Quantum Error Correction

SOURCES:
Michele Mosca
Richard Spillman
PROBLEM: When computing with a quantum computer, you can’t look at what the computer is doing
   - You are only allowed to look at the end

RESULT: What happens if an error is introduced during calculation?

SOLUTION: We need some sort of quantum error detection/correction procedure
Classical Error Codes

- In standard digital systems bits are added to a data word in order to detect/correct errors.
- A code is **e-error detecting** if any fault which causes at most \( e \) bits to be erroneous can be detected.
- A code is **e-error correcting** if for any fault which causes at most \( e \) erroneous bits, the set of all correct bits can be automatically determined.
- The **Hamming Distance**, \( d \), of a code is the minimum number of bits in which any two code words differ.
  - the **error detecting/correcting capability** of a code depends on the value of \( d \).
**Parity Checking**

- **PROCESS:** Add an extra bit to a word before transmitting to make the total number of bits even or odd (even or odd parity)
  - at the receiving end, check the number of bits for even or odd parity
  - It will detect a single bit error
  - Cost: extra bit

- **Example:** Transmit the 8-bit data word 1 0 1 1 0 0 0 1
  - Even parity version: 1 0 1 1 0 0 0 1 0
  - Odd parity version: 1 0 1 1 0 0 0 1 1
In 1995, Peter Shor developed an improved procedure using 9 qubits to encode a single qubit of information.

His algorithm was a majority vote type of system that allowed all single qubit errors to be detected and corrected.
Suppose errors in our physical system for storing 0 and 1 cause each physical bit to be toggled independently with probability $p$.

We can reduce the probability of error to be in $O(p^2)$ by using a “repetition code”.

E.g.: encode a logical 0 with the state 000 and a logical 1 with the state 111.
Reversible networks for encoding and decoding
After the errors occur, decode the logical bits by taking the majority answer of the three bits and correct the encoded bits.

So:

000 → 000  111 → 111
001 → 000  011 → 111
010 → 000  101 → 111
100 → 000  110 → 111
As long as less than 2 errors occurred, we will keep the correct value of the logical bit.

The probability of 2 or more errors is

$$3p^2(1 - p) + p^3 = 3p^2 - 2p^3 \in O(p^2)$$

(which is less than $p$ if $p < \frac{1}{2}$)
A 3-bit quantum error correction scheme uses an encoder and a decoder circuit as shown below:
The **encoder** will **entangle** the two redundant qubits with the input qubit:

1. If the input state is $|0\rangle$ then the encoder does nothing so the output state is $|000\rangle$

2. If the input state is $|1\rangle$ then the encoder flips the lower states so the output state is $|111\rangle$

3. If the input is an superposition state, then the output is the entangled state $a|000\rangle + b|111\rangle$
Problem: Any correction must be done without looking at the output

- The decoder looks just like the encoder:

If the input to the decoder is $|000\rangle$ or $|111\rangle$, there was no error so the output of the decoder is:

<table>
<thead>
<tr>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>000\rangle$</td>
</tr>
<tr>
<td>$</td>
<td>111\rangle$</td>
</tr>
</tbody>
</table>

Error free flag
Consider all the possible error conditions:

No Errors:
\[ a|000\rangle + b|111\rangle \text{ decoded to } a|000\rangle + b|100\rangle = (a|0\rangle + b|1\rangle)|00\rangle \]

Top qubit flipped:
\[ a|100\rangle + b|011\rangle \text{ decoded to } a|111\rangle + b|011\rangle = (a|1\rangle + b|0\rangle)|11\rangle \]

So, flip the top qubit = \( (a|0\rangle + b|1\rangle)|11\rangle \)

Middle qubit flipped:
\[ a|010\rangle + b|101\rangle \text{ decoded to } a|010\rangle + b|110\rangle = (a|0\rangle + b|1\rangle)|10\rangle \]

Bottom qubit flipped:
\[ a|001\rangle + b|110\rangle \text{ decoded to } a|001\rangle + b|101\rangle = (a|0\rangle + b|1\rangle)|01\rangle \]
The prior decoder circuit requires the measurement of the two extra bits and a possible flip of the top bit.

