Quantum Computing & Cryptography  
Week 11  

Quantum error correction  
(Introduction only)  
- Important in quantum computers  
  - quantum errors arise easily  
- Non-trivial  
  - must correct errors without measuring data  
  
Steve Vickers

Classical error correction

In classical computers - not much need  
- Stored bits: 0, 1 very different - unlikely to flip for extraneous reasons  
- Internal transmission: voltages circuitry allows time for transitions to stabilize

Not much need for error correction inside the computer

Classical error correction - outside computer

Signal transmission - attenuates over distance

- Needs boosting, if need error correction  
Use redundant information to detect & correct errors  
Simplest scheme: send each bit 3 times  
0 = 000 if one bit flips, other two "outvote" it - correct error  
If two bits flip - get wrong answer

Practical schemes more sophisticated

Classical error correction - outside computer

RAID Redundant array of inexpensive discs

File data  
If a disc fails: pull it out and replace it  
File store keeps working  
Error correction ⇒ can reconstruct data from working discs
Quantum error correction

1. Decoherence
   - Can't completely isolate qubit from environment
   - Qubit gets entangled with environment - disrupts computer state
   - A qubit that doesn't interact easily with environment - probably doesn't interact with rest of computer

2. Measurement
   - To detect an error, must measure
   - But that already disrupts state 😞
   - Strategy
     - Error has happened
     - How to correct it
     - It must not learn anything about correct state
     - Use ancillas, measure them.

3. Error types
   - For qubits: error = bit flip ⚠️
   - For qubits: more complicated...
     - E.g. phase errors such as $|0\rangle + |1\rangle \rightarrow |0\rangle - |1\rangle$ ⚡

4. Continuity
   - For qubits: discrete
     - Qubit either unchanged or flipped
     - No in-between
   - For qubits: errors can grow continuously
   - Quantum measurement turns small error into probability. Measurement probably restores correct state, sometimes gives definite correctable error state
**Strategy**
- Use several data qubits to store (redundantly) one bit.
- Use ancilla qubits to "measure involutions" on data qubits.
- Aim: choose involutions carefully so that measurement gives either the correct state or a known error state that can be corrected. Similar to what happens in teleportation.

**Measuring an involution**
\[ H, A H, \psi, m \rightarrow \psi \leq H, c A \frac{1}{\sqrt{2}} (\psi + \psi) \]
\[ = H, \frac{1}{\sqrt{2}} (\psi + \psi) \]
\[ = \frac{1}{2} (\psi + \psi) + \psi + \psi = \psi - \psi \]
\[ = \frac{1}{2} (\psi + \psi) + \frac{1}{2} (\psi - \psi) \]

**Projectors**

<table>
<thead>
<tr>
<th>State</th>
<th>Projectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 1/2</td>
<td>\psi\rangle (</td>
</tr>
</tbody>
</table>

Where \( P_0 = \frac{1 + A}{2} \), \( P_1 = \frac{1 - A}{2} \) are projectors.
- Self-adjoint but not unitary.
- Idempotent: \( P_0^2 = P_0 \), \( P_1^2 = P_1 \), \( P_0 P_1 = 0 \), \( P_0 + P_1 = 1 \)

**Eigenstates of A**
\[ A P_0^A = (-1)^x P_0^A \quad \Rightarrow \quad A P_1^A = (-1)^x P_1^A \]
By def., eigenstates have to be \( \geq 0 \).
If \( P_0^A |\psi\rangle \neq 0 \) then it is an eigenstate for A.
Eigenvalue = \( (-1)^x \)

\[ A |\psi\rangle = |\psi\rangle \iff P_0^A |\psi\rangle = |\psi\rangle \iff P_1^A |\psi\rangle = 0 \]
\[ A |\psi\rangle = -|\psi\rangle \iff P_1^A |\psi\rangle = |\psi\rangle \iff P_0^A |\psi\rangle = 0 \]
General state \( |\psi\rangle = P_0^A |\psi\rangle + P_1^A |\psi\rangle \) is a superposition of eigenstates for eigenvalues +1, -1.
Measuring the control qubit

State before measurement is
\[ |0⟩ P_0^A |ψ⟩ + |1⟩ P_1^A |ψ⟩ \]
Result is 0 or 1
State of other qubits reduces to normalized form \(|ψ_x⟩\) of \(P_x^A |ψ⟩\)

Note: \(A |ψ_x⟩ = |ψ_x⟩ \)

If \(|ψ⟩ = 0\) it's an eigenstate for \(A\)

Eigenvalue = \(-|x⟩\)

Diagnosing error states

Idea:

* \(|ψ⟩\) a superposition of correct state & error states

* Measuring \(A\)

1. Reduces to a single eigenstate
2. Tells you (result \(x\)) what happened
3. Helps you plan correction to \(|ψ_x⟩\)

Eigenstates for \(A\):

\(P^A_x\) is another projector

\[ P^A_x P^A_y = \begin{cases} P^A_x & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases} \]

\[ 1 = \sum_{x=0}^{2^n-1} P^A_x \]

\(P^A_x |ψ⟩\) an eigenstate for all \(A\)'s with eigenvalues \((-|x⟩\)

If \(|ψ⟩\) already an eigenstate for \(A\)'s, eigenvalues \((-|x⟩\)

Then \(P^A_x |ψ⟩ = \begin{cases} |ψ⟩ & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases} \)
Where errors come from

Environment also a quantum system
Overall state with one data qubit
\[ |e\rangle \otimes |x\rangle \rightarrow |e\rangle |x\rangle |0\rangle + |e\rangle |x\rangle |1\rangle \]

