 & 0 \\ 0 & 1 - a_1^2 \end{pmatrix}$$

$$\rho_2^B = \begin{pmatrix} x & \beta^* \\ \beta & 1 - x \end{pmatrix}$$

where

$$x = \frac{1}{2}\left[1 + b_{++}^2 - b_{=}^2\right]$$

$$\beta = \sqrt{\frac{1 - b_{++}^2 - b_{=}^2}{2}}\left\{b_{++}e^{-i\theta_{+-}} + b_{=}e^{i\theta_{+-}}\right\}$$

Optimisation analytically rather difficult.
$\rightarrow$ *Matlab*

However, optimised states are easily written down in analytical form
$\rightarrow$ should do the calculation analytically later.

An optimum information copier

Define an orthogonal basis $\{|+\rangle, |-\rangle\}$ so that the input states are given by

$$\begin{aligned} |s_1\rangle &= \cos\theta\,|+\rangle + \sin\theta\,|-\rangle \\ |s_2\rangle &= \sin\theta\,|+\rangle + \cos\theta\,|-\rangle \end{aligned}$$

They have overlap

$$z = \langle s_1 | s_2\rangle = \sin 2\theta$$

One of the optimum copiers is the so-called *Wootters-Zurek Quantum Copying Machine* first mentioned in the proof of the no-cloning theorem.

$$\begin{cases} |+\rangle & \rightarrow |+\rangle\,|+\rangle \\ |-\rangle & \rightarrow |-\rangle\,|-\rangle \end{cases}$$

About as simple a copying machine as you can get.

Compare this to the fidelity-optimising copier:

$$\begin{aligned}
|0\rangle &\rightarrow a\,|00\rangle + b\,(|01\rangle + |10\rangle) + c\,|11\rangle \\
|1\rangle &\rightarrow c\,|00\rangle + b\,(|01\rangle + |10\rangle) + a\,|11\rangle
\end{aligned}$$

where

$$\begin{aligned}
a &= \frac{\cos\theta(P + Q\cos 2\theta) - \sin\theta(P - Q\cos 2\theta)}{\cos 2\theta} \\
b &= P\tan 2\theta(\cos\theta - \sin\theta) \\
c &= \frac{\cos\theta(P - Q\cos 2\theta) - \sin\theta(P + Q\cos 2\theta)}{\cos 2\theta}
\end{aligned}$$

and,

$$\begin{aligned}
P &= \frac{1}{2}\sqrt{\frac{1 + \sin 2\theta}{1 + \sin^2 2\theta}} \\
Q &= \frac{1}{2}\frac{\sqrt{1 - \sin 2\theta}}{\cos 2\theta}
\end{aligned}$$

The transformation of input states

$$\begin{aligned}
|s_1\rangle &= \cos\theta\,|1\rangle + \sin\theta\,|0\rangle \\
|s_2\rangle &= \sin\theta\,|1\rangle + \cos\theta\,|0\rangle
\end{aligned}$$

is even more involved.

Comparison

- The Wootter-Zurek Quantum Copying Machine is much more useful than any copiers that maximise fidelity, whether state-dependent or universal.

- The simplest copiers are the best ones.

- Optimum information copiers give entangled copies, but the copies are mixed states.

- For small overlap between signal states, can get quite good information transfer to the copies.

Long Words

If B makes a measurement on whole sequences of signal states at once, where only some sequences are allowed, the information capacity of the channel per signal state can approach the Holevo bound, which is somewhat greater than the mutual information per state given above. However,

- That sort setup is not feasible in the near future.

- Equivalent to sending signals from a large alphabet, with complicated behaviour. Should be treated as such, because more optimisation of signal probability and copying machine is then possible.

The results using the Holevo bound are qualitatively the same as shown before, but the quantitative difference between information and fidelity-optimised copiers is smaller.

Unfinished Business

- Is a Wootters-Zurek Quanum Copying Machine practically realizable?

- What is the role of the entanglement between the copies? How does it help?

- Does any qualitatively new behaviour arise with more than two signal states, or more than two copies?

- Are pure signal states sufficient for optimal information transfer?

- Are additional “helper” states really unnecessary for optimality?

- Derive optimal information bounds and copier transformations analytically.

Thank You