- Both these operations can be implemented automatically using a Toffoli gate.

If these are both 1 then flip the top bit.
Reversible 5-qubit network for error correction

Assume that \( e_3 + e_2 + e_1 \leq 1 \) \( e_i \in \{0,1\} \)

- If \( s_1s_2 = 00 \) then no error occurred
- Otherwise, the error occurred in bit \( j \) where \( j = 2s_1 + s_2 \)
Equivalently using measurements
This is implementing a $Z_1$ measurement (interpreting 0 as +1, and 1 as -1)
This is implementing a $Z_1 Z_2$ measurement
This is implementing a $X_1X_2$ measurement.
For an $n$-qubit system $Z_j$ denotes
\[
I \otimes I \otimes \ldots \otimes I \otimes Z \otimes I \otimes \ldots \otimes I
\]
where $j-1$ and $n-j$ are superscripts.

E.g. $n=3$, then
\[
Z_1 Z_2 = (Z \otimes I \otimes I)(I \otimes Z \otimes I) = (Z \otimes Z \otimes I)
\]
Perform operations on logical bits

- e.g. NOT gate

```
  b -------- X -------- b
  |      |      |      |
  b -------- X -------- b
  |      |      |      |
  b -------- X -------- b
```
Perform operations on logical bits

- e.g. c-NOT gate
Quantum Error Correcting Codes

- e.g.: encode a logical $|0\rangle$ with the state $|000\rangle$
- and a logical $|1\rangle$ with the state $|111\rangle$
Quantum network for encoding

\[ |b\rangle \rightarrow |b\rangle \]

\[ |0\rangle \rightarrow |0\rangle \]

\[ (\alpha |0\rangle + \beta |1\rangle) |0\rangle |0\rangle \rightarrow \alpha |0\rangle |0\rangle |0\rangle + \beta |1\rangle |1\rangle |1\rangle \]
Quantum network for correcting errors

- Assume that \( e_3 + e_2 + e_1 \leq 1 \quad e_i \in \{0,1\} \)

\[
\begin{align*}
\alpha |e_3\rangle |e_2\rangle |e_1\rangle + \beta |1\oplus e_3\rangle |1\oplus e_2\rangle |1\oplus e_1\rangle & \rightarrow \\
\alpha |0\rangle |0\rangle |0\rangle + \beta |1\rangle |1\rangle |1\rangle
\end{align*}
\]
Equivalently
Perform operations on logical bits

- e.g. Hadamard gate

$$\begin{align*}
|b\rangle &\quad \xrightarrow{H} \quad \frac{1}{\sqrt{2}} |b\rangle|b\rangle|b\rangle + \\
|\overline{b}\rangle &\quad \xrightarrow{\text{CNOT}} \quad \frac{(-1)^b}{\sqrt{2}} |b\rangle|\overline{b}\rangle|\overline{b}\rangle
\end{align*}$$
What is the problem with classical cryptography?

- **Secret key cryptography**
  - Requires secure channel for key distribution
  - *In principle* every classical channel can be monitored passively
  - Security is mostly based on complicated non-proven algorithms

- **Public key cryptography**
  - Security is based on non-proven mathematical assumptions (e.g. difficulty of factoring large numbers)
  - We DO know how to factorize in polynomial time! Shor’s algorithm for quantum computers. Just wait until one is built.
  - Breakthrough renders messages insecure *retroactively*
Key distribution

- Secret key cryptography requires secure channel for key distribution.
- **Quantum cryptography** distributes the key by transmitting quantum states in *open channel*.
The holy grail: One-time pad

- The only cipher mathematically proven
- Requires massive amounts of key material
**Crypto Definitions: Alice, Bob and Eve**

- It is a standard in cryptography to define the sender, receiver, and interceptor as:
  - **Alice** is the one who sends the ciphertext
  - **Bob** is the one who receives the ciphertext
  - **Eve** is the (evil) one who tries to steal the plaintext or key