Environment data corruption can be rewritten in form
\[ |e\rangle |\psi\rangle \rightarrow (|d\rangle |1\rangle + |k\rangle |x\rangle + |b\rangle |y\rangle + |c\rangle |z\rangle ) |\psi\rangle \]

Normally: environment becomes entangled with data
- decoherence
- bad news, but error correction can fix it

5 qubit error correcting code

Code 1 bit using 5 qubits
Assume errors rare enough not to hit 2 qubits together
For each qubit: 3 dimensions of error
\[ |1\rangle \rightarrow x|1\rangle \text{ bit flip} \]
\[ |1\rangle \rightarrow z|1\rangle \text{ phase error} \]
\[ |1\rangle \rightarrow y|1\rangle \text{ combination} \]
\[ 1 + 5 \times 3=16=2^4 \] need 4 ancillas

Some commuting involutions on 5 qubits

\[
\begin{array}{c|c|c|c|c}
Z & X & X & X & Z \\
X & X & Z & Z & Z \\
X & Z & X & Z & Z \\
Z & Z & Z & Z & Z \\
\end{array}
\]

\[
\begin{array}{c}
M_0 \\
M_1 \\
M_2 \\
M_3 \\
M_4 \\
\end{array}
\]

\[
\begin{array}{c}
2, x_2 x_3 \\
2, x_2 x_3 \\
2, x_2 x_3 \\
2, x_2 x_3 \\
2, x_2 x_3 \\
\end{array}
\]

Properties of \(M_i\):

- Each \(M_i\) is an involution \(M_i^2 = 1\)
- The \(M_i\)s commute
  - for each pair, have two qubits with anticommuting \(X\) and \(Z\)
  - \(XZ = -ZX\)
- The two phase factors -1 cancel
- \(M_0 M_1 M_2 M_3 M_4 = 1\)

Because of this, we only use first 4 in error correction
Code states Coding a single bit
\[ |0\rangle = \frac{1}{\sqrt{2}} (|1\rangle + |M_2\rangle) (|1\rangle + |M_3\rangle) \]
\[ |1\rangle = \frac{1}{\sqrt{2}} (|1\rangle - |M_2\rangle) (|1\rangle - |M_3\rangle) \]

Since \( M_i (1+M_i) = 1+M_i \), the states \( |0\rangle \) and \( |1\rangle \) are fixed by every \( M_i \). Their superpositions \( \alpha |0\rangle + \beta |1\rangle \) have eigenstates with eigenvalue 1.

Inner products
\[ (1+M_2)^2 = 2 (1+M_2), \quad \text{so} \]
\[ \langle 0 | 0 \rangle = \langle 0 | M_2 (1+M_2) (1+M_2) (1+M_3) | 0 \rangle \]
\[ = 1 \]

Can use \( (1+M_0) (1+M_2) (1+M_3) \)
\[ = 1 + M_0 M_2 + M_2 + M_0 + M_4 \]
\[ + M_0 M_1 + M_0 M_3 + M_0 M_4 + M_1 M_3 + M_1 M_4 + M_3 M_4 \]

Similarly
\[ \langle 1 | 1 \rangle = 1 \quad \langle 0 | 1 \rangle = 0 \]

Error states - introduced by \( X_i \), \( Y_i \) or \( Z \):
Each of those either commutes or anticommutes with each \( M_i \).
\[ |\psi\rangle = \alpha |0\rangle + \beta |1\rangle \]
when \( |X_i \psi\rangle \), \( |Y_i \psi\rangle \), \( |Z_i \psi\rangle \) all eigenstates of every \( M_j \), eigenvalues ±1.

E.g. \( Y_4 \) anticommutes with \( M_0 \).
\[ |Y_4 \psi\rangle \) eigenstate for \( M_0 \), eigenvalue -1.

Different errors
\[
\begin{array}{cccc}
M_0 & M_1 & M_2 & M_3 \\
2x2 & 2x2 & 2x2 & 2x2 \\
2x2 & 2x2 & 2x2 & 2x2 \\
2x2 & 2x2 & 2x2 & 2x2 \\
\end{array}
\]

\[ X_0, Y_0, Z_0, X_1, Y_1, Z_1, X_2, Y_2, Z_2, X_3, Y_3, Z_3, X_4, Y_4, Z_4 \]

Every column is different.
Read columns as binary numbers:

0  +  +  +  + 
1  =  =  =  = 

Summation of $M$s, then apply correction $A_{x}$ based on result $x$.

Error states: Correct state $|\psi_{0}\rangle = a_{0}|0\rangle + a_{1}|1\rangle$

Corrected state $|\psi\rangle = \sum_{y=0}^{1} a_{y} A_{y} |\psi_{0}\rangle$

$A_{y} |\psi\rangle$ an eigenstate for all $M$s; eigenvalues $(-1)^{y}$

$P_{x}^{M} A_{y} |\psi\rangle = \begin{cases} A_{x} |\psi\rangle & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases}$

Error correction: $p_{x}^{M} |\psi\rangle = A_{x} |\psi\rangle$

How correction works:

Corrupt state $|\psi\rangle = \sum_{y=0}^{1} a_{y} A_{y} |\psi_{0}\rangle$

Measured result $x$ depends probabilistically on amplitudes $a_{y}$

Measurement also reduces state, to $A_{x} |\psi_{0}\rangle$

If $x = 0$, measurement has already corrected state

If $x \neq 0$, measurement reduces to a definite error state $A_{x} |\psi_{0}\rangle$, which can be corrected by applying $A_{x